사범대생을 위한 대수학

-정상조 저 (2018년, 경문사)- 2018년 7월7일 수정본

책 본문내용 또는 연습문제 풀이에 대한 오류나 수정할 사항이 있으면 math888@naver.com 으로 연락 주시면 감사합니다.

정오표(↓ 3번째 줄=위에서 3번째 줄, ↑10번째 줄=아래에서 10번째 줄)

쪽	라인	틀린 문장(오)	정정한 문장(정)
36	↓ 2번째 줄	**15. 표현하라.**	**표현할 수 있음을 보여라.**
36	↓13번째 줄	**19. 정수** n	**자연수** n
36	↑10번째 줄	26.	정리 3.1.10을 이용하여
45	↓12번째 줄	**12.**	**정리** 2.3.5를 이용하여
45	↑ 9번째 줄	**13.**	**정리** 2.3.5를 이용하여
53	↓15번째 줄	6.	정리 3.1.10을 이용하여
53	↓17번째 줄	7번 문항 삭제(연습문제 2.2.9와 중복)	
54	↑ 5번째 줄	17. $i\in\mathbb{Z}$	$i\in\mathbb{N}\cup\{0\}$
64	↑ 4번째 줄	2. (문제수정)다음 물음에 답하라. (1) $\sigma\in S_6$과 원소 $a, b\in A=\{1, 2, 3, 4, 5, 6\}$에 대하여 $a\sim b$일 필요충분조건을 적당한 $n\in\mathbb{Z}$에 대하여 $b=\sigma^n(a)$라 할 때 관계 $\sim$은 A 위에서 σ에 의한 동치 관계임을 보여라. (2) 연습문제 1번의 치환 σ, τ, μ에 의한 동치관계에서 각 각의 상집합 S_6/σ, S_6/τ, S_6/μ을 구하라.	
66	↑ 4번째 줄	16. $r(=0, \cdots, n)$	$r(=0, \cdots, n-1)$
89	↑ 5번째 줄	**17. 동형사상이**	**준동형사상이**
90	↑ 9번째 줄	20. (1)과 (2)의 순서를 바꿈	
103	↑ 2번째 줄	8. 부분군 $G'<Z(G)$에 대하여 $\theta: G'\to G$,	부분군 $C_G<Z(G)$에 대하여 $\theta: G\to G$,
104	↓10번째 줄	12. G의 정규부분군	H의 정규부분군
105	↑ 4번째 줄	31. 위수 $2n$인	위수 $2n$(단, n은 소수)인
113	↓ 5번째 줄	2.(1) 부분군의 개수	원소의 개수
113	↓ 6번째 줄	2.(2) 부분군의 개수	원소의 개수
113	↓ 7번째 줄	2.(3) 부분군의 개수	원소의 개수
132	↑ 2번째 줄	3.(8) $(\mathbb{Z}_4\times\mathbb{Z}_8)/<(2, 4)>$	$(\mathbb{Z}_4\times\mathbb{Z}_8)/<(1, 2)>$
140	↑ 6번째 줄	4. $C_x\lhd G$, $\{e\}\subsetneq C_x\subsetneq G$	$G_x\lhd G$, $\{e\}\subsetneq G_x\subsetneq G$
155	↓ 5번째 줄	3.(2) 35인 부분군	35인 정규부분군
155	↓13번째 줄	7. 28인 비가환군에서	28인 군에서
155	↑ 7번째 줄	10. 보여라.	보여라. (참조: $\|a\|=11$일 때 $a=g^{231}ag^{-231}$이용)
155	↑ 2번째 줄	14번 문항 삭제(참조: 박승안 대수학 8판. 연습문제 (6.2) 7번)	
169	↑11번째 줄	14. (문제 수정) 환 R에 대하여 다음 물음에 답하라. (1) R이 영이 아닌 멱영원을 가지지 않을 필요충분조건은 $x^2=0$의 해가 0뿐임을 보여라. (2) 특히 R이 영이 아닌 멱영원을 가지지 않을 때 원소 $a, b\in R$에 대하여 다음을 증명하라. (2-1) $ab=0$이면 $ba=0$이다. (2-2) $aba=0$이면 $ab=0$이다. (2-3) $ab=0$이면 임의의 $x\in R$에 대하여 $axb=0$이다.	
170	↓ 4번째 줄	17. $S=D-\{0\}$	$D^*=D-\{0\}$
170	↑ 5번째 줄	18.(5) 무엇과 같은가?	무엇과 동형인가?
186	↓ 9번째 줄	10. 다음 함수는 환 동형사상임을 보여라.	환 동형사상이 되는 다음 함수를 구하라.
186	↓15번째 줄	13. (문제수정) 체 F와 환 R에 대하여 함수 $\phi: F\to R$가 환 준동형사상이면, $\phi=0$이거나 단사임을 보여라.	
186	↓16번째 줄	14. (문제수정) 체 F에서 환 $R(\neq\{0\})$로의 환 준동형사상 $f: F\to R$이 전사이면, f는 동형사상임을 보여라.	

쪽	라인	틀린 문장(오)	정정한 문장(정)
187	↓ 1번째 줄	17. (문제 수정) 함수 $\phi: \mathbb{H}\to M_2(\mathbb{C})$를 $$\phi(a+bi+cj+dk)=a\begin{pmatrix}1&0\\0&1\end{pmatrix}+b\begin{pmatrix}0&1\\-1&0\end{pmatrix}+c\begin{pmatrix}0&i\\i&0\end{pmatrix}+d\begin{pmatrix}i&0\\0&-i\end{pmatrix}$$ 로 정의하면 ϕ가 단사 환 준동형사상임을 보여라	
187	↑ 7번째 줄	18.(2) $End(R)$의 부분환	$(End(R),+,\circ)$ ($\circ$는 함수의 합성)의 부분환
195	↑ 5번째 줄	2.(4) $\mathbb{Z}_{12}[x]$	$\mathbb{Z}_{12}$
222	↑ 5번째 줄	5. 영과 영인자가 아닌	영인자가 아닌
234	↑ 9번째 줄	13. $N(R)$	$N(R)=\{a\in R\mid a^n=0,\ \exists n\in\mathbb{N}\}$
234	↑ 6번째 줄	14. (문제수정) 가환환 R에 대하여 다음 물음에 답하라. (1) R의 아이디얼 N에 대하여 $\sqrt{N}=\{a\in R\mid \exists n\in\mathbb{N},\ a^n\in N\}$은 R의 아이디얼임을 보여라. 이 아이디얼 $\sqrt{N}$을 N의 래디컬(radical)이라 한다. (2) (정리 6.2.20) (1998학년도 임용시험 출제) $N(R)=\{a\in R\mid a^n=0,\ \exists n\in\mathbb{N}\}$은 R의 아이디얼임을 보여라. 아이디얼 $N(R)$을 닐래디칼(nilradical)이라 한다.	
244	↑ 2번째 줄	8. $\mathbb{Z}_2$	$\mathbb{Z}_3$
247	↓??번째 줄	문제 6.4.6과 따름정리 6.4.8에서 $\{e\}$를 모두 $\{0\}$으로 교체	
278	↓ 1번째 줄	7.2.4 (1) $\gcd(a,b)=\gcd(b,c)=1$	$\gcd(a,c)=\gcd(b,c)=1$
278	↓12번째 줄	7.2.5 $a,b\in D$	$a,b\in D-\{0\}$
282	↓13번째 줄	3. (1) $\gcd(a,b)=\gcd(b,c)=1$	$\gcd(a,c)=\gcd(b,c)=1$
294	↓13번째 줄	2. 구하고, ... 구하라.	한 개씩 구하고, ... 한 개씩 구하라.
295	↑ 7번째 줄	7. $I=\{a\in D\mid \delta(a)>\delta(1)\}\cup\{0\}$	$I=\{a\in D^*\mid \delta(a)>\delta(1)\}\cup\{0\}$
299	↑ 6번째 줄	$a^2-b^2m\geq 0$	$\lvert a^2-b^2m\rvert\geq 0$
302	↓ 4번째 줄	1. (2) $\mathbb{Z}_2$이지만	$\mathbb{Z}_2$는 체이지만
302	↑ 3번째 줄	11. (1) 체임을 증명하라.	체임을 보이고 위수를 구하라.
314	↑14번째 줄	10. $\left\langle \frac{1}{3}x^4-x+6\right\rangle'$(2군데 모두)	$\left\langle \frac{1}{3}x^4-x+2\right\rangle'$
351	↑ 1번째 줄	5(2) 원시다항식	2차 원시다항식
352	↑10번째 줄	14. **위수 p^n 인 유한체 F에서 모든 원소는 단 한 개의 p-제곱근을 가짐을 보여라.**	**위수 p^n 인 유한체 F에서 모든 원소는 단 한 개의 p-제곱근을 가짐을 보여라.** 단, p는 소수
371	↓15번째 줄	$\mathbb{Q}$ 위에서 다항식 $x^3-\sqrt{2}$	$\mathbb{Q}$ 위에서 다항식 x^3-2
378	↑ 4번째 줄	21. 차수를 구하라.	차원을 구하라.
390	↓ 9번째 줄	2. [참조: 정리 9.3.10]	[참조: 정리 9.3.13]
406	↑ 5번째 줄	10. 체 F의 Gaois 확대체	체 F의 유한 Gaois 확대체
407	↑ 8번째 줄	14(3) 치환군 $S_n=\{\alpha_i\mid i=1,\cdots,n\}$의 부분군	$\{\alpha_i\mid i=1,\cdots,n\}$ 위의 치환군 S_n의 부분군
422	↑ 3번째 줄	13. (1) 보여라.	(1) 보여라. 단, $a\neq 0$이다.

== 연습문제 (1.1) ==

1.1.1 (1) $n=1$일 때, $1=\frac{1(1+1)}{2}$이므로 $n=1$일 때는 참이다.

$n=k$에 대하여 즉, $1+2+\cdots+k=\frac{k(k+1)}{2}$이라고 가정하자.

$n=k+1$인 경우

$$1+2+3+\cdots+k+(k+1)=\frac{k(k+1)}{2}+(k+1)=\frac{k(k+1)}{2}+\frac{2(k+1)}{2}=\frac{(k+1)(k+1)}{2}$$

이므로 $1+2+3+\cdots+k+(k+1)=\frac{(k+1)(k+2)}{2}$ 이다. 그러므로 $n=k+1$일 때 등식은 참이다. 따라서 수학적 귀

납법에 의해 임의의 자연수 n에 대하여 등식 $1+2+3+\cdots+n=\frac{n(n+1)}{2}$가 성립한다.

(2) $n=1$일 때, $1=1^2$이므로 참이다.

$n=k$일 때 $1+3+\cdots+(2k-1)=k^2$이라고 가정하자.

$n=k+1$인 경우

$$1+3+\cdots+(2k-1)+(2k+1)=k^2+(2k+1)=(k+1)^2$$

이므로 수학적 귀납법에 의해 임의의 자연수 n에 대하여 $1+3+5+\cdots+(2n-1)=n^2$ 이다.

(3) 수학적 귀납법 Ⅱ를 사용하자.

$n=1$일 때, $a-1=(a-1)\cdot 1$ 이므로 등식이 성립한다.

$1<n\le k$에서 $a^n-1=(a-1)(a^{n-1}+a^{n-2}+a^{n-3}+\cdots+a+1)$이라 가정하자.

$n=k+1$일 때

$$\begin{aligned}a^{k+1}-1&=(a+1)(a^k-1)-a(a^{k-1}-1)\\&=(a+1)(a-1)(a^{k-1}+\cdots+a+1)-a(a-1)(a^{k-2}+\cdots+a+1)\\&=(a-1)[(a+1)(a^{k-1}+\cdots+a+1)-a(a^{k-2}+\cdots+a+1)]\\&=(a-1)[(a^k+\cdots+a^2+a)+(a^{k-1}+\cdots+a+1)-(a^{k-1}+\cdots+a^2+a)]\\&=(a-1)(a^k+a^{k-1}+\cdots+a+1)\end{aligned}$$

이므로 $n=k+1$일 때 성립한다. 다라서, 수학적 귀납법 Ⅱ에 의해 임의의 자연수 n에 대하여

$$a^n-1=(a-1)(a^{n-1}+a^{n-2}+a^{n-3}+\cdots+a+1)$$이다.

1.1.2. 정수 n, m의 곱 mn이 짝수라 하면, mn은 2의 배수이다. 2가 소수이므로 m, n 중의 하나는 2의 배수가 되어 짝수이다. 대우에 의하여 nm은 홀수이다.

1.1.3. 정수 n에 대하여 $n+m=0$이 되는 정수 m이 유일하게 존재함을 귀류증명을 이용하여 증명하여라.

(풀이) (귀류증명) 정수 n에 대하여 $n+m=0$ 이 되는 정수 m이 유일하지 않다고 하자.

즉, $n+m=0$ 를 만족하는 정수 m_1, m_2가 존재한다고 하자.(단, $m_1\neq m_2$)

그러면 $n+m_1=0$이고, $n+m_2=0$ 이므로, $n+m_1=n+m_2$ 이다. 따라서 $m_1=m_2$가 나오는데 이는 가정에 모순이다. 따라서 주어진 명제는 참이다.

(연역증명) 서로 다른 정수 m, m'에 대하여 $n+m=0=n+m'$이라하면 소거법칙에 의해 $m=m'$이 되어 모순이다. 따라서 $n+m=0$인 정수 m이 유일하게 존재한다.

1.1.4. $i)$ x가 음이 아닌 정수인 경우에는 $|-x|=x=|x|$이다.

$ii)$ x가 음수인 경우에는 $|-x|=-x=|x|$이다.

따라서 $|-x|=|x|$ 이 성립한다.

1.1.5.

유리수 근 $x=\frac{a}{b}$(단, a, b는 서로소)가 존재한다고 하자.

$$\left(\frac{a}{b}\right)^2-p\left(\frac{a}{b}\right)+q=0\text{에서}\quad a^2-pab+qb^2=0\text{이다.}$$

a, b는 서로소이므로 둘 다 짝인 경우는 없다.

나머지 경우는 p, q가 홀수이므로

a가 홀수, b가 짝수이면 좌변은 $a^2-pab+qb^2=(\text{홀})-(\text{짝})+(\text{짝})=\text{홀수}$가 되어 모순이다.

a가 짝수, b가 홀수이면 좌변은 $a^2-pab+qb^2=(\text{짝})-(\text{짝})+(\text{홀})=\text{홀수}$가 되어 모순이다.

a가 홀수, b가 홀수이면 좌변은 $a^2-pab+qb^2=(\text{홀})-(\text{홀})+(\text{홀})=\text{홀수}$가 되어 모순이다.

따라서 $x^2-qx+p=0$의 유리수 근이 존재하지 않는다.

1.1.6. 복소수 u, v에 대하여 $\overline{u+v}=\bar{u}+\bar{v}$, $\overline{a\cdot b}=\bar{a}\cdot\bar{b}$를 이용하면

$$\begin{aligned}
&0=f(z)=a_nz^n+\cdots+a_1z+a_0\\
\Rightarrow\ &\bar{0}=\overline{f(z)}=\overline{a_nz^n+\cdots+a_1z+a_0}\\
\Rightarrow\ &0=\overline{a_n}\overline{z^n}+\cdots+\overline{a_1}\bar{z}+\overline{a_0}\\
\Rightarrow\ &0=a_n\bar{z}^n+\cdots+a_1\bar{z}+a_0=f(\bar{z})(\because \text{계수가 실수})
\end{aligned}$$

1.1.7. (1) $z=|z|(\cos\theta+i\sin\theta)$라 하자.

$$1=z^6=|z|^6(\cos6\theta+i\sin6\theta)\Rightarrow|z|=1,\ \cos6\theta+i\sin6\theta=1\Rightarrow\theta=\frac{2n\pi}{6}=\frac{n\pi}{3},\ n\in\mathbb{Z}$$

이므로

$$z=\begin{cases}
\cos0+isin0 & = & 1\\
\cos\dfrac{\pi}{3}+isin\dfrac{\pi}{3} & = & \dfrac{1+\sqrt{3}i}{2}\\
\cos\dfrac{2\pi}{3}+isin\dfrac{2\pi}{3} & = & \dfrac{-1+\sqrt{3}i}{2}\\
\cos\pi+isin\pi & = & -1\\
\cos\dfrac{4\pi}{3}+isin\dfrac{4\pi}{3} & = & \dfrac{-1-\sqrt{3}i}{2}\\
\cos\dfrac{5\pi}{3}+isin\dfrac{5\pi}{3} & = & \dfrac{1-\sqrt{3}i}{2}
\end{cases}$$

(2) $z=|z|(\cos\theta+i\sin\theta)$라 하자.

$$-1=z^6=|z|^6(\cos6\theta+i\sin6\theta)\Rightarrow|z|=1,\ \cos6\theta+i\sin6\theta=-1\Rightarrow\theta=\frac{(2n-1)\pi}{6},\ n\in\mathbb{Z}$$

이므로

$$z=\begin{cases}
\cos\dfrac{\pi}{6}+isin\dfrac{\pi}{6} & = & \dfrac{\sqrt{3}+i}{2}\\
\cos\dfrac{\pi}{2}+isin\dfrac{\pi}{2} & = & i\\
\cos\dfrac{5\pi}{6}+isin\dfrac{5\pi}{6} & = & \dfrac{-\sqrt{3}+i}{2}\\
\cos\dfrac{7\pi}{6}+isin\dfrac{7\pi}{6} & = & \dfrac{-\sqrt{3}-i}{2}\\
\cos\dfrac{3\pi}{2}+isin\dfrac{3\pi}{2} & = & -i\\
\cos\dfrac{11\pi}{6}+isin\dfrac{11\pi}{6} & = & \dfrac{\sqrt{3}-i}{2}
\end{cases}$$

(3) $z=|z|(\cos\theta+i\sin\theta)$라 하자.

$$-27i=z^3=|z|^3(\cos3\theta+i\sin3\theta)\Rightarrow|z|=3,\ \cos3\theta+i\sin3\theta=-i\Rightarrow\theta=\frac{\left(2n+\frac{3}{2}\right)\pi}{3}=\frac{(4n+3)\pi}{6},\ n\in\mathbb{Z}$$

이므로

$$z=\begin{cases}
3\left(\cos\dfrac{\pi}{2}+isin\dfrac{\pi}{2}\right) & = & 3i\\
3\left(\cos\dfrac{7\pi}{6}+isin\dfrac{7\pi}{6}\right) & = & \dfrac{-3\sqrt{3}-3i}{2}\\
3\left(\cos\dfrac{11\pi}{6}+isin\dfrac{11\pi}{6}\right) & = & \dfrac{3\sqrt{3}-3i}{2}
\end{cases}$$

== 연습문제 (1.2) ==

1.2.1. (1) 60 (2) 40 (3) 100

== 연습문제 (1.3) ==

1.3.1. (1) 추이관계만 성립한다.
동치관계를 만족시키기 위해서는 반사, 대칭, 추이 관계를 만족해야 한다. 반사관계를 만족하기 위해서는 {(1,1),(2,2),(3,3)}이 포함되어야 하고, 대칭관계를 만족시키기 위해서는 {(2,1)}이 포함되어야 하며, 위의 모든 것을 포함할 때 추이관계를 만족한다.
그러므로 집합 $B=\{(1,1),(2,2),(3,3),(1,2),(2,1)\}$이다.
R'에 의한 A의 상집합 $A/R'=\{\overline{1},\overline{2},\overline{3}\}=\{\overline{1},\overline{3}\}=\{\overline{2},\overline{3}\}=\{\{1,2\},\{3\}\}$이다.

(2) 대칭관계와 추이관계만 성립한다.
동치관계를 만족시키기 위해서는 반사, 대칭, 추이 관계를 만족해야 한다. 반사관계를 만족하기 위해서는 {(1,1),(2,2),(3,3)}이 포함되어야 하므로 {(3,3)}을 포함시켜주면 반사, 대칭, 추이 관계를 만족한다.
그러므로 집합 $B=\{(1,1),(2,2),(3,3)\}$이다.
R'에 의한 A의 상집합 $A/R'=\{\overline{1},\overline{2},\overline{3}\}=\{\{1\},\{2\},\{3\}\}$ 이다.

(3) 반사관계와 추이관계만 성립한다.
동치관계를 만족시키기 위해서는 반사, 대칭, 추이 관계를 만족해야 한다. 대칭관계를 만족하기 위해서는 {(2,1),(3,2),(3,1)}이 포함되어야 한다.
그러므로 집합 $B=\{(1,1),(2,2),(3,3),(1,2),(2,3),(1,3),(2,1),(3,2),(3,1)\}$이다.
R'에 의한 A의 상집합 $A/R=\{\overline{1}\}=\{\overline{2}\}=\{\overline{3}\}=\{\{1,2,3\}\}$이다.

(4) A위에서 모든 동치관계는 $\{(1,1),(2,2),(3,3)\}$, $\{(1,1),(2,2),(3,3),(1,2),(2,1)\}$,
$\{(1,1),(2,2),(3,3),(2,3),(3,2)\}$, $\{(1,1),(2,2),(3,3),(1,3),(3,1)\}$,
$\{(1,1),(2,2),(3,3),(1,2),(2,3),(1,3),(2,1),(3,2),(3,1)\}$이다.

1.3.2.
R이 A 위에서 동치관계라 하자. R의 상집합 $A/R=\{\overline{a_i}\subset A \mid i\in I\}$라 하자.

먼저, 임의의 원소 $a\in A$에 대하여 $(a,a)\in R$이므로 $a\in\overline{a}\in A/R$이다. 따라서 $\bigcup_{i=1}^{n}\overline{a_i}=A$이다.

이제, 임의의 원소 a_m, a_n에 대하여 $\overline{a_m}\cap\overline{a_n}=\varnothing$이거나 $\overline{a_m}=\overline{a_n}$임을 보이면 된다.
$\overline{a_m}\cap\overline{a_n}\neq\varnothing$이라 하자. 그러면 적당한 원소 $b\in\overline{a_m}\cap\overline{a_n}$가 존재하고,
$(a_m,b)\in R$이고 $(a_n,b)\in R$이다.
R이 동치관계이므로 대칭관계에 의해서 $(b,a_m),(b,a_n)\in R$이므로
$(a_m,b),(b,a_n)\in R$이고 $(a_n,b),(b,a_m)\in R$이다.
임의의 원소 $x\in\overline{a_m}$에 대하여
$x\in\overline{a_m}\Rightarrow(a_m,x)\in R\Rightarrow(b,x)\in R(\because(b,a_m)\in R)\Rightarrow(a_n,x)\in R(\because(a_n,b)\in R)\Rightarrow x\in\overline{a_n}$
이다. 그러므로 $\overline{a_m}\subset\overline{a_n}$이다. 같은 방법으로 $\overline{a_n}\subset\overline{a_m}$을 보일 수 있다.
따라서 $\overline{a_m}=\overline{a_n}$ 이다. 그러므로 $A/R=\{\overline{a_i}\subset A \mid i\in I\}$은 A의 분할이다.

1.3.3. $\overline{a}=\{a,b,c\}$, $\overline{d}=\{d\}$

1.3.4. (1) 동치관계를 만족하기 위해서는 반사, 대칭, 추이 관계를 만족해야 한다.
① 반사 : $\forall a\in\mathbb{Z}$, $(a,a)\Leftrightarrow a-a=0$는 항상 5의 배수이므로 $(a,a)\in R$
$\therefore$ 반사관계를 만족한다.
② 대칭 : $\forall x,y\in\mathbb{Z}$, $(x,y)\in R\Rightarrow(y,x)\in R$ 이면 대칭관계
$x-y=5k,k\in\mathbb{Z}$ 이므로 ($\because$ 가정에서 $(x,y)\in R$)
$y-x=-5k=5(-k)$ 가 성립한다. $\therefore$ 대칭관계를 만족한다.
③ 추이 : $\forall x,y,z\in\mathbb{Z}$, $(x,y),(y,z)\in R\Rightarrow(x,z)\in R$ 이면 추이관계
$x-y=5k, y-z=5l, k,l\in\mathbb{Z}$ 이므로
$x-z=5k-5l=5(k-l)$ 이 성립한다. $\therefore$ 추이관계를 만족한다. $\therefore$ 동치관계
1의 동치류는 $\overline{1}=\{1-5k|k\in\mathbb{Z}\}$이다.

(2) 동치관계를 만족하기 위해서는 반사, 대칭, 추이 관계를 만족해야 한다.
① 반사 : $\forall(x,y)\in\mathbb{Z}\times\mathbb{Z}$, $(x,y)R(x,y)\Leftrightarrow x+y=y+x$ 이므로 반사관계를 만족한다.
② 대칭 : $\forall(a,b),(c,d)\in\mathbb{Z}\times\mathbb{Z}$, $(a,b)R(c,d)\Rightarrow(c,d)R(a,b)$ 임을 보이자.
$(a,b)R(c,d)$가 성립하므로 $a+d=b+c$ 가 성립한다.
$(c,d)R(a,b)$를 정리하면 $c+b=a+d$ 이므로 대칭관계를 만족한다.
③ 추이 : $\forall(a,b),(c,d),(e,f)\in\mathbb{Z}\times\mathbb{Z}$, $(a,b)R(c,d)\wedge(c,d)R(e,f)\Leftrightarrow(a,b)R(e,f)$이 성립함을 보이자.
$(a,b)R(c,d)$와 $(c,d)R(e,f)$ 가 성립하므로 $a+d=b+c$ 이고, $c+f=d+e$ 이 성립한다. 두 위의 식을 조작하면 각각, $a-b=c-d$ 와 $c-d=e-f$ 가 되고
$a-b=e-f$ 가 된다. 따라서 $a+f=b+e\Leftrightarrow(a,b)R(e,f)$ 가 성립하고 추이관계를 만족한다. $\therefore$ 동치관계이다.
답) $\overline{(1,1)}=\{(a,b):1+b=a+1\}=\{(a,a):a\in\mathbb{Z}\}$

1.3.5.
임의의 $x\in X$에 대하여 $(x,x)\in R$이므로 반사관계이다.
$(a,b)\in R$이라 하자. a가 홀수이면 $a=b$이어야 하므로 $(b,a)=(a,a)\in R$ 이다.
a가 짝수이면 $(b,a)\in R$ 이므로 R 은 대칭관계이다.
$(a,b),(b,c)\in R$ 이라 하자.
a가 홀수이면 $a=b$이어야 하므로 b도 홀수가 되어 $b=c$이다. 따라서 $(a,c)=(a,a)\in R$ 이다.
a가 짝수이면 b도 짝수이어야 하므로 c도 짝수이다. 그러므로 $(a,c)\in R$ 이므로 R 은 추이관계이다.
따라서 R 은 동치관계이다.

1.3.6. 동치관계를 만족하기 위해서는 반사, 대칭, 추이 관계를 만족해야 한다.
① 반사 : $\forall a\in\mathbb{R}$, $\int_a^a f(x)\,dx=0$이므로 aRa이다.
② 대칭 : $\forall a,b\in\mathbb{R}$, aRb 라 하자.

$$aRb\Rightarrow\int_a^b f(x)\,dx=0\Rightarrow\int_b^a f(x)=-\int_a^b f(x)=0\Rightarrow bRa$$

이므로 대칭관계를 만족한다.
③ 추이 : aRb와 bRc이면, $\int_a^b f(x)dx=0$, $\int_b^c f(x)=0$이다.

$$\int_a^c f(x)dx=\int_a^b f(x)dx+\int_b^c f(x)dx=0+0=0$$

이므로 추이관계를 만족한다. $\therefore$ 동치관계이다.

1.3.7. (1) $\forall x\in\mathbb{R},\ f(x)=f(x) \Rightarrow xSx$이다. 즉, 반사관계이다.
$xSy \Rightarrow f(x)=f(y) \Rightarrow f(y)=f(x) \Rightarrow ySx$이이므로 대칭관계이다.
$xSy,\ ySz$라 하면
$f(x)=f(y),\ f(y)=f(z) \Rightarrow f(x)=f(z) \Rightarrow xSz$이므로 추이관계가 성립한다.
그러므로 동치관계이다.

(2) $x\in\overline{1} \Rightarrow f(x)=f(1) \Rightarrow x^2=1 \Rightarrow x=1,-1$
그러므로 $\overline{1}=\{1,-1\}$

(3) $x\in\overline{-2} \Rightarrow f(x)=f(-2)=2 \Rightarrow \begin{cases} -\frac{1}{x}=2,\ \text{if } x>0 \Rightarrow x=-\frac{1}{2}(\text{모순}) \\ -x=2,\ \text{if } x<0 \Rightarrow x=-2 \end{cases}$
그러므로 -2의 동치류는 -2뿐이다.
그러므로 $\overline{-2}=\{-2\}$

== 연습문제 (1.4) ==

1.4.1. f의 역함수를 f',f''이라 하자. 그러면 $f\circ f'=f'\circ f=id,\ f\circ f''=f''\circ f=id$이다.
$$f'=f'\circ id=f'\circ(f\circ f'')=(f'\circ f)\circ f''=id\circ f''=f''$$
$\therefore$ 함수 f의 역함수가 존재하면 유일하다.

1.4.2. ($\Rightarrow$) f의 역함수 f^{-1}가 존재한다고 하자. 그러면 $f\circ f^{-1}=I_Y,\ f^{-1}\circ f=I_X$이다.
$f(x)=f(x') \Rightarrow f^{-1}(f(x))=f^{-1}(f(x')) \Rightarrow I_X(x)=I_X(x') \Rightarrow x=x'$
이므로 f는 단사함수이다. 또한 임의의 $y\in Y$에 대하여
$y=I_Y(y)=f\circ f^{-1}(y)=f(f^{-1}(y))(\exists f^{-1}(y)\in X)$이므로 f는 전사함수이다.
그러므로 f는 전단사함수이다.

($\Leftarrow$) f는 전단사함수라 하자. f가 전사 함수이므로
함수 $g:Y\to X,\ g(y)=x,$ (단, $f(x)=y$)라 정의하자. 그러면 임의의 $x\in X$에 대하여
$f(x)=y$인 $y\in Y$가 유일하게 존재하므로 g는 잘 정의된다.
또한 임의의 $x\in X,\ y\in Y$에 대하여
$$\begin{cases} f\circ g(y)=f(g(y))=f(x)=y \\ g\circ f(x)=g(f(x))=g(y)=x \end{cases}$$
이므로 $f\circ g=I_Y,\ g\circ f=I_X$가 되어 g가 f의 역함수이다.

1.4.3. (1) $x\in A \Rightarrow f(x)\in f(A) \Rightarrow x\in f^{-1}(f(A))$이므로 $\therefore A\subset f^{-1}(f(A))$

(2) 거짓
(반례) $f:\mathbb{Z}\to\mathbb{Z},\ f(x)=2x,\ B=\{1\} \Rightarrow f^{-1}(B)=\varnothing$

(3) $f(a)\in f(A\cup A') \Leftrightarrow a\in A\cup A' \Leftrightarrow a\in A \vee a\in A' \Leftrightarrow f(a)\in f(A) \vee f(a)\in f(A') \Leftrightarrow f(a)\in f(A)\cup f(A')$
$\therefore f(A\cup A')=f(A)\cup f(A')$

(4) $X=\{1,2,3\},\ A=\{1,2\},\ A'=\{2,3\},\ B=\{1\},\ f(x)=1$ 이라 하면
$f(A-A')=1\neq f(A)-f(A')=\varnothing$ 이다.

(5) $x\in f^{-1}(B\cap B') \Leftrightarrow f(x)\in B\cap B' \Leftrightarrow f(x)\in B\wedge f(x)\in B' \Leftrightarrow x\in f^{-1}(B)\wedge x\in f^{-1}(B))$
$\Leftrightarrow x\in f^{-1}(B)\cap f^{-1}(B') \quad \therefore f^{-1}(B\cap B')=f^{-1}(B)\cap f^{-1}(B')$

1.4.4. (1) f의 정의역 $x\in\mathbb{R}$, 공역 $y>-1$ 으로 정하면, $f(x)$의 역함수는
$y=\ln(x+1)-2\,(x>-1)$이 된다.

(2) $x,x'\in(\mathbb{R}-\{1\})$, $f(x)=f(x') \Leftrightarrow 2+\frac{1}{x-1}=2+\frac{1}{x'-1} \Leftrightarrow x=x'$이므로 f는 단사,

$\forall y\in(\mathbb{R}-\{2\})$, $\exists \frac{1}{y-2}+1\in(\mathbb{R}-\{1\})$, $f(x)=y$ 이므로 f는 전사이다. 따라서

f는 전단사이다. $f^{-1}(x)=\frac{1}{x-2}+1$이다.

1.4.5.
(1) $g\circ f(x)=g\circ f(y)$ 이면 함수 g가 단사이므로 $f(x)=f(y)$이고 함수 f가 단사이므로 $x=y$가 된다. 따라서 함수 $g\circ f$는 단사이다.

(2) $g\circ f(X)=g(f(X))=g(Y)=Z$이므로 $g\circ f$는 전사이다.

(3) (1)과 (2)에 의하여 성립한다.

(4) $f(x)=f(y)$
$\Rightarrow g(f(x))=g(f(y))$
$\Rightarrow x=y(\because g\circ f$가 단사$)$
그러므로 f는 단사함수이다.

(5) $g\circ f$가 전사이므로 $Z=g(f(X))\subset g(Y)\subset Z$이다. 따라서 $g(Y)=Z$가 되어 g는 전사함수이다.

(6) (4)와 (5)에 의하여 성립한다.

== 연습문제 (2.1) ==

2.1.1.

$a*b=ab+1$
$b*a=ba+1=ab+1$

$(a*b)*c=(ab+1)*c=(ab+1)c+1=abc+c+1$
$a*(b*c)=a*(bc+1)=a(bc+1)+1=abc+a+1$

이므로 가환적이지만 결합적이지 않다.

2.1.2. 임의의 원소 $a,b\in H, x\in S$에 대하여

$$(a*b)*x=a*(b*x)=a*(x*b)=(a*x)*b=(x*a)*b=x*(a*b)$$

이므로 $a*b\in H$이다. 따라서 H는 $*$ 아래서 닫혀있다.

2.1.3. 임의의 원소 $a,b\in H$에 대하여

$$(a*b)*(a*b)=a*(b*a)*b=a*(a*b)*b=(a*a)*(b*b)=a*b$$

이므로 $a*b\in H$이다. 따라서 H는 $*$ 아래서 닫혀있다.

2.1.4. (1) $*$ 의 항등원은 1이다. (2) $1^{-1}=1,\ 2^{-1}=4,\ 3^{-1}=3,\ 4^{-1}=2$

2.1.5.
$$a*c=a*(b*d)=(a*b)*d=b*d=c$$
$$a*d=a*(b*b)=(a*b)*b=b*b=d$$
$$d*b=(c*c)*b=c*(c*b)=c*a=c$$
$$d*c=(c*c)*c=c*(c*c)=c*d=b$$

항등원 a

역원 $a^{-1}=a,\ b^{-1}=c,\ c^{-1}=b,\ d^{-1}=d$

(별해) 연산표가 군이 되기 위해서는 세로와 가로가 같은 원소가 오면 안되므로 $d*b=c$가 되어야 한다.
따라서 $d*c=b$가 되어야 하고, 차례로 $a*c=c,\ a*d=d$가 되어야 한다.

2.1.6.

(1) $(a*b)*c=(a+b+ab)*c=(a+b+ab)+c+(a+b+ab)c=abc+ab+ac+bc+a+b+c$
$a*(b*c)=a*(b+c+bc)=a+(b+c+bc)+a(b+c+bc)=abc+ab+ac+bc+a+b+c$
$\Rightarrow (a*b)*c=a*(b*c)$

(2) $a*b=a+b+ab=b+a+ba=b*a$

(3) $a*b=a*c$
$\Leftrightarrow a+b+ab=a+c+ac$
$\Leftrightarrow (a+1)(b-c)=0$
$\Leftrightarrow b-c=0(\because a\neq -1)$
$\Leftrightarrow b=c$

2.1.7.

(1) 항등원을 e라 하자.
$$a=a*e=a+e-ae(=e+a-ea=e*a)$$
$\Rightarrow (1-a)e=0$
$\Rightarrow e=0(\because a\neq 1)$

(2) (1)에서 항등원 0이 존재한다.
$$(a*b)*c=(a+b-ab)*c=(a+b-ab)+c-(a+b-ab)c=abc-ab-ac-bc+a+b+c$$
$$a*(b*c)=a*(b+c-bc)=a+(b+c-bc)-a(b+c-bc)=abc-ab-ac-bc+a+b+c$$
$$\Rightarrow (a*b)*c=a*(b*c)$$

역원을 x라 하자.
$$0=a*x=x*a=a+x-ax$$
$$\Rightarrow x(a-1)=a$$
$$\Rightarrow a^{-1}=x=\frac{a}{a-1}(\because a\neq 1)$$

이므로 (G,$*$)는 군이다.

(3) $2*x*3=-1 \Rightarrow x=\frac{2}{2-1}*(-1)*\frac{3}{3-1}=0$

2.1.8. (1) $\forall\, a,b,c\in\mathbb{R}$에 대해
$$(a\circ b)\circ c=(a+b+5)\circ c=(a+b+5)+c+5=a+b+c+10$$
$$a\circ(b\circ c)=a\circ(b+c+5)=a+(b+c+5)+5=a+b+c+10$$

이므로 결합법칙이 성립한다.

$a\in\mathbb{R}$
$(a\circ e)=a+e+5=a$
$(e\circ a)=e+a+5=a$
$\therefore e=-5$ (항등원 존재)

$a, a'\in\mathbb{R}$
$a\circ a'=a+a'+5=-5$
$a'\circ a=a'+a+5=-5$
$\therefore a'=-10-a$ (역원존재)

$\mathbb{R}$에서 $x\circ y=x+y+5$이면 군이다.

(2) $\forall a, b, c \in \mathbb{R}$에 대해

$$(a \circ b) \circ c = \left(\frac{ab}{2}\right) \circ c = \frac{\frac{ab}{2}c}{2} = \frac{abc}{4}$$

$$a \circ (b \circ c) = a \circ \left(\frac{bc}{2}\right) = \frac{a\frac{bc}{2}}{2} = \frac{abc}{4}$$

$\therefore (a \circ b) \circ c = a \circ (b \circ c)$

$a \in \mathbb{R}$에 대해

$$a \circ e = \frac{ae}{2} = a$$

$$e \circ a = \frac{ea}{2} = a \qquad \therefore e = 2$$

이므로 항등원 2가 존재한다.

$a, a' \in \mathbb{R}$에 대해

$2 = a \circ a' = \frac{aa'}{2}$에서 $a = 0$이면 역원이 없어 군이 아니다.

(3) (6번문제와 같음) $\forall a, b, c \in \mathbb{R} - \{-1\}$에 대해

$(a \circ b) \circ c = (a+b+ab) \circ c = (a+b+ab)+c+(a+b+ab)c = a+b+c+ab+ac+bc+abc$
$a \circ (b \circ c) = a \circ (b+c+bc) = a+(b+c+bc)+a(b+c+bc) = a+b+c+ab+ac+bc+abc$
$\therefore (a \circ b) \circ c = a \circ (b \circ c)$

$\forall a \in \mathbb{R} - \{-1\}$에 대해

$a \circ e = a+e+ae = a$
$e \circ a = e+a+ea = a$
$e(a+1) = 0 \qquad \therefore e = 0 \ (\because a \neq -1)$ (항등원 존재)

$\forall a, a' \in \mathbb{R} - \{-1\}$에 대해

$a \circ a' = a+a'+aa' = 0$
$a' \circ a = a'+a+a'a = 0$
$a' = \frac{-a}{a+1}$ (역원존재)

$\mathbb{R} - \{-1\}$에서 $x \circ y = x+y+xy$이면 군이다.

(4) $\forall a, b, c \in I$에 대해

$$a \circ (b \circ c) = a \circ \left(\frac{bc}{bc+1}\right) = \frac{a\frac{bc}{bc+1}}{a\frac{bc}{bc+1}+1} = \frac{abc}{abc+bc+1}$$

$$(a \circ b) \circ c = \left(\frac{ab}{ab+1}\right) \circ c = \frac{c\frac{ab}{ab+1}}{c\frac{ab}{ab+1}+1} = \frac{abc}{abc+ab+1}$$

$\therefore a \circ (b \circ c) \neq (a \circ b) \circ c$

결합법칙이 성립하지 않는다.

$I = (-1,1)$ 에서 $x \circ y = \frac{xy}{xy+1}$이면 군이 되지 않는다.

2.1.9. ① 2의 곱셈 역원이 없어 군이 아님.
② 군이다.

③ 군이다.

④ 2의 곱셈 역원이 없어 군이 아님.

2.1.10. (1) 교환법칙 성립 안함

(반례) $f_2(f_4(x)) = f_2\left(\frac{1}{x}\right) = \frac{x}{x-1}$,

$f_4(f_2(x)) = f_2\left(\frac{1}{1-x}\right) = 1-x$

(2) f_1

(3) ${f_1}^{-1} = f_1,\ {f_2}^{-1} = f_3,\ {f_3}^{-1} = f_2,\ {f_4}^{-1} = f_4,\ {f_5}^{-1} = f_5,\ {f_6}^{-1} = f_6$

(4) 함수의 합성은 결합법칙이 성립(정리 1.4.8)하므로 (2)와 (3)에 의하여 군이다.

2.1.11. 먼저 집합 $n\mathbb{Z}$가 + 연산에 닫혀있음을 보이자.

임의의 $na, nb \in n\mathbb{Z}$에 대하여 $na+nb = n(a+b) \in n\mathbb{Z}$이므로 집합 $n\mathbb{Z}$는 +연산에 닫혀있다.

결합법칙이 성립함을 보이자.

$na, nb, nc \in n\mathbb{Z}$에 대하여 $na+(nb+nc) = na+n(b+c) = n(a+b+c)$ 이고

$(na+nb)+nc = n(a+b)+nc = n(a+b+c)$이므로 이항연산$(n\mathbb{Z},+)$은 결합법칙이 성립한다.

항등원이 존재함을 보이자.

$0 = n \cdot 0 \in n\mathbb{Z}$이고 $na+0 = 0+na = na$이므로 이항연산$(n\mathbb{Z},+)$는 항등원 0이 존재한다.

역원이 존재함을 보이자. $na \in n\mathbb{Z}$에 대하여 $n(-a) \in n\mathbb{Z}$가 존재하여

$na+n(-a) = n(a+(-a)) = n \cdot 0 = 0$ 이다. 따라서 모든 $na \in n\mathbb{Z}$에 대하여 역원이 존재한다. 따라서 이항연산 $(n\mathbb{Z},+)$는 군이다.

2.1.12. $a' = a-2,\ b' = b-2$라 하면 $a = a'+2,\ b = b'+2$이므로

$$(a-2)*(b-2) = a+b-2$$
$$\Rightarrow a'*b' = (a'+2)+(b'+2)-2 = a'+b'+2$$

이다.

$\forall a, b, c \in \mathbb{Z}$에 대해

$$(a \circ b) \circ c = (a+b+2) \circ c = (a+b+2)+c+2 = a+b+c+4$$
$$a \circ (b \circ c) = a \circ (b+c+2) = a+(b+c+2)+2 = a+b+c+4$$
$$\therefore (a \circ b) \circ c = a \circ (b \circ c)$$

$\forall a \in \mathbb{Z}$에 대해

$$a \circ e = a+e+2 = a$$
$$e \circ a = e+a+2 = a$$
$$\therefore e = -2 \text{(항등원 존재)}$$

$\forall a, a' \in \mathbb{Z}$에 대해

$$a \circ a' = a+a'+2' = -2$$
$$a' \circ a = a'+a+2 = -2$$
$$a' = -a-4 \text{(역원존재)}$$

$\forall a, b \in \mathbb{Z}$에 대해

$$a \circ b = a+b+2 = b+a+2 = b \circ a$$
$$\therefore a \circ b = b \circ a$$

$(\mathbb{Z},*)$은 가환군이다.

2.1.13. $\forall a+a'i,\ b+b'i,\ c+c'i \in \mathbb{C}-\{0\} = \mathbb{C}^*$에 대해

$$((a+a'i)\cdot(b+b'i))\cdot(c+c'i) = (a+a'i)\cdot((b+b'i)\cdot(c+c'i))$$

$\forall a+a'i \in \mathbb{C}^*$에 대해

$$(a+a'i)\cdot 1 = a+a'i = 1\cdot(a+a'i)$$

$\forall\, a+a'i,\ \dfrac{a-a'i}{a^2+a'^2}\in\mathbb{C}^*$에 대해

$$(a+a'i)\cdot\frac{a-a'i}{a^2+a'^2}=\frac{a-a'i}{a^2+a'^2}\cdot(a+a'i)=1$$

$\forall\, a+a'i,\ b+b'i\in\mathbb{C}^*$에 대해

$$(a+a'i)\cdot(b+b'i)=ab-a'b'+(ab'+a'b)i=(b+b'i)\cdot(a+a'i)$$

$(\mathbb{C}^*,\cdot)$은 가환군이다.

2.1.14. (1) $\forall\, a,b,c\in\mathbb{R}^+,\ (a*b)*c=\sqrt{\sqrt{ab}\,c}\neq\sqrt{a\sqrt{bc}}=a*(b*c)$이므로 (G_1) 결합법칙이 성립하지 않는다.

(2) (G_1)은 성립한다. 하지만 $a*e=|a\cdot e|=a\Rightarrow e=\pm1$이므로 (G_2) 항등원이 존재하지 않는다.

2.1.15.
$$\begin{aligned} & axa=a \\ \Rightarrow\ & x(axa)x=xax \\ \Rightarrow\ & x((axa)xa)x=xax \\ \Rightarrow\ & (xax)a(xax)=xax \end{aligned}$$

이므로 $y=xax$라 하면 $yay=y$이고

$$aya=a(xax)a=(axa)xa=axa=a$$

가 성립한다.

2.1.16.
$$\begin{aligned} & x^2=x\circ x=x \\ \Rightarrow\ & (x\circ x)\circ x_R=x\circ x_R \\ \Rightarrow\ & x\circ(x\circ x_R)=e_R \\ \Rightarrow\ & x\circ e_R=e_R \\ \Rightarrow\ & x=e_R \end{aligned}$$

2.1.17. $(a_Ra)(a_Ra)=a_R(aa_R)a=(a_Re_R)a=a_Ra$이므로 16번에 의하여 $a_Ra=e_R$이다. 그러므로 a_R은 a의 좌역원이다.
다음에 임의의 $a\in G$에 대하여

$$e_Ra=(aa_R)a=a(a_Ra)=ae_R=a$$

이므로 e_R은 좌항등원이다. 그러므로 G는 군이다.

(별해) 좌항등원과 좌역원이 존재함을 보이면 된다. 먼저 좌역원이 존재함을 보이자.
a'을 a의 우역원이라 하고, a''을 a'의 우역원이라 하자. 그러면

$$aa'=e_R,\ \ aa''=e_R$$

이다. 따라서 첫 번째 식에 a'의 우역원 a''을 오른쪽에 곱하면, 결합법칙이 성립하므로

$$e_Ra''=(aa')a''=a(a'a'')=ae_R=a\quad\Rightarrow\quad a=e_Ra''$$

이다. 이를 이용하여 a'이 a의 좌역원임을 보이자.

$$a'a=a'(e_Ra'')=(a'e_R)a''=a'a''=e_R$$

이므로 a'은 a의 좌역원이다.
다음에 e_R이 좌항등원임을 보이자.

$$e_Ra=(aa')a=a(a'a)=ae_R=a$$

이므로, e_R은우항등원이다. 따라서 G는 군이 된다.

2.1.18. (1) $(a*b)*c=(|a|b)*c=|ab|c=|a||b|c=|a|(b*c)=a*(b*c)$
$\therefore\ (a*b)*c=a*(b*c)$

(2) $a = e_L{}^*a = |e_L|a \;\Rightarrow\; e_L = \pm 1$이므로 좌항등원이 존재하지만 $a = a^*e_R = |a|e_R$에서 우항등원(고정된 원소가 존재해야 하므로, 즉, $e_R = 1$[존재한다고 가정하면 $a < 0$일 때 모순]은 존재하지 않는다. 같은 방법으로 $e_R = -1$도 존재하지 않는다. 따라서 항등원의 유일성에 모순이다.

$\pm 1 = a^*a_R = |a|a_R \;\Rightarrow\; a_R = \pm\frac{1}{a}$이므로 우역원이 존재한다. 하지만 $\pm 1 = a_L{}^*a = |a_L|a$이라서 좌역원이 존재하지 않는다.

(3) 우항등원이 없으므로 군이 아니다.

(4) 연산이 결합적이고 좌항등원과 우역원이 존재하더라도 방향(왼쪽 항등원과 오른쪽 역원)이 다르게 존재하면 군이 되지 않는다. (참조: 좌공리와 우공리)

2.1.19. $|G| = m$이라 하자.
임의의 $x \in G$에 대하여 $\{e, x, ..., x^m\} \subset G$, $|G| = m$이므로 $|\{e, x, ..., x^m\}| \le m$이어야 한다.
따라서 $x^i = x^j (0 \le j < i \le m)$인 x^i, x^j가 존재하고, 소거법칙에 의해서 $e = x^{i-j}$인 $i - j = m \in \mathbb{N}$이 존재한다.
$\therefore x^m = e$가 되는 자연수 m이 존재한다.

2.1.20.
$x^*y = e$
$\Rightarrow \; (x^*y)^*x = e^*x = x^*e$
$\Rightarrow \; x^*(y^*x) = x^*e$
$\Rightarrow \; y^*x = e \; (\because$ 소거법칙 정리 2.1.10$)$

(별해) G가 군이므로 $x \in G$이면 $x^{-1} \in G$이다. $x^*y = e$에 양변의 왼쪽에 x^{-1}을 연산하면 $y = x^{-1}$이다. $y^*x = x^{-1}{}^*x = e$이다.

2.1.21. (풀이) $(ab)^{-1} = a^{-1}b^{-1} \;\Leftrightarrow\; ab(ab)^{-1} = aba^{-1}b^{-1} \;\Leftrightarrow\; e = aba^{-1}b^{-1} \;\Leftrightarrow\; b = aba^{-1} \;\Leftrightarrow\; ba = ab$
(별해) $(ab)^{-1} = a^{-1}b^{-1} \Leftrightarrow \left((ab)^{-1}\right)^{-1} = \left(a^{-1}b^{-1}\right)^{-1} \Leftrightarrow ab = (b^{-1})(a^{-1})^{-1} = ba$

2.1.22. $a, b \in G$
$(ab)^2 = a^2b^2$
$\Rightarrow \; (ab)(ab) = a^2b^2$
$\Rightarrow \; a^{-1}(ab)(ab)b^{-1} = a^{-1}aabbb^{-1}$
$\Rightarrow \; ebae = eabe$
$\Rightarrow \; ba = ab$
G는 가환군이다.

2.1.23.
$(ab)^3 = a^3b^3 \Rightarrow baba = a^2b^2$
$(ab)^5 = a^5b^5 \;\Rightarrow\; ababababab = a^5b^5 \;\Rightarrow\; (baba)(baba) = a^4b^4 \;\Rightarrow\; \left(a^2b^2\right)\left(a^2b^2\right) = a^4b^4 \;\Rightarrow\; b^2a^2 = a^2b^2 = baba$
$\Rightarrow \; bbaa = baba \;\Rightarrow\; ba = ab$

2.1.24.
1) $(ab)^{i-1} = a^{i-1}b^{i-1} \;\Rightarrow\; \underbrace{(ab)\cdots(ab)}_{i-1\text{개}} = a^{i-1}b^{i-1} \;\Rightarrow\; \underbrace{(ba)\cdots(ba)}_{i-2\text{개}} = a^{i-2}b^{i-2} \;\Rightarrow\; (ba)^{i-2} = a^{i-2}b^{i-2}$
2) $(ab)^i = a^ib^i \;\Rightarrow\; \underbrace{(ab)\cdots(ab)}_{i\text{개}} = a^ib^i \;\Rightarrow\; \underbrace{(ba)\cdots(ba)}_{i-1\text{개}} = a^{i-1}b^{i-1} \;\Rightarrow\; (ba)^{i-1} = a^{i-1}b^{i-1} \;\Rightarrow\; a^{i-2}b^{i-2}ba = a^{i-1}b^{i-1}$
$\Rightarrow \; b^{i-2}ba = ab^{i-1}$

3) $(ab)^{i+1}=a^{i+1}b^{i+1} \Rightarrow \underbrace{(ab)\cdots(ab)}_{i+1개}=a^{i+1}b^{i+1} \Rightarrow \underbrace{(ba)\cdots(ba)}_{i개}=a^ib^i \Rightarrow a^{i-1}b^{i-1}ba=a^ib^i \Rightarrow b^{i-1}ba=ab^i$

$\Rightarrow b(b^{i-2}ba)=ab^i \Rightarrow b(ab^{i-1})=ab^i \Rightarrow ab=ba$

2.1.25.

(1) $x^2=b,\ x^5=e \Rightarrow b^2x=e \Rightarrow x=b^{-2}$

(2) $xxa=bxc^{-1} \Rightarrow x(xac)=bx \Rightarrow x(acx)=bx \Rightarrow xac=b \Rightarrow x=bc^{-1}a^{-1}$

(3) $(xax)^3=(xax)(xax)(xax)=xa(x^2a)(x^2a)x=bx \Rightarrow xa(xa)^{-1}(xa)^{-1}x=bx \Rightarrow (xa)^{-1}x=bx \Rightarrow (xa)^{-1}=b$

$\Rightarrow xa(xa)^{-1}=xab \Rightarrow e=xab \Rightarrow x=b^{-1}a^{-1}$

2.1.26. (3.1) 연습문제로 보내기.

(풀이) 라그랑주 정리(정리 3.1.10)에 의하여 G의 항등원이 아닌 원소 a에 대하여 $\langle a\rangle$의 위수는 홀수 $2n+1$의 약수이므로 2(즉, $a^2=e$)가 될 수 없다. 그러므로 a는 역원 a^{-1}은 a와 다르다.

따라서 $G=\{e, a_1, \cdots, a_n, a_1^{-1}, \cdots, a_n^{-1}\}$이고 모든 원소의 곱은 $ea_1a_1^{-1}\cdots a_na_n^{-1}=e$이다.

2.1.27. 항등원이 아닌 원소 a 중에서 $a^2=e$인 원소가 없다고 하자. 또한 모든 원소의 역원이 유일하므로 임의의 원소 $a, b\in G-\{e\}$에 대하여 $\{a, a^{-1}\}=\{b, b^{-1}\}$ 이거나 $\{a, a^{-1}\}\cap\{b, b^{-1}\}=\varnothing$이다. 그러면 $a\neq a^{-1}$이므로 $|\{a, a^{-1}\}|=2$이다. 따라서 $|G-\{e\}|$는 짝수가 되어야 한다. 그러므로 $|G|$는 홀수가 되어 모순이다.

따라서 항등원이 아닌 원소 a 중에서 $a^2=e$인 원소가 존재한다.

(별해) $|G|=2n$이므로 $G=\{e, a_1, a_2, \cdots, a_{2n-1}\}$이라 하자. $a(\neq e)\in G$에 대하여 $a\neq a^{-1}$이므로 $|\{a, a^{-1}\}|=2$이다. 이러한 원소 A를 모두 제거하면 짝수개가 줄어들음으로 $G-A=\{e, b_1, b_2, \cdots, b_{2k-1}\}$ $(k\geq 1)$가 되어야 하므로

따라서 항등원이 아닌 원소 $b_i(1\leq i\leq 2k-1)$는 $b_i^2=e$가 되어야 한다.

== 연습문제 (2.2) ==

2.2.1. ⅰ) $\forall ai, bi\in i\mathbb{R},\ ai+bi=(a+b)i\in i\mathbb{R}$

ⅱ) $\exists 0i(=0)\in i\mathbb{R},\ \forall ai\in i\mathbb{R},\ ai+0i=0i+ai=(a+0)i=ai$

ⅲ) $\forall ai\in i\mathbb{R},\ (-a)i\in i\mathbb{R},\ ai+(-a)i=(-a)i+ai=(a+(-a))i=0i=0$

$\therefore$ $i\mathbb{R}$는 덧셈 아래서 복소수의 군 $\mathbb{C}$의 부분군이다.

2.2.2. (1) $S=\{A\in GL(n,\mathbb{R}) : |A|=1$ 또는 $-1\}$라 하자.

$|I_n|=1$이므로 $I_n\in S$이다.

$\forall A, B\in S$, $|A^{-1}|=\frac{1}{|A|}=1\text{or}-1$, $|AB|=|A||B|=1\text{or}-1$이므로 $I_n, A^{-1}, AB\in S$을 만족한다.

$\therefore$ 부분군이다.

(2) $S=\{A\in GL(n,\mathbb{R}) : A^TA=I_n\}$라 하자.

$I_n^TI_n=I_nI_n=I_n,$

$\forall A, B\in S,\ (AB)^T(AB)=B^TA^TAB=B^TB=I_n$

$\forall A\in S,\ A^TA=I_n \Rightarrow AA^T=I_n$이므로

$(A^{-1})^TA^{-1}=(A^T)^{-1}A^{-1}=(AA^T)^{-1}=I_n^{-1}=I_n$

이므로 $I_n, A^{-1}, AB\in S$을 만족한다. $\therefore$ 부분군이다.

2.2.3. (1) 덧셈 항등원 $f(x)=0$이 F'의 원소가 되지 못하므로 거짓이다.

(2) $f(x)=1$인 항등원이 F'의 원소이므로 항등원이 존재한다.
$f(x)=x\in F'$의 역원이 존재하지 않으므로($xg(x)=1$인 $g(x)$가 없음) 군이 아니다.

2.2.4. $(\mathbb{Z},*)$는 항등원은 -1이고 $a^{-1}=-a-2$인 군이다.
$(\mathbb{Z},*)$가 순환군이면 적당한 원소 $a\in\mathbb{Z}$에 대하여 $\mathbb{Z}=\langle a\rangle$이다.

$\forall m\in\mathbb{Z},\ m=a^n=na+(n-1)=(a+1)n-1$인 a와 n를 선택하자.

$\frac{m}{a+1}\in\mathbb{Z}$가 되어야 하므로 $a=0,\ -2$를 선택할 수 있다.

즉, $a=0,\ n=m+1$이라 하면 $m=(m+1)0+((m+1)-1)=0^{m+1}$이 성립하므로
$(\mathbb{Z},*)=\langle 0\rangle$가 되어 순환군이 된다.

또한 $a=-2,\ n=-m-1$이라 하면 $m=(-m-1)(-2)+((-m-1)-1)=(-2)^{-m-1}$이 성립하므로
$(\mathbb{Z},*)=\langle -2\rangle$가 되어 순환군이 된다.

(참고: 군 $(\mathbb{Z},+)$은 항등원이 0이고 생성원이 1인 순환군이다. 이때
$(\mathbb{Z},*)$의 항등원이 -1이므로 생성원이 0인 순환군임을 추측할 수 있다.)

2.2.5. (1) $ea=ae$이므로 $e\in H_a$이다.

ii) $x,\ y\in H_a$라 하자. 그러면 $ya=ay$이므로 $ay^{-1}=y^{-1}a$이다.

$$(xy^{-1})a=x(y^{-1}a)=x(ay^{-1})=x(ay^{-1})=(xa)y^{-1}=(ax)y^{-1}=a(xy^{-1})$$

이므로 $xy^{-1}\in H_a$이다. 따라서 H_a 는 G 의 부분군이다.

(2) $x^2ax=a^{-1}\ \Rightarrow\ a(x^2ax)=aa^{-1}=e\ \Rightarrow\ ax^2a=x^{-1}\ \Rightarrow\ x^2(ax^2a)=(x^2ax)xa=x$

$\Rightarrow\ a^{-1}xa=x\ \Rightarrow\ xa=ax$

$\therefore\ x\in H_a$

(별해) $x^2ax=a^{-1}\ \Rightarrow\ a=(x^2ax)^{-1}=x^{-1}a^{-1}x^{-2}=x^{-1}(x^2ax)x^{-2}=xax^{-1}\ \Rightarrow\ ax=xa$

$\therefore\ x\in H_a$

2.2.6. i) $\forall g\in G,\ g^2e=g^2=eg^2\qquad\therefore\ e\in H$

ii) $\forall x,y\in H,\ g^2x=xg^2,\ g^2y=yg^2$이므로

$$g^2(xy)=(g^2x)y=(xg^2)y=x(g^2y)=x(yg^2)=(xy)g^2\quad\therefore\ xy\in H$$

iii) $y^{-1}g^2yy^{-1}=y^{-1}yg^2y^{-1}\ \Rightarrow\ y^{-1}g^2=g^2y^{-1}\quad\therefore\ y^{-1}\in H$

$\therefore\ H<G$

2.2.7. (1) $\begin{pmatrix}1&0\\0&1\end{pmatrix}\in H$

$$\forall\begin{pmatrix}a&b\\0&d\end{pmatrix}\in H,\quad\begin{pmatrix}a&b\\0&d\end{pmatrix}^{-1}=\frac{1}{ad}\begin{pmatrix}d&-b\\0&a\end{pmatrix}\in H\quad(ad\neq 0)$$

$$\forall\begin{pmatrix}a&b\\0&d\end{pmatrix},\begin{pmatrix}a'&b'\\0&d'\end{pmatrix}\in H,\quad\begin{pmatrix}a&b\\0&d\end{pmatrix}\begin{pmatrix}a'&b'\\0&d'\end{pmatrix}=\begin{pmatrix}aa'&ab'+bd'\\0&dd'\end{pmatrix}\in H\ ((aa')(dd')=ada'd'\neq 0)$$

$\therefore\ G$의 부분군이다.

하지만 $\begin{pmatrix}a'&b'\\0&d'\end{pmatrix}\begin{pmatrix}a&b\\0&d\end{pmatrix}=\begin{pmatrix}a'a&a'b+b'd\\0&d'd\end{pmatrix}\neq\begin{pmatrix}aa'&ab'+bd'\\0&dd'\end{pmatrix}=\begin{pmatrix}a&b\\0&d\end{pmatrix}\begin{pmatrix}a'&b'\\0&d'\end{pmatrix}$

$ab'+bd'\neq a'b+b'd$ 이므로 가환이 아니다.

(2) 임의의 원소 $h\in H$에 대하여 H가 부분군이므로 $hH\subset H$이고 $Hh\subset H$이다.

그리고 모든 원소 $g\in H$에 대하여 $g=hh^{-1}g\in hH,\ g=gh^{-1}h\in Hh \Rightarrow H\subset hH$이고 $H\subset Hh$이다.
따라서 $hH=H=Hh$이므로 $H\subset A$이다.

한편 임의의 $\begin{pmatrix}a\ b\\ c\ d\end{pmatrix}\in A$에 대하여 $\begin{pmatrix}a\ b\\ c\ d\end{pmatrix}H=H\begin{pmatrix}a\ b\\ c\ d\end{pmatrix}$이다. 그러면

$$\begin{pmatrix}a\ b\\ c\ d\end{pmatrix}\begin{pmatrix}1\ 1\\ 0\ 1\end{pmatrix}\in\begin{pmatrix}a\ b\\ c\ d\end{pmatrix}H=H\begin{pmatrix}a\ b\\ c\ d\end{pmatrix}$$

이므로 적당한 $\begin{pmatrix}a'\ b'\\ 0\ d'\end{pmatrix}\in H$에 대하여

$$\begin{pmatrix}a\ b\\ c\ d\end{pmatrix}\begin{pmatrix}1\ 1\\ 0\ 1\end{pmatrix}=\begin{pmatrix}a'\ b'\\ 0\ d'\end{pmatrix}\begin{pmatrix}a\ b\\ c\ d\end{pmatrix}$$

이므로 $\begin{cases}a=aa'+b'c\\ a+b=a'b+b'd\\ c=cd'\\ c+d=dd'\end{cases}$이다. 여기서 $c=0$이어야 한다. 따라서 $\begin{pmatrix}a\ b\\ c\ d\end{pmatrix}=\begin{pmatrix}a\ b\\ 0\ d\end{pmatrix}\in H$이므로 $A\subset H$이다.
그러므로 $A=H$가 되어 G의 부분군이다.

2.2.8. ($\Rightarrow$) $m\mathbb{Z}\subset n\mathbb{Z}$이라 하자. 그러면

$$m=m\cdot 1\in m\mathbb{Z}\subset n\mathbb{Z}$$

이므로 적당한 정수 $a\in\mathbb{Z}$가 존재하여 $m=na$이다. 따라서 $n|m$ 이다.
($\Leftarrow$) $n|m$ 이라 하자. 그러면 적당한 정수 $a\in\mathbb{Z}$가 존재하여 $m=na$이다. 따라서 임의의 원소 $mb\in m\mathbb{Z}$에 대하여

$$mb=nab\in n\mathbb{Z}$$

이므로 $m\mathbb{Z}\subset n\mathbb{Z}$이다.
$\therefore$ $m\mathbb{Z}\subset n\mathbb{Z}$일 동치조건은 n이 m의 약수이면 된다.

2.2.9. $\{e\}$와 G는 G의 부분군이다. 그러면 부분군이 2개 밖에 존재하지 않으므로 원소 $a(\neq e)\in G$가 생성원인 순환군 $\langle a\rangle$은 G가 되어야 한다. 즉, $|\langle a\rangle|=|G|=p$이다. 이때 p가 합성수이면 자연수 $d, d'(1<d, d'<p), p=dd'$이 존재한다. 그러면 다음과 같은 3개의 부분군이 존재한다.

$$\{e\}<\langle a^d\rangle=\{e, a^d, \cdots, a^{d(d'-1)}\}<\langle a\rangle$$

이것은 부분군이 2개에 모순이다. 그러므로 p는 소수이다.

2.2.10.

$\forall\, mx+ny\in m\mathbb{Z}+m\mathbb{Z},\ \exists\, m0+n0\in m\mathbb{Z}+n\mathbb{Z}\ \ s.t.\ (mx+ny)+(m0+n0)=m(x+0)+n(y+0)=mx+ny$
$\therefore$ 항등원 존재
$\forall\, mx+ny, mx'+ny'\in m\mathbb{Z}+m\mathbb{Z},\ (mx+ny)+(m(-x')+n(-y))='m(x+(-x'))+n(y+(-y'))\in m\mathbb{Z}+n\mathbb{Z}$
$\therefore$ $m\mathbb{Z}+m\mathbb{Z}$는 $\mathbb{Z}$의 부분군

2.2.11. $e\in G,\ e\cdot e=e,\ e=ee\in HK$
$\forall\ hk, h'k'\in HK,\ hk(h'k')^{-1}=hkk'^{-1}h'^{-1}=(hh'^{-1})(kk'^{-1})\in HK$
이므로 $HK<G$

2.2.12. (2.3절 2.3.5 참조)
(1) 순환군 $G=\langle a\rangle=\{e, a^1, \cdots, a^8\}$의 모든 부분군은 순환군이다(정리 2.3.5). 부분군을 $\langle a^b\rangle(b=0, 1, \cdots, 8)$라 하자. $a^b\in\langle a\rangle$에 대하여 $\gcd(9,b)=1$ 또는 3이다.
$\gcd(9,b)=1$인 경우. 그러면 적당한 정수 $x, y\in\mathbb{Z}$에 대하여 $9x+by=1$이다. $\langle a^b\rangle\subset\langle a\rangle$은 분명히 성립한다.
임의의 원소 $a^c\in\langle a\rangle$에 대하여

$$a^c = a^{9xc+byc} = (a^9)^{xc}(a^b)^{yc} = e^{xc}(a^b)^{yc} = (a^b)^{yc} \in \langle a^b \rangle$$

이므로 $\langle a^b \rangle = \langle a \rangle = G$이다. 따라서 a^b는 G의 생성원이다.

$\gcd(9,b) = 3$인 경우에는 $b = 3b'$이므로

$$\langle a^b \rangle = \langle a^{3b'} \rangle = \{e, a^{3b'}, a^{6b'}, a^{9b'}(=e)\} \leqq \langle a \rangle$$

이 되어 생성원이 될 수 없다. 그러므로 G의 서로 다른 생성원의 수는 지수가 9와 서로소일 때 생성원이 된다. 생성원은 $a, a^2, a^4, a^5, a^7, a^8$로 6개이다.

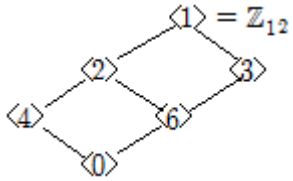
(2) 항등원이 아닌 원소의 지수 2개가 모두 9와 서로소가 아니고 2개가 서로소인 쌍이 기약생성원이 된다. 하지만

$\langle a^3, a^6 \rangle = \langle a^3 \rangle$이므로 2개로 된 기약 생성원은 존재하지 않는다.

2.2.13. (1) $\mathbb{Z}_{12} = \{0, 1, \cdots, 10, 11\}$의 부분군은 모두 순환부분군이므로 모든 부분군은 다음과 같다.

$\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \mathbb{Z}_{12}$, $\langle 2 \rangle = \langle 10 \rangle = \{0, 2, 4, 6, 8, 10\}$, $\langle 3 \rangle = \langle 9 \rangle = \{0, 3, 6, 9\}$,

$\langle 4 \rangle = \langle 8 \rangle = \{0, 4, 8\}$, $\langle 6 \rangle = \{0, 6\}$이고 포함관계는 아래와 같이 생성원이 배수(약수)관계가 있으면 포함관계가 성립한다. 예를 들면, $<0> \subset <6> \subset <3> \subset <1>$, $<0> \subset <6> \subset <2> \subset <1>$이 성립한다.



(2) 항등원이 아닌 원소 2개가 모두 12와 서로소가 아니고 2개가 서로소인 쌍이 기약생성원이 된다(문제 12번). 그러므로 2, 3, 4, 6, 8, 9, 10에서 쌍마다 서로소인 (2, 3), (2, 9), (3, 4), (3,8), (4, 9), (8, 9), (9, 10)인 7개의 쌍이 기약생성원이 된다.

2.2.14. $H < G$, $e \in H$이므로 $e = e^{-1} \in H^{-1}$이다.

$\forall a, b \in H$, $b^{-1}a \in H$이다. 그러면 $\forall a^{-1}, b^{-1} \in H^{-1}$, $a^{-1}(b^{-1})^{-1} = (b^{-1}a)^{-1} \in H^{-1}$이다.

그러므로 부분군 판정조건에 의해 $H^{-1} < G$이다.

2.2.15. (1) 곱셈군 $(\mathbb{R}^*, \cdot)$에서 $H = \mathbb{N}$, $G = \mathbb{R}^*$ (2) 덧셈군 $(\mathbb{Z}, +)$에서 $H = \{1, -1\}$, $G = \mathbb{Z}$

== 연습문제 (2.3) ==

2.3.1 (1) $\gcd(30,25) = 5$이므로 정리 2.3.4에 의하여 $|25| = \dfrac{30}{\gcd(30,25)} = 6$개

(2) $e^{\frac{2\pi i}{8}} = \dfrac{1+i}{\sqrt{2}}$이므로 U_8의 원소수인 8개(예 2.1.5(4) 참조)

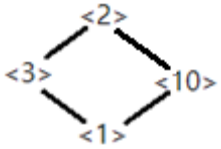
2.3.2 정리 2.3.4를 이용하자.

$\mathbb{Z}_{11}^*$에서 $\langle 2 \rangle = \{2,4,8,5,10,9,7,3,6,1\}$이므로 $\mathbb{Z}_{11}^* = \langle 2 \rangle$이다. $|2| = 10$이다.

$$|1|=|2^0|=\frac{10}{\gcd(0,10)}=1,\ |2|=|2^1|=\frac{10}{\gcd(1,10)}=10,\ |4|=|2^2|=\frac{10}{\gcd(2,10)}=5,$$
$$|8|=|2^3|=\frac{10}{\gcd(3,10)}=10,\ |5|=|2^4|=\frac{10}{\gcd(4,10)}=5,\ |10|=|2^5|=\frac{10}{\gcd(5,10)}=2,$$
$$|9|=|2^6|=\frac{10}{\gcd(6,10)}=5,\ |7|=|2^7|=\frac{10}{\gcd(7,10)}=10,\ |3|=|2^8|=\frac{10}{\gcd(8,10)}=5,$$
$$|6|=|2^9|=\frac{10}{\gcd(9,10)}=10$$

Hasse 다이어그램 정리 2.3.11을 이용하자. 위수가 같으면 같은 부분군이므로 다음과 같은 4개의 부분군이 존재한다.

위수 10인 부분군 : $\mathbb{Z}_{11}^* = \langle 2\rangle = \langle 6\rangle = \langle 7\rangle = \langle 8\rangle$
위수 5인 부분군 : $\langle 3\rangle = \langle 4\rangle = \langle 5\rangle = \langle 9\rangle = \{1, 3, 9, 5, 4\}$
위수 2인 부분군 : $\langle 10\rangle = \{1, 10\}$
위수 1인 부분군 : $\langle 1\rangle = \{1\}$



2.3.3 (1) 따름정리 2.3.12에 의하여 24와 서로소인 원소이므로 생성원은 1, 5, 7, 11, 13, 17, 19, 23이다.

(2) 정리 2.3.4에 의하여 $6=\frac{24}{\gcd(a,24)}$이므로 $\gcd(a,24)=4$인 4와 20인 2개이다.. 따라서 위수가 6인 원소는 2개이다.

2.3.4

(1) $|a|=12$이므로 $a^{12}=e$이다. 이 때 $\mathrm{lcm}(8,12)=24$이므로 $8k=24$가 되는 k가 최소 양의 정수이다. 따라서 $k=3$이다.

(2) $|a^n|=\frac{12}{\gcd(n,12)}=12$이므로 $\gcd(n,12)=1$인 양의 정수 n이 $|a^n|=12$가 되는 모든 n이다. 따라서 $n=1,5,7,11$이다.

2.3.5 pq와 서로소인 원소수는 오일러함수이므로 $\phi(pq)=(p-1)(q-1)$개

2.3.6 라그랑주 정리(정리 3.1.10)에 의해 위수가 6인 군(= H)의 진부분군의 위수는 1,2,3 뿐이다.
위수가 1이면 당연히 순환부분군이다. 위수가 2 또는 3이면 3.1.10에 의하여 2와 3은 소수이므로 순환부분군이다.

2.3.7 (연습문제 2.2.9와 같은 문제)

2.3.8

$\mathbb{Z}_p$는 위수 p인 순환군이므로 $\mathbb{Z}_p=\langle a\rangle$ H가 $\mathbb{Z}_p$의 비자명 부분군이면 $a^b(\neq e)\in H$에 대하여 p가 소수이므로 $|a^b|=\frac{p}{\gcd(b,p)}=p$이다. 따라서 $\mathbb{Z}_p=\langle a^b\rangle\subset H\subset\mathbb{Z}_p \Rightarrow H=\mathbb{Z}_p$가 되어 부분군은 $\{e\}$과 $\mathbb{Z}_p$뿐이다.
따라서 p가 소수이면 $\mathbb{Z}_p$는 비자명 진부분군을 갖지 않는다.

2.3.9. (1) $A^2=\begin{pmatrix}0&-1\\1&0\end{pmatrix}^2=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\Rightarrow A^4=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\quad B^3=\begin{pmatrix}0&1\\-1&1\end{pmatrix}^3=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\Rightarrow B^6=\begin{pmatrix}1&0\\0&1\end{pmatrix}$이지만

$$AB=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\-1&1\end{pmatrix}=\begin{pmatrix}1&-1\\0&1\end{pmatrix}\Rightarrow (AB)^n=\begin{pmatrix}1&-n\\0&1\end{pmatrix}\neq\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

(2) $C^2=\begin{pmatrix}0&1\\1&0\end{pmatrix}^2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $D^3=\begin{pmatrix}0&-1\\1&-1\end{pmatrix}^3=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $B^3=\begin{pmatrix}0&1\\-1&1\end{pmatrix}^3=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\Rightarrow B^6=\begin{pmatrix}1&0\\0&1\end{pmatrix}$이지만

$$CD=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&-1\\1&-1\end{pmatrix}=\begin{pmatrix}1&-1\\0&-1\end{pmatrix}\Rightarrow (CD)^2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

2.3.10. $|ab|=n$이므로

$$e=(ab)^n=\underbrace{(ab)\cdots(ab)}_{n개}\Rightarrow a^{-1}b^{-1}=\underbrace{(ba)\cdots(ba)}_{n-1개}\Rightarrow e=\underbrace{(ba)\cdots(ba)}_{n-1개}(ba)=(ba)^n$$

이다. 따라서 ba의 위수는 유한이고 $|ba|=m$이라면 $m\leqq n$이다. 같은 방법으로 $n\leqq m$을 증명할 수 있다.
따라서 $|ba|=m=n$이다.

2.3.11.

(1) 곱셈에 대한 교환법칙이 성립하므로 $(ab)^{nm}=a^{nm}b^{nm}=(a^n)^m(b^m)^n=e^me^n=e$이다.

이제 $|ab|=t$라 하자. 그러면 $(ab)^t=e$이므로 $t|nm$이다.

$e=e^{nt}=(ab)^{nt}=a^{nt}b^{nt}=b^{nt}$이므로 $m|nt\Rightarrow m|t$이다.

$e=e^{mt}=(ab)^{mt}=a^{mt}b^{mt}=a^{mt}$이므로 $n|mt\Rightarrow n|t$이다.

$m|t\wedge n|t$이고 $\gcd(n,m)=1$이므로 $\mathrm{lcm}(n,m)|t\Rightarrow nm|t$이다.

따라서 $nm=t$이므로 $|ab|=|a||b|=nm$이다. 그러므로 위수가 nm인 G의 순환부분군 $\langle ab\rangle$가 존재한다.

(2) $\gcd(n,m)=d$이고 $\mathrm{lcm}(n,m)=s$이라 하자. 이 때 $n=dn'$, $m=dm'$이라 하자. 그러면 $\gcd(n',m')=1$이므로 d를 다시 분해하여

$$d=d_1d_2,\ \gcd(d_1,d_2)=1\ \Rightarrow\ \gcd(d_1n',d_2m')=1$$

을 만족하도록 인수분해하자. 그러면

$$s=\frac{nm}{d}=\frac{dn'dm'}{d}=dn'm'=d_1d_2n'm'=(d_1n')(d_2m')$$

이다. 또한 $|a^{d_2}|=\dfrac{d_1d_2n'}{d_2}=d_1n'$, $|b^{d_1}|=\dfrac{d_1d_2m'}{d_1}=d_2m'$(정리 2.3.4)이다. 그러면 (1)에 의하여

$$|a^{d_2}b^{d_1}|=d_1n'd_2m'=dn'm'=s=\mathrm{lcm}(n,m)$$

이다. 따라서 위수가 $\mathrm{lcm}(n,m)$인 G의 순환부분군이 존재한다.

2.3.12. (1) $d\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}\Leftrightarrow \gcd(a,b)=d$임을 보이자.

$a,b\in a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$이므로 $a=da'$, $b=db'$인 정수 a', b'이 존재한다. 그러므로 $d|a$이고 $d|b$ 이다.

(2) $d\in d\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$이므로 $d=ax+by$인 정수 x,y가 존재한다. 그러므로 $d'|a$이고 $d'|b$이면 적당한 정수 a', b'가 존재하여 $a=d'a'$, $b=d'b'$이다. 따라서

$$d=ax+by=d'a'x+d'b'y=d'(a'x+b'y)$$

이므로 $d'|d$이다.

2.3.13.

(1) 순환군 $G=<a>$의 부분군 $<a^n>$, $<a^m>$ $m,n\in\mathbb{N}$에 대하여

n,m의 최소공배수 $s=\mathrm{lcm}(m,n)$는 $<a^m>\cap<a^n>$ $=<a^s>$라 정의한다.

(2) $\mathrm{lcm}(m,n)=\dfrac{nm}{\gcd(m,n)}$이므로 $\gcd(n,m)=1$일 때 $\mathrm{lcm}(m,n)=mn$이 되므로

$n.m$은 서로소일 때 성립한다.

(3) $d=\gcd(n,m)$라 하자. 그러면 $n=dn'$, $m=dm'(\gcd(n',m')=1)$이다.

$$\mathrm{lcm}(n,m)=\mathrm{lcm}(dn',dm')=d\,\mathrm{lcm}(n',m')=dn'm'$$
$$\Rightarrow d\cdot\mathrm{lcm}(n,m)=ddn'm'=nm$$
$$\therefore \gcd(n,m)\cdot\mathrm{lcm}(n,m)=mn$$

2.3.14. (1) $H < G$이므로 $h \in H, h' \in H$이고, $hh'^{-1} \in H$이다. 분명히 $e = geg^{-1} \in gHg^{-1}$이다.
$ghg^{-1}, gh'g^{-1} \in gHg^{-1}$에 대하여

$$ghg^{-1} \cdot (gh'g^{-1})^{-1} = ghh^{-1}g^{-1} \in gHg^{-1}$$이다.

$\therefore gHg^{-1} < G$

(2) $H, gHg^{-1} < K$에서 $|H| = |gHg^{-1}| \Leftrightarrow H = gHg^{-1}$(정리 2.3.11(2))임을 보이자.
함수 $f : H \to gHg^{-1}, f(h) = gh'g^{-1}$을 생각하자. 전사임은 분명하다.

$$f(h) = f(h') \Rightarrow ghg^{-1} = gh'g^{-1} \Rightarrow g^{-1}(ghg^{-1})g = g^{-1}(gh'g^{-1})g \Rightarrow h = h'$$

이므로 f는 단사함수 이다. 따라서 f가 전단사함수가 되어 $|H| = |gHg^{-1}|$이다. K는 유한순환부분군이므로 정리 2.3.11(2)에 의하여 $H = gHg^{-1}$이다.

2.3.15.

$b^2 = \mathrm{ab}a^{-1}$, $b^4 = ab^2a^{-1} = a(aba^{-1})a^{-1} = a^2ba^{-2}$
$b^8 = ab^4a^{-1} = a(a^2ba^{-2})a^{-1} = a^3ba^{-3}$,
$b^{16} = ab^8a^{-1} = a(a^3ba^{-3})a^{-1} = a^4ba^{-4}$,
$b^{32} = ab^{16}a^{-1} = a(a^4ba^{-4})a^{-1} = a^5ba^{-5} = b$,
이므로

$b^{32} = \mathrm{b}$
$\Rightarrow b^{32} \cdot b^{-1} = b \cdot b^{-1}$ ($\because b \in G$, G는 군)
$\Rightarrow b^{31} = \mathrm{e}$
b의 위수가 t라면 정리 2.3.3에 의하여 $t|31$이다. 31은 소수이므로 $t = 1, 31$이어야 하는데 b는 항등원이 아니므로 $|b| = 31$이다.

2.3.16.
$G = \langle a \rangle$라 하자.
$\langle a \rangle = \langle a^{-1} \rangle$이고, 가정에서 단 하나의 생성원을 가지므로 $a = a^{-1}$이다. 즉, $a^2 = aa = aa^{-1} = e$이다.
그러면 $a^{2n+1} = (a^2)^n a = a$, $a^{2n} = (a^2)^n = e\ (n \geq 0)$이므로 $G = \{a, e\}$이다.

2.3.17. (1) $a, b \in H$에 대해 $|a| \leqq 2$, $|b| \leqq 2$이다.
$e^1 = e$이므로 $|e| = 1$이다. 따라서 $e \in H$이다.
$(ab^{-1})^2 = a^2(b^{-1})^2 = e(b^2)^{-1} = e$이므로 $|ab^{-1}| \leq 2$이다. 따라서 $ab^{-1} \in H$이이다.
따라서 $H < G$이다.

(2) $i = 0$일 때 $|e| = 1 = p^0$이므로 $e \in H$이다.
$x, y \in H$이면 적당한 음이 아닌 정수 n, m에 대하여 $|x| = p^m, |y| = p^n$이다.
$|xy^{-1}| \mid \mathrm{lcm}(|x|, |y^{-1}|) = \mathrm{lcm}(|x|, |y|) = p^{\mathrm{lcm}(m,n)}$(정리 2.3.16)이고 p가 소수이므로 $xy^{-1} \in H$이다.
따라서 $H < G$이다.

2.3.18. $H = \{g \in G : |g| < \infty\}$라 하자.
항등원e의 위수는 1이므로 유한위수를 갖는다. $e \in H$이다.
$g \in H$라 하면 적당한 자연수 n이 존재하여 $|g| = n$이므로, $g^n = e$이다.

$(g^{-1})^n = (g^n)^{-1} = e$

이므로 $g^{-1} \in H$이다.

$\forall g, h \in H$라 하면 적당한 자연수 n, m이 존재하여 $|g| = n$, $|h| = m$이므로 $g^n = e$, $h^m = e$이다.

$(gh)^{nm} = (g^{nm})(h^{nm}) = (g^n)^m (h^m)^n = e^m e^n = e$ (G는 가환군)

이므로 $(gh)^{nm} = e$이다. 따라서 gh의 위수는 유한위수이다.

$gh \in H$가 되어 $H < G$이다.

2.3.19. 위수 n인 유한순환군 G에서 m이 n의 양의 약수일 때, 방정식 $x^m = e$는 G 내에서 정확히 m개의 해가 존재함을 보여라.

(풀이) $G = \langle a \rangle$라 하자. $|a| = n$이고 $m|n$이다. 그러면 자연수 m'이 존재하여 $n = mm'$이다.

이때 G의 부분군 $\langle a^{m'} \rangle$은 위수는 $|a^{m'}| = \dfrac{n}{\gcd(m', n)} = m$이므로 위수 m인 부분군이 반드시 존재하고 유일하다(정리 2.3.10). 그리고 위수 m인 부분군의 서로 다른 m개의 원소는 방정식 $x^m = e$의 해가 된다.

한편 $a^y \in \langle a \rangle - \langle a^{m'} \rangle$가 $x^m = e$의 해라고 하면 정리 2.3.3에 의하여

$(a^y)^m = e \Rightarrow a^{my} = e \Rightarrow n|my \Rightarrow my = nt = mm't (\exists t \in \mathbb{N}) \Rightarrow y = m't$

이다. 그러면 $a^y = a^{m't} \in \langle a^{m'} \rangle$가 되어 모순이다. 따라서 $x^m = e$의 해는 꼭 m개를 가진다.

== 연습문제 (2.4) ==

2.4.1. $\sigma = (1\,3\,4\,5\,6\,2)$, $\tau = (1\,2\,4\,3)(5\,6)$, $\mu = (1\,5)(3\,4)$이므로 $\sigma^6 = (1)$, $\tau^4 = (1)$, $\mu^2 = (1)$이다.

(1) $\sigma^{-1}\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}$

(2) $\sigma^{100} = \sigma^{6 \cdot 16}\sigma^4 = (1)^{16}\sigma^{-2} = \sigma^{-2} = (1\,6\,4)(2\,5\,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 3 & 3 & 4 \end{pmatrix}$

(3) $\tau^{100} = \tau^{4 \cdot 25} = (1)$

(4) $\mu^{100} = \mu^{2 \cdot 50} = (1)$

2.4.2. 다음 물음에 답하라.

(1) $\sigma \in S_6$과 원소 $a, b \in A = \{1, 2, 3, 4, 5, 6\}$에 대하여 $a \sim b$일 필요충분조건을 적당한 $n \in \mathbb{Z}$에 대하여 $b = \sigma^n(a)$라 할 때 관계 $\sim$은 A 위에서 동치 관계임을 보여라.

(2) 연습문제 1번의 치환 σ, τ, μ 에 의한 동치관계에서 각 각의 상집합 을 구하라.

(풀이)

(1) 임의의 원소 $a \in A$에 대하여 $a = \sigma^0(a)$이므로 $a \sim a$

$a \sim b$라 하자. 그러면 적당한 정수가 존재하여 $b = \sigma^n(a)$이다. 그러면 $a = \sigma^{-n}(b)$이므로 $b \sim a$이다.

$a \sim b$, $b \sim c$라 하자. 그러면 적당한 정수 n, m에 존재하여 $b = \sigma^n(a)$, $c = \sigma^m(b) \Rightarrow c = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(a)$이므로 $a \sim c$이다. 따라서 $\sim$은 A 위에서 동치관계이다.

(2) $S_6/\sigma = \{\{1, 2, 3, 4, 5, 6\}\}$, $S_6/\tau = \{\{1, 2, 3, 4\}, \{5, 6\}\}$, $S_6/\mu = \{\{1, 5\}, \{3, 4\}\}$

2.4.3. 서로소인 순환치환 $(1\,8)(3\,6\,4)(5\,7)$. 호환의 곱 $(1\,8)(3\,4)(3\,6)(5\,7)$

2.4.4. (1) $\sigma^{-1} = (2\,1\,3)$, $\sigma^2 = (1\,3\,2)$, $\sigma^3 = (1)$, $\sigma^5 = \sigma^3\sigma^2 = (1\,3\,2)$

(2) $a^{-1} = (1\,4\,3\,2)$, $a^2 = (1\,2\,3\,4)(1\,2\,3\,4) = (1\,3)(2\,4)$

$a^{-1} = a^3$이므로 $a^3 = (1\,4\,3\,2)$이다.

$a^5 = a$이므로 $a^5 = (1\ 2\ 3\ 4)$이다.

(3) $a^{-1} = (1\ 6\ 5\ 4\ 3\ 2)$이다. $a^{-1} = a^5$이므로 $a^5 = (1\ 6\ 5\ 4\ 3\ 2)$이다.
$a^2 = (1\ 3\ 5)(2\ 4\ 6)$
$a^3 = (1\ 4)(2\ 5)(3\ 6)$이다.

2.4.5. (1) $\theta = (1\ 3\ 8)(2\ 7)(4\ 9\ 6\ 5)$이고 $|\theta| = \mathrm{lcm}(3,2,4) = 12$이다.
$|\theta^{100}| = |(\theta^{12})^8 \bullet \theta^4| = |\theta^4|$이고 $\theta^4 = (1\ 3\ 8)$이므로 $|\theta^4| = 3$이다.
(2) $\theta^{2008}(9) = \theta^4(9)$이므로 $\theta^4(9) = 9$이다.
(3) $\sigma^{-2017} = (\sigma^{2017})^{-1} = \sigma^{-1} = (1\ 8\ 3)(2\ 7)(4\ 5\ 6\ 9)$

2.4.6. (1) $|\sigma| = 4$, $\sigma^{2007} = \sigma^3 = (1752)$
(2) $|\sigma| = 6$, $\sigma^{2007} = \sigma^{6 \cdot 334 + 3} = \sigma^3 = (15)$

2.4.7. $|\sigma| = |(1\ 2)(4\ 7\ 8)(2\ 1)(7\ 2\ 8\ 1\ 5)| = |(1\ 5\ 8)(2\ 1)(2\ 4\ 7)| = \mathrm{lcm}(3,2,3) = 6$

2.4.8. (1) 3을 고정하고 나머지 3개의 원소가 1대1 대응하므로 원소수는 $|S_3| = 6$과 같다.
(2) (1)과 같이 2가 5로 고정하고 나머지 4개(정의역은 $\{1, 3, 4, 5\}$, 공역은 $\{1, 2, 3, 4\}$)의 원소가 1대1 대응하므로 원소수는 $|S_4| = 24$와 같다.

2.4.9. (1) $H = \{\sigma \in S_A | \sigma(b) = b\}$라 하자. 항등사상 $\sigma^0 \in S_A$에 대하여 $\sigma^0(b) = b$이므로 $\sigma^0 \in H$이다.
$\sigma, \delta \in H$에 대하여 $\sigma(b) = b, \delta(b) = b$이므로 $\sigma(\delta(b)) = \sigma(b) = b$이다. 따라서 $\sigma\delta \in H$이다.
또한 $\sigma^{-1}(b) = b$이므로 $\sigma^{-1} \in H$이다. 그러므로 $H < S_A$이다.

(2) (1) $H = \{\sigma \in S_A \mid \sigma(B) \subset B\}$라 하자. 항등사상 $\sigma^0 \in S_A$에 대하여 $\sigma^0(B) = B \subset B$이므로 $\sigma^0 \in H$이다.
$\sigma, \delta \in H$에 대하여 $\sigma(B) \subset B, \delta(B) \subset B$이므로 $\sigma(\delta(B)) \subset \sigma(B) \subset B$이다. 따라서 $\sigma\delta \in H$이다.
하지만 $\sigma^{-1}(B) \subset B$은 A가 무한집합이면 거짓이므로 $H \not< S_A$이다.
(반례) $A = \mathbb{Z}$, $B = \mathbb{N}$, $\sigma(n) = n + 1 \Rightarrow \sigma^{-1}(B) = \mathbb{N} \cup \{0\} \not\subset \mathbb{N} = B$.

2.4.10. 회전이동 변환을 한 원소에서는 한 꼭짓점을 기준으로 다른 꼭짓점까지 원점을 중심으로 $\frac{2\pi}{n}$만큼씩 회전시킨 형태(위수 n인 순환군이 됨)이다.
선대칭변환에 관한 원소는

n이 짝수이면 꼭짓점−꼭짓점($\frac{n}{2}$개)/변의 중점−변의 중점($\frac{n}{2}$개),

n이 홀수이면 꼭짓점−변의 중점(n개)

을 기준으로 도형이 절반으로 나눠지도록 대칭축에 의해 대칭 시킨 형태이다. 이 원소의 위수는 2이다.

2.4.11. 모든 S_n에는 $(1,2)(1,3)$이 포함되어 있으므로
$(1,2)(1,3) \neq (1,3)(1,2)$이므로 S_n은 가환군이 아니다.

2.4.12. $\lambda_a(g_1) = \lambda_a(g_2) \Rightarrow ag_1 = ag_2 \Rightarrow g_1 = g_2$ $\therefore \lambda$는 단사
$\forall g \in G$, $a^{-1}g \in G$가 존재,
$g = a(a^{-1}g) = \lambda_a(a^{-1}g)$ $\therefore \lambda$는 전사

$\therefore \lambda$는 전단사 함수이므로 G는 치환이다.

2.4.13. $\forall \lambda_a \in H,\ g \in G,\quad \lambda_e(\lambda_a(g)) = \lambda_e(ag) = eag = ag = \lambda_a(g)$
λ_e(항등원)$\in H$.

$\forall g \in G,\ \lambda_a, \lambda_b \in H$

$\lambda_a\lambda_b(g) = \lambda_a(bg) = a(bg) = (ab)g = \lambda_{ab}(g)$
$\therefore \lambda_a\lambda_b = \lambda_{ab} \in H$

$\lambda_a\lambda_{a^{-1}}(g) = \lambda_a(a^{-1}g) = a(a^{-1}g) = g = \lambda_e(g)$
$\lambda_{a^{-1}}\lambda_a(g) = \lambda_{a^{-1}}(ag) = a^{-1}(ag) = g = \lambda_e(g)$
$\Rightarrow\ \lambda_a\lambda_{a^{-1}} = \lambda_{a^{-1}}\lambda_a = \lambda_e$
$\Rightarrow\ (\lambda_a)^{-1} = \lambda_{a^{-1}} \in H$

$\therefore$ 부분군판정조건에 의하여 H는 S_G의 부분군이다.

2.4.14. (1) $\sigma = (a_1\, a_2\, \cdots\, a_n)$이라 하자.

($\Rightarrow$) n이 홀수라 하자. 그러면 $\sigma^2 = (a_1\, a_3\, \cdots\, a_n\, a_2\, \cdots\, a_{n-1})$ ($\therefore n$은 홀수)

$\therefore \sigma^2$은 순환치환

($\Leftarrow$) n이 짝수라고 하자. 이때, $\sigma^2 = (a_1, a_3, \cdots, a_{2n-1})(a_2, a_4, \cdots, a_{2n})$이 되어 순환치환이 아니다.

가정에 모순이므로 n은 홀수이다.

(2) s가 n의 배수일 때 $|\sigma^s| = \dfrac{n}{\gcd(s,n)} = 1$이므로 $\sigma^s = (1)$은 순환치환이다.

s가 n의 배수가 아닐 때, $|\sigma^s| = \dfrac{n}{\gcd(s,n)} = n$이다. $a_1, a_2, \cdots, a_n$으로 이루어진 길이(위수) n인 치환은 n이 소수이므로 순환치환뿐이다. 따라서 σ^s는 순환치환이다.

(별해) σ는 길이가 n인 순환치환이므로 $|\sigma| = n$이다. 그러면 $|\langle\sigma\rangle| = n$이다.
$\langle\sigma^s\rangle < \langle\sigma\rangle$이므로 $|\langle\sigma^s\rangle|$은 n의 약수이다. n은 소수이므로 $|\langle\sigma^s\rangle| = 1$ or n이다

$|\langle\sigma^s\rangle| = 1$인 경우에는 $\sigma^s = (1)$이므로 길이가 1인 순환치환이다.

$|\langle\sigma^s\rangle| = n$인 경우에는 σ^s을 서로소인 순환치환의 곱 $\sigma^s = \sigma_1\sigma_2\cdots\sigma_k$으로 나타낼 수 있다(정리 2.4.12). 그러면

$$n = |\sigma^s| = |\sigma_1\sigma_2\cdots\sigma_k| = |\sigma_1||\sigma_2|\cdots|\sigma_k|$$

이다. 이때 n이 소수이므로 $|\sigma_1| = n$, $|\sigma_2| = 1$, $\cdots$, $|\sigma_k| = 1$이어야 한다. 따라서 $\sigma^s = \sigma_1$이 되어 길이가 n인 순환치환이다.

2.4.15. σ를 서로소인 순환치환의 곱 $\sigma^s = \sigma_1\sigma_2\cdots\sigma_k$으로 나타낼 수 있다(정리 2.4.12). 그러면

$$p = |\sigma| = |\sigma_1\sigma_2\cdots\sigma_k| = |\sigma_1||\sigma_2|\cdots|\sigma_k|$$

이다. 이때 p가 소수이므로 $|\sigma_1| = p$, $|\sigma_2| = 1$, $\cdots$, $|\sigma_k| = 1$이어야 한다. 따라서 $\sigma = \sigma_1$이 되어 길이가 p인 순환치환이다.

2.4.16. $r = 0$인 경우 $(123\cdots n)^0(12)(123\cdots n)^{n-0} = (12)$이다.
$r = 1$인 경우 $(123\cdots n)^1(12)(123\cdots n)^{n-1} = (23)$이다.
$r = 2$인 경우 $(123\cdots n)^2(12)(123\cdots n)^{n-2} = (34)$이다.
…
$r = n-2$인 경우 $(123\cdots n)^{n-2}(12)(123\cdots n)^2 = (n-1\, n)$이다.
$r = n-1$인 경우 $(123\cdots n)^{n-1}(12)(123\cdots n)^1 = (n\, 1)$이다.
한편 임의의 서로 다른 $i, j \in \{1, 2, \cdots, n\}(i < j)$에 대하여

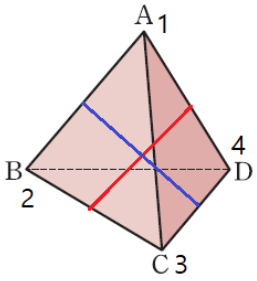
$$(i\ j)=(i\ \ i+1)(i+1\ i+2)\cdots(j-2\ j-1)(j-1\ j)(j-2\ j-1)\cdots(i+1\ i+2)(i\ i+1)$$

이다. 따름정리 2.4.13에 의하여 임의의 치환은 호환의 곱으로 나타낼 수 있으므로 모든 치환은 $\{(1,2),(1\,2\,3\cdots n)\}$에 의하여 생성된다.

2.4.17.

정사면체 군(T_d)은 정사면체$ABCD$의 각 꼭지점과 대면의 무게중심을 지나는 직선을 축으로 하는 회전변환과 각 선분의 중점과 평행인 선분의 중점을 지나는 축으로 하는 회전변환을 원소로 갖는 집합이다.

원소는 다음 과 같이 12개가 있다.



e : 제자리(항등변환) , $e=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=(1\ 2)$

a_1 : 꼭지점A 축 120° 회전변환 , $a_1=\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}=(2\ 3\ 4)$

a_2 : 꼭지점A 축 240° 회전변환 , $a_2=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}=(2\ 4\ 3)$

b_1 : 꼭지점B 축 120° 회전변환 , $b_1=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}=(1\ 3\ 4)$

b_2 : 꼭지점B 축 240° 회전변환 , $b_2=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}=(1\ 4\ 3)$

c_1 : 꼭지점C 축 120° 회전변환 , $c_1=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}=(1\ 2\ 4)$

c_2 : 꼭지점C 축 240° 회전변환 , $c_2=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}=(1\ 4\ 3)$

d_1 : 꼭지점D 축 120° 회전변환 , $d_1=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}=(1\ 2\ 3)$

d_2 : 꼭지점D 축 240° 회전변환 , $d_2=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}=(1\ 3\ 2)$

l_1 : 선분$\overline{AB}$ 중점과 선분 $\overline{CD}$중점 축 180° 회전변환 , $l_1=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=(1\ 2)(3\ 4)$

l_2 : 선분$\overline{AC}$ 중점과 선분 $\overline{BD}$중점 축 180° 회전변환 , $l_2=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(1\ 3)(2\ 4)$

l_3 : 선분$\overline{AD}$중점과 선분 $\overline{BC}$중점 축 180° 회전변환 , $l_3=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=(1\ 4)(2\ 3)$

$T_d=\{e,a_1,a_2,b_1,b_2,c_1,c_2,d_1,d_2,l_1,l_2,l_3\}$에서 연산을 함수(변환)의 합성으로 주면 교대군 A_4가 된다.

따라서 $T_d\cong A_4$ 즉, T_d는 S_4의 부분군 A_4와 동형이다.

== 연습문제 (3.1) ==

3.1.1. 잉여류 : $4\mathbb{Z}=\{\cdots,-4,0,4,8,\cdots\}$, ,
$1+4\mathbb{Z}=\{\cdots,-3,1,5,9,\cdots\}$,
$2+4\mathbb{Z}=\{\cdots,-2,2,6,10,\cdots\}$,
$3+4\mathbb{Z}=\{\cdots,-1,3,7,11,\cdots\}$

지수 : 4

3.1.2. 잉여류 : $4\mathbb{Z}=\{\cdots, -4, 0, 4, 8, \cdots\}$, ,
$2+4\mathbb{Z}=\{\cdots, -2, 2, 6, 10, \cdots\}$,

지수 $|2\mathbb{Z}/4\mathbb{Z}|=2$

3.1.3. 잉여류 : $<2>=\{0, 2, 4, 6, 8, 10\}$, ,
$1+<2>=\{1, 3, 5, 7, 9, 11\}$

지수 : 2

3.1.4. $<3>=\{0, 3, 6, 9, 12, 15, 18, 21\}$,
$1+<3>=\{1, 4, 7, 10, 13, 16, 19, 22\}$,
$2+<3>=\{2, 5, 8, 11, 14, 17, 20, 23\}$

지수 $|\mathbb{Z}_{24}/<3>|=3$

3.1.5. 좌잉여류를 먼저 구하자.

$(1)\langle(1\ 3)\rangle=\{(1),(1\ 3)\}$

$(1\ 3)\langle(1\ 3)\rangle=\{(1),(1\ 3)\}$

$(1\ 2)\langle(1\ 3)\rangle=\{(1\ 2),(1\ 3\ 2)\}$

$(2\ 3)\langle(1\ 3)\rangle=\{(2\ 3),(1\ 2\ 3)\}$

$(1\ 2\ 3)\langle(1\ 3)\rangle=\{(1\ 2\ 3),(2\ 3)\}$

$(1\ 3\ 2)\langle(1\ 3)\rangle=\{(1\ 3\ 2),(1\ 2)\}$

이므로 좌잉여류는 모두

$\langle(1\ 3)\rangle=\{(1),(1\ 3)\}$, $(1\ 2)\langle(1\ 3)\rangle=\{(1\ 2),(1\ 3\ 2)\}$, $(2\ 3)\langle(1\ 3)\rangle=\{(2\ 3),(1\ 2\ 3)\}$

로 3개이다.

다음에 우잉여류를 구하자.

$\langle(1\ 3)\rangle(1)=\{(1),(1\ 3)\}$
$\langle(1\ 3)\rangle(1\ 3)=\{(1),(1\ 3)\}$
$\langle(1\ 3)\rangle(1\ 2)=\{(1\ 2),(1\ 2\ 3)\}$
$\langle(1\ 3)\rangle(2\ 3)=\{(2\ 3),(1\ 3\ 2)\}$
$\langle(1\ 3)\rangle(1\ 2\ 3)=\{(1\ 2\ 3),(1\ 2)\}$
$\langle(1\ 3)\rangle(1\ 3\ 2)=\{(1\ 3\ 2),(2\ 3)\}$

이므로 우잉여류는 모두

$\langle(1\ 3)\rangle=\{(1),(1\ 3)\}$, $\langle(1\ 3)\rangle(1\ 2)=\{(1\ 2),(1\ 2\ 3)\}$, $\langle(1\ 3)\rangle(2\ 3)=\{(2\ 3),(1\ 3\ 2)\}$

로 3개이다.

지수는 $|S_3:\langle(13)\rangle|=\dfrac{|S_3|}{|\langle(13)\rangle|}=\dfrac{6}{2}=3$

3.1.6. $|G|=pg$이므로 G의 진부분군H의 위수는 $1,p,g$이다(라그랑주 정리 3.1.10).

ⅰ) $|H|=1$. $|H|=1$이므로 항등원을 생성원으로 하는 순환군이다.

ⅱ) $|H|=p$. $|H|=p$이면 항등원이 아닌 원소의 위수가 p이므로 $H=\langle a\rangle$가 성립하여 순환군이다(정리 3.1.16).

ⅲ) $|H|=q$. ⅱ와 동일한 이유로 순환군이다.

3.1.7. $e\neq a\in G$에 대하여 $\langle a\rangle$는 G의 부분군이므로 $\langle a\rangle=G$이고 순환군이다. 만약 유한군이 아니면 부분군 $\langle a^2\rangle$은 $\langle e\rangle\subsetneqq\langle a^2\rangle\subsetneqq\langle a\rangle$이므로 가정에 모순이다. 따라서 G는 유한군이다. 또한 G의 위수가 합성수 $|G|=mn,(1<m,n)$라 하면 위수 m인 부분군이 존재(정리 2.3.4)하여 가정에 모순이다. 따라서 G의 위수는 소수이다.

3.1.8. I) $\forall a\in G$, $a^{-1}a=e\in H$이므로 $a\sim_L a$ (반사관계 성립)

II) $a\sim_L b$가 성립한다 하자. 그러면 $a^{-1}b\in H$이다.

H가 부분군이므로 $b^{-1}a=(a^{-1}b)^{-1}\in H$

$b\sim_L a$(대칭관계 성립)

III) $a \sim_L b,\ b \sim_L c$가 성립한다 하자. 그러면 $a^{-1}b \in H,\ b^{-1}c \in H$ 이다.
H가 부분군이므로 $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$
$a \sim_L c$(추이관계 성립)
관계$\sim_L$은 G위에서 동치관계이다.

같은 방법으로 관계 $\sim_R$은 G위에서 동치관계임을 증명할 수 있다.

3.1.9.
Ha가 G의 부분군이면 $e \in Ha$이므로 적당한 $h \in H$에 대하여 $e = ha$이다. 그러므로 $a = h^{-1} \in H$가 되어 정리 3.1.7에 의하여 $Ha = H$가 되어 모순이다. 따라서 Ha는 G의 부분군이 아니다.

(별해) $G/_R H$는 G의 분할(정리 3.1.1)이므로 $Ha = H$ or $Ha \cap H = \varnothing$ 이다.
$Ha \neq H$이므로 $Ha \cap H = \varnothing$ 이다. 따라서 $e \in H$이고 $e \notin Ha$이다.
$\therefore Ha \not\leq G$

3.1.10. (정리 3.1.5) 함수 $f : H \to aH,\ f(h) = ah$라 정의하자. 정의에 의하여 분명히 전사함수이다.
다음에 군의 소거법칙을 이용하면

$$f(h) = f(h') \Rightarrow ah = ah' \Rightarrow h = h'$$

이므로 f는 단사함수가 되어 전사함수이다. 따라서 $|H| = |aH|$이다.
같은 방법으로 $|H| = |Ha|$를 증명할 수 있다.

3.1.11. (정리 3.1.7) 군 G의 부분군 H와 원소 $a, b \in G$에 대하여 다음을 증명하라.
(1) $aH = bH \quad \Leftrightarrow \quad a^{-1}b \in H \quad \Leftrightarrow \quad b^{-1}a \in H$
(2) $aH = bH \quad \Leftrightarrow \quad b \in aH \quad \Leftrightarrow \quad \exists\, h \in H,\ b = ah$
(3) $aH = bH \quad \Leftrightarrow \quad a \in bH \quad \Leftrightarrow \quad \exists\, h \in H,\ a = bh$
(4) $aH = H \quad \Leftrightarrow \quad a \in H$
(풀이) (1) $aH = bH \quad \Leftrightarrow \quad a^{-1}b \in H$를 증명하자.
($\Rightarrow$) $aH = bH$이라 하자. $\exists\, h, h' \in H,\ ah = bh' \Rightarrow b^{-1}ah = h'$
$\Rightarrow b^{-1}a = h'h \in H \quad \therefore b^{-1}a \in H$
($\Leftarrow$) $b^{-1}a \in H$이라 하자. $\exists\, h \in H, b^{-1}a = h \ \Rightarrow a = bh \wedge b = ah^{-1}$
($\subset$) $\forall\, ah' \in aH,\ ah' = bhh' \in bH \Rightarrow aH \subset bH$
($\supset$) $\forall\, bh' \in bH,\ bh' = ah^{-1}h' \in aH \Rightarrow bH \subset aH$
$\therefore aH = bH$
$aH = bH \Leftrightarrow b^{-1}a \in H$도 위와 같은 방법으로 증명할 수 있다.

(2) $aH = bH \quad \Leftrightarrow \quad b \in aH$를 증명하자.
($\Rightarrow$) $aH = bH$이라 하자. $b \in aH$이므로 $\therefore \exists\, h \in H, b = ah \in aH$
($\Leftarrow$) $b \in aH$이라 하자. $\exists\, h \in H,\ b = ah$이다. 그러면 위 (1)의 증명과 같이 $aH = bH$을 증명할 수 있다.
$aH = bH \Leftrightarrow \exists\, h \in H, b = ah$도 위와 같은 방법으로 증명할 수 있다.

(3) $bH = aH$이므로 (2)번과 같다.

(4) (3)에서 $b = e$이면 성립한다.

3.1.12. **(1)**

$a = (1)$	$a = (1\,2\,3)$	$a = (1\,3\,2)$
$\Rightarrow Ha = \{(1), (1\,2)\}$	$\Rightarrow Ha = \{(1\,2\,3), (2\,3)\}$	$\Rightarrow Ha = \{(1\,3\,2), (1\,3)\}$
$\Rightarrow aH = \{(1), (1\,2)\}$	$\Rightarrow aH = \{(1\,2\,3), (1\,3)\}$	$\Rightarrow aH = \{(1\,3\,2), (2\,3)\}$

$a=(1\,2)$ $\Rightarrow Ha=\{(1\,2),\,(1)\}$ $\Rightarrow aH=\{(1\,2),\,(1)\}$

$a=(1\,3)$ $\Rightarrow Ha=\{(1\,3),\,(1\,3\,2)\}$ $\Rightarrow aH=\{(1\,3),\,(1\,2\,3)\}$

$a=(2\,3)$ $\Rightarrow Ha=\{(2\,3),\,(1\,2\,3)\}$ $\Rightarrow aH=\{(2\,3),\,(1\,3\,2)\}$

이므로 $a=(1\,3),\,(2\,3),\,(1\,2\,3),\,(1\,3\,2)$이다.

(2) (1)에 의해서 성립함을 확인할 수 있다.

(3) $a=(1)$ $\Rightarrow Ka=\{(1),\,(1\,2\,3),\,(1\,3\,2)\}$ $\Rightarrow aK=\{(1),\,(1\,2\,3),\,(1\,3\,2)\}$

$a=(1\,2\,3)$ $\Rightarrow Ka=\{(1\,2\,3),\,(1\,3\,2),\,(1)\}$ $\Rightarrow aK=\{(1\,2\,3),\,(1\,3\,2),\,(1)\}$

$a=(1\,3\,2)$ $\Rightarrow Ka=\{(1\,3\,2),\,(1),\,(1\,2\,3)\}$ $\Rightarrow aK=\{(1\,3\,2),\,(1),\,(1\,2\,3)\}$

$a=(1\,2)$ $\Rightarrow Ka=\{(1\,2),\,(1\,3),\,(2\,3)\}$ $\Rightarrow aK=\{(1\,2),\,(1\,3),\,(2\,3)\}$

$a=(1\,3)$ $\Rightarrow Ka=\{(1\,3),\,(2\,3),\,(1\,2)\}$ $\Rightarrow aK=\{(1\,3),\,(2\,3),\,(1\,2)\}$

$a=(2\,3)$ $\Rightarrow Ka=\{(2\,3),\,(1\,2),\,(1\,3)\}$ $\Rightarrow aK=\{(2\,3),\,(1\,2),\,(1\,3)\}$

이므로 모든 $x\in G$에 대하여 $xK=Kx$이다.

(별해) $[S_3:K]=2$이므로 뒤 문제(3.1.14)에 의하여 모든 $x\in G$에 대하여 $xK=Kx$이다.

3.1.13. $\forall\, ah\in aH \Rightarrow ah=ah(a^{-1}a)=(aha^{-1})a=[(a^{-1})^{-1}ha^{-1}]a\in Ha(\because (a^{-1})^{-1}ha^{-1}\in H)$
$\Rightarrow aH\subset Ha$

$\forall\, ha\in aH \Rightarrow ha=(aa^{-1})ha=a(a^{-1}ha)\in aH(\because a^{-1}ha\in H)$
$\Rightarrow Ha\subset aH$

그러므로 $aH=Ha$이다.

3.1.14. $a\in H \Rightarrow aH=H=Ha(\because$ 정리 3.1.7(4))

$a\notin H$인 경우에는 H의 좌잉여류와 우잉여류 전체집합은 다음과 같다.

$$G/\sim_L=\{H,\,aH\},\quad G/\sim_R=\{H,\,Ha\}$$

그러므로 $H\cup aH=G=H\cup Ha,\ \ H\cap aH=H\cap Ha=\varnothing$ 이므로

$$aH=G-H=Ha$$

가 되어 $aH=Ha$이다.

3.1.15. (정리 3.1.18) $|G:H|=r$일 때, H의 좌잉여류 전체 집합을 $\{a_1H,\,a_2H,\,\cdots,\,a_rH\}$이라 하자. 그리고 $|H:K|=s$일 때, K의 좌잉여류 전체집합을 $\{b_1K,b_2K,\,\cdots,\,b_sK\}$이라 하자. 이때 $\{a_ib_jK\,|\,1=1,\cdots,r,\,j=1,\cdots,s\}$가 G의 K의 좌잉여류 집합임을 증명하면 $|G:K|=|G:H|\,|H:K|$이 성립한다.

$$G=\cup_{i=1}^{r}a_iH=\cup_{i=1}^{r}a_i(\cup_{j=1}^{s}b_jK)=\cup_{i=1,\cdots,r,\,j=1,\cdots,s}a_ib_jK$$

이고 $a_ib_jK\cap a_{i'}b_{j'}K\neq\varnothing$이라 하자. 그러면 $a_ib_jk=a_{i'}b_{j'}k'$, $k,\,k'\in K$, $a_i,a_{i'}\in G$, $b_j,b_{j'}\in H$가 존재한다. 그러므로 $b_jk,\,b_{j'}k'\in H$이므로 $a_ib_jk=a_{i'}b_{j'}k'\in a_iH\cap a_{i'}H$이다. 따라서 $a_iH=a_{i'}H$이다. 잉여류의 정의에 의하여 $a_i=a_{i'}$이다.

$$a_ib_jk=a_{i'}b_{j'}k' \Rightarrow a_ib_jk=a_ib_{j'}k' \Rightarrow b_jk=b_{j'}k'\in b_jK\cap b_{j'}K$$

이므로 잉여류의 정의에 의하여 $b_jK=b_{j'}K$이다. 따라서 $b_j=b_{j'}$이다. 따라서

$$a_ib_jK=a_{i'}b_{j'}K$$

이다. 그러므로 $\{a_ib_jK\,|\,1=1,\cdots,r,\,j=1,\cdots,s\}$가 G의 K의 좌잉여류 집합이 되어 $|G:K|=|G:H|\,|H:K|$이 성립한다.

3.1.16. (1) $a^6=b^{24}=e$
$\therefore |b|=2$ or 3 or 4 or 6 or 12 or 24

$|b|=2 \Rightarrow e=b^4=a\neq e$이 되어 모순이다.

$|b|=3 \Rightarrow e=b^{12}=a^3\neq e$이 되어 모순이다.

$|b|=4 \Rightarrow e=b^4=a\neq e$이 되어 모순이다.

$|b|=6 \Rightarrow e=b^{12}=a^3\neq e$이 되어 모순이다.

$|b|=12 \Rightarrow e=b^{12}=a^3\neq e$이 되어 모순이다.

$\therefore |b|=24$

(별해) $6=|a|=|b^4|=\dfrac{|b|}{\gcd(|b|,4)}$이므로 $|b|=6\cdot\gcd(|b|,4)$이다. 이때 $\gcd(|b|,4)=1$ 또는 2 또는 4뿐이다.

$\gcd(|b|,4)=1$일 때 $|b|=1\cdot 6=6$이다. 이때 $\gcd(6,4)=2$이므로 모순이다.

$\gcd(|b|,4)=2$일 때 $|b|=2\cdot 6=12$이다. 이 때 $\gcd(12,4)=4$이므로 모순이다.

$\gcd(|b|,4)=4$이어야 하므로 $|b|=4\cdot 6=24$이다.

(2) $b^4=aba^{-1}aba^{-1}=ab^2a^{-1}=a^2ba^{-2}$

$b^8=a^2ba^{-2}a^2ba^{-2}=a^2b^2a^{-2}=a^3ba^{-3}$

$b^{16}=a^3ba^{-3}a^3ba^{-3}=a^3b^2a^{-3}=a^4ba^{-4}$

$b^{32}=a^4ba^{-4}a^4ba^{-4}=a^4b^2a^{-4}=a^5ba^{-5}=b$

$\Rightarrow\ b=b^{32}$

$\Rightarrow\ b^{31}=e$

b의 위수는 라그랑주 정리에 의하여 1 또는 31이다. b가 항등원이 아니므로 b의 위수는 31이다.

(3) $a^2=e$이고 $aba^{-1}=b^2$이다. 그러므로

$b^4=ab^2a^{-1}=a^2b(a^{-1})^2=b\Rightarrow b^3=e$

이 때, 3은 소수 이므로 $\therefore |b|=3$

라그랑주 정리에 의해 $|b|=1$ 또는 $|b|=3$이다. b가 항등원이 아니므로 b의 위수는 3이다.

(4) $|a^2|=\dfrac{|a|}{\gcd(2,|a|)}=\dfrac{n}{\gcd(2,n)}$이다. n은 홀수이므로 $\gcd(2,n)=1$이다.

따라서 $|a^2|=n$이다.

(별해) $|a^2|=t$,라 하자. 그러면 $(a^2)^t=e\Rightarrow n|2t(\because$정리 2.3.3)이다. n이 홀수이므로 $n|t$이과 $t\leqq n$이므로 $t=n$이어야 한다.

(5) a의 위수가 소수이므로 라그랑주 정리에 의해 $<a>$의 부분군의 위수는 1 또는 p이다.

a가 항등원이 아니므로 $\therefore |a|=p$

(별해) $|a|=n$이라 하자. 그러면 $a^n=e$이다. 따라서 $n|p$이다(정리 2.3.3). 이 때 p가 소수이고 a가 항등원이 아니므로 $n=p$이다. 따라서 $|a|=p$이다.

3.1.17. $\gcd(|H|,|K|)=1$이므로 $H\cap K$는 라그랑주 정리에 의해

$|H\cap K||H|,\ |H\cap K||K|\ \Rightarrow\ \therefore |H\cap K||1$

이는 $|H\cap K|=1$이므로

$\therefore H\cap K=\{e\}$뿐이다.

(별해) $\forall x\in H\cap K,\ |x|=k$라 두자. 라그랑주 정리에 의하여

$k|12\ \Rightarrow\ k=1,2,3,4,6,12$이고

$k|5\ \Rightarrow\ k=1,5$

$\Rightarrow\ k=1$

$|x|=1$이므로 $x=e$이다.

3.1.18. 라그랑주 정리에 의해 $|g|=1$ or 2 or 4 or 8 이다. G는 순환군이 아니므로 $|g|\neq 8$

$|g|=1\Rightarrow g=e\Rightarrow g^4=e$

$|g|=2\Rightarrow g^2=e\Rightarrow g^4=e$

$|g|=4\Rightarrow g^4=e$

$\therefore$ 모든 $g\in G$에 대해서 $g^4=e$이다.

3.1.19. (1) $H\cap K\neq e$이라 하자. $a(\neq e)\in H\cap K$가 존재한다.

$a^p = e$이고 p가 소수이므로 $< a > = H$ 이다. $a \in K$ 이므로 $H = < a > \subset K$이다.
그러므로 $H \subset K$이다.

(2) $\{e\} = H \cap K$인 경우. $|H \cup K| = |H| + |K| - |H \cap K| = p + p - 1 = 2p - 1$
$\{e\} \neq H \cap K$인 경우. $\exists (e \neq) a \in H \cap K$에 대하여 $a \in H$이고 $a \in K$이다.
p가 소수이므로 $< a > = H$ 이고 $< a > = K$이다.
따라서 $H = < a > = K$ 이다.

(3) $a \in H \cap K$에 대하여
$a \in H, |a| = 1 \text{ or } p$이고 $a \in K, |a| = 1 \text{ or } q$
이다. p, q는 $p \neq q$이므로 $|a| = 1$이 되어 $a = e$이다.
따라서 $H \cap K = \{e\}$이고
$|H \cup K| = |H| + |K| - |H \cap K| = p + q - 1$

(4) $\forall a \in H \cap K$에 대하여 $\langle a \rangle < H \wedge \langle a \rangle < K$ 이다.
라그랑주 정리에 의해 $|a| \mid |H| \wedge |a| \mid |K|$ 이므로 $|a| \mid \gcd(|H|, |K|) = 1$이다.
따라서 $|a| = 1$이므로 $a = e$이다. 따라서 $H \cap K = \{e\}$ 이다.

$H < G, K < G$ 이므로 $HK \subset G$이다. 또한

$$|G| = |H||K| = \frac{|H||K|}{|H \cap K|} = |HK| \ (\because H \cap K = \{e\}) \text{ (정리 3.1.14)}$$

이므로 $G = HK$이다.

3.1.20. (1) $\left|\mathbb{Z}_n^*\right| = p - 1$이므로 임의의 $a \in \mathbb{Z}^*$에 대하여 $a^{p-1} = 1$ ($\because$ 라그랑주 정리)이므로 $a^p = a$이다.
(2) $\left|\mathbb{Z}_n^*\right| = \phi(n)$이므로 $\forall a \in \mathbb{Z}_n^*, |a| \mid \phi(n)$
$a^{\phi(n)} = 1$ ($\because$ 라그랑주 정리)

== 연습문제 (3.2) ==

3.2.1 $f(n) \equiv nf(1) \equiv 4n \pmod 7$
$\ker(f) = \{a \in \mathbb{Z} \mid 0 \equiv f(a) \equiv 4a \pmod 7\}$
$= \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 7\}$
$= 7\mathbb{Z}$
$f^{-1}(\{f(1)\}) = \{a \in \mathbb{Z} \mid f(a) \equiv f(1) \pmod 7\} = \{a \in \mathbb{Z} \mid 4a \equiv 4 \pmod 7\} = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 7\} = 1 + 7\mathbb{Z}$

3.2.2. $\ker(f) = \{0\}$, $Im(f) = 2\mathbb{Z}_{20}$
$\ker(f) = \{a \in \mathbb{Z}_{10} \mid 0 \equiv f(a) \equiv 6a \pmod{20}\}$
$= \{a \in \mathbb{Z}_{10} \mid 3a \equiv 0 \pmod{10}\}$
$= \{a \in \mathbb{Z}_{10} \mid a \equiv 0 \pmod{10}\}$
$= \{0, 10\}$
$Im(f) = \{a \in \mathbb{Z}_{10} \mid f(a) = 6a \in \mathbb{Z}_{20}\} = \{0, 6, 12, 18, 4, 10, 16, 22, 8, 14\} = \{0, 4, 6, 8, 10, 12, 14, 16, 18, 22\}$

3.2.3. (1) $\forall x, y \in \mathbb{Z}$에 대하여 $f(x+y) = a^{x+y} = a^x a^y = f(x)f(y)$이므로 f는 준동형사상이다.
(2) $Im(f) = f(\mathbb{Z}) = \{f(n) = a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$

$$\ker(f)=\{k\in\mid f(k)=e\}=\{k\in\mathbb{Z}\mid a^k=e\}=\begin{cases}|a|\mathbb{Z},\ |a|\text{가 유한},\\ \{0\},\ |a|\text{가 무한}\end{cases}$$

3.2.4. (1) $\forall a,b\in\mathbb{Z},\ f(a+b)=a+b=f(a)+f(b)$

$\therefore f$는 준동형사상

(2) $\forall a_i,b_i\in G_i,\ f_i(a_ib_i)=(e_1,e_2,\cdots,a_ib_i,\cdots,e_r)$
$=(e_1,e_2,\cdots,a_i,\cdots,e_r)(e_1,e_2,\cdots,b_i,\cdots,e_r)$
$=f_i(a_i)f_i(b_i)$

$\therefore f$는 준동형사상

(3) (반례) $G=S_3$라 하자.

$f((12)(123))=f(23)=(23)^{-1}=(23)$이고, $f((12))f((123))=(12)(132)=(13)$이므로
$f((12)(123))\neq f((12))f((123))$이다. $\therefore f$는 준동형사상이 아니다.

3.2.5. (1) $f(G)=\{f(a)\mid a\in G\}$이므로 $|f(G)|\leq|G|$이므로 $|f(G)|$도 유한이다. 한편 정리 3.2.22에 의하여

$$|f(G)|=|\{f^{-1}(\{f(a)\})\mid a\in G\}|=|\{aKer(f)\mid a\in G\}|=|G:Ker(f)|=|G|/|Ker(f)|$$

이므로 $|f(G)|$는 $|G|$의 약수이다.

(2) $f(G)<G'$이고, $|G'|$이 유한이므로 $|f(G)|$도 유한이다. 라그랑주 정리에 의해 $|f(G)|||G'|$이 성립한다.

3.2.6. (1) 존재한다.

$$\varphi(a)=\begin{cases}(1,2)\ ,\ \text{기치환}\in D_4\\ (1)\ ,\ \text{우치환}\in D_4\end{cases}$$

(2) 존재한다.

$$\varphi(a)=\begin{cases}(1,2)\ ,\ \text{기치환}\in S_4\\ (1)\ ,\ \text{우치환}\in S_4\end{cases}$$

(3) $f(1)=a\neq0$라 하면 $0=f(4\cdot1)=4f(1)=4a\Rightarrow a=0$이 되어 모순이다. 따라서 비자명 준동형사상은 존재하지 않는다.

3.2.7. 다음 준동형사상의 개수를 구하여라. [참조 : 항등원과 생성원에 대하여 생각하라.]

(1) $f:\mathbb{Z}_{12}\to\mathbb{Z}_6$ (2) $f:\mathbb{Z}_{12}\to\mathbb{Z}_{16}$

(4) $f:\mathbb{Z}\to\mathbb{Z}_8$ (4) $f:\mathbb{Z}_2\to\mathbb{Z}$

(5) $f:\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$ (6) $f:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$

(7) $f:\mathbb{Z}_6\to\mathbb{Z}_2\times\mathbb{Z}_2$ (8) $f:\mathbb{Z}_2\times\mathbb{Z}_2\to\mathbb{Z}_6$

(풀이) (풀이) $\mathbb{Z}=\langle1\rangle$, $\mathbb{Z}_n=\langle1\rangle$이므로 생성원 1의 상 $f(1)$의 개수가 준동형사상의 개수이다. 한편 $f(0)=0$이므로 $1\in\mathbb{Z}_n$에 대하여 $0=f(0)=f(n\cdot1)=nf(1)$을 이용하여 준동형사상의 개수를 구하자.

(1) $f(1)=a$라 하자. $0\equiv f(0)\equiv f(12\cdot1)\equiv12f(1)\equiv12a(\mathrm{mod}\,6)$이므로 $a=0,1,2,3,4,5$이 6개이다.

(별해) 문제 3.2.9에 의하여 준동형의 개수는 $\gcd(12,6)=6$개다.

(2) $f(1)=a$라 하자.

$$0\equiv f(0)\equiv f(12\cdot1)\equiv12f(1)\equiv12a(\mathrm{mod}\,16)\Rightarrow3a\equiv0(\mathrm{mod}\,4)\Rightarrow a\equiv0(\mathrm{mod}\,4)$$

이므로 $a=0,4,8,12$로 4개이다.

(별해) 문제 3.2.9에 의하여 준동형의 개수는 $\gcd(12,16)=4$개다.

(3) $\mathbb{Z}$에서 항등원은 0밖에 없으므로 $a=0,1,2,3,4,5,6,7$이 8개이다.

(4) 정리에 의하여 $Imf<\mathbb{Z}$이다. 그런데 $|Imf|\leq2$이므로 $\mathbb{Z}$의 유한 부분군이다.

$\mathbb{Z}$에서 유한인 부분군은 $\{0\}$뿐이므로 $Imf=\{0\}$밖에 없다. 결국 준동형사상의 개수는 영사상으로 1개이다.

(5) $f(1)=(a,b)\in\mathbb{Z}\times\mathbb{Z}$라 하자. 임의의 $m, n\in\mathbb{Z}$에 대하여

$$f(m+n)=(m+n)f(1)=(m+n)(a,b)=m(a,b)+n(a,b)=mf(1)+nf(1)=f(m)+f(n)$$

이므로 준동형의 개수는 정수개(가부번)이다.

(6) $\mathbb{Z}\times\mathbb{Z}$의 생성원 $(1,0),(0,1)$의 상 $f(1,0)=a, f(0,1)=b$라 하자.

임의의 $(m,n), (m',n')\in\mathbb{Z}\times\mathbb{Z}$에 대하여

$$f((m,n)+(m',n'))=f(m+m',n+n')=(m+m')f(1,0)+(n+n')f(0,1)$$
$$f(m,n)+f(m',n')=m(1,0)+nf(0,1)+m'f(1,0)+n'f(0,1)=(m+m')f(1,0)+(n+n')f(0,1)$$
$$\Rightarrow f((m,n)+(m',n'))=f(m,n)+f(m',n')$$

이므로 준동형의 개수는 정수개(가부번)이다.

(7) $f(1)=(a,b)$일 때, $(0,0)\equiv f(6\cdot 1)=6\cdot f(1)=(6a,6b)$이므로

$\begin{cases}6a\equiv 0\pmod 2\\ 6b\equiv 0\pmod 2\end{cases}$에서 $\begin{matrix}a=0,1\\ b=0,1\end{matrix}$ 이 성립한다. 따라서 생성원이 될 수 있는 가짓수는 $2\times 2=4$가지 이다.

(8) $\forall\, a,b\in\mathbb{Z}_2$ $f(a,b)=af(1,0)+bf(0,1)$이고,

$$0\equiv f(0,0)\equiv f(2\cdot 1,0)\equiv 2f(1,0)\pmod 6,\ \therefore f(1,0)\equiv 0 \text{ or } 3\pmod 6$$
$$0\equiv f(0,0)\equiv f(0,2\cdot 1)\equiv 2f(0,1)\pmod 6,\ \therefore f(0,1)\equiv 0 \text{ or } 3\pmod 6$$
$$\therefore f(a,b)\equiv 0 \text{ or } 3a \text{ or } 3b \text{ or } 3a+3b\pmod 6 \quad \therefore 4\text{개}$$

3.2.8. I) $n>0$일 때

$$\phi(n)=\phi(1+\cdots+1)=n\phi(1)$$
$$\phi(-n)=\phi((-1)+\cdots+(-1))=|n|\phi(-1)$$

$$\phi(0)=\phi(1+(-1))=\phi(1)+\phi(-1)=0\ \Rightarrow\ \phi(-1)=-\phi(1),$$
$$\phi(-n)=-n\phi(1)$$

결국, 임의의 $m\in\mathbb{Z}$에 대하여 $\phi(m)=m\phi(1)$이므로 준동형사상은 $|\mathbb{Z}|$개다.

II) 전사 군준동형을 찾아보자. $f(1)=a$일 때, 전사이므로 $\exists\, b\in\mathbb{Z}$에 대하여 $f(b)=1$이다. 그러면 $bf(1)=1$이 성립하고, 결국 $ba=1$이 된다. $a=1,-1$뿐이므로 따라서 전사 준동형사상인 함수 f는 2개 뿐이다.

III) 동형사상을 찾아보자. 우선 위의 전사인 $f(1)=1$와 $f(1)=-1$인 경우를 모두 살펴보면 각각 $f(n)=n$이고, $f(m)=-m$이다. 이런 함수들의 $\ker f$는 당연히 $\{0\}$뿐이다. 주어진 함수 두 개는 모두 단사이므로, 함수 f는 동형사상일 경우 2가지가 존재한다.

3.2.9. f가 준동형사상이라 하고, $\gcd(m,n)=d$라 하자.

$$0\equiv f(0)\equiv f(n\cdot 1)\equiv nf(1)\pmod m$$

$\frac{n}{d}f(1)\equiv 0\pmod{\frac{m}{d}}$이고, $f(1)\equiv 0\pmod{\frac{m}{d}}$

$$\therefore f(1)\equiv 0, \frac{m}{d}, \frac{2m}{d}, \cdots, \frac{(d-1)m}{d}\pmod m \quad \therefore d\text{개다.}$$

3.2.10. ($\Rightarrow$) f가 전사함수라 하자. 그러면 적당한 $a\in\mathbb{Z}_n$가 존재하여 $f(a)=1$이다. 그러면

$$0\equiv f(0)\equiv f(n\cdot a)\equiv nf(a)\equiv n\cdot 1\equiv n\pmod m\ \Rightarrow\ n=mt\ \Rightarrow\ m|n$$

이므로 $m|n$이다

($\Leftarrow$) $m|n$이라 하자. 그러면 $\gcd(m,n)=m$이므로 위 문제 3.2.9에 의하여 함수

$$f:\mathbb{Z}_n\to\mathbb{Z}_m,\quad f(1)=\frac{m}{m}=1$$

인 군 준동형사상이 존재한다. $m\leqq n$이므로 분명히 전사함수이다.

3.2.11. ($\Rightarrow$) $f(G)$가 가환이라고 하자.

$$\begin{aligned} f(xyx^{-1}y^{-1}) &= f(x)f(y)f(x^{-1})f(y^{-1}) \\ &= f(x)f(x^{-1})f(y)f(y^{-1}) \\ &= f(xx^{-1}yy^{-1}) \\ &= f(e) \\ &= e \end{aligned}$$

$\therefore xyx^{-1}y^{-1} \in \ker(f)$

($\Leftarrow$) $xyx^{-1}y^{-1} \in \ker(f)$이라 하자

$$\begin{aligned} e &= f(xyx^{-1}y^{-1}) \\ &= f(x)f(y)f(x^{-1})f(y^{-1}) \\ &= f(x)f(y)f(x)^{-1}f(y)^{-1} \end{aligned}$$

$f(y)(x) = f(x)(y)$이므로 $f(G)$는 가환이다.

3.2.12. (1) $f(n) = -n$ 이라 정의하면 잘 정의된다.

$i)$ $f(n) = f(n')$

$-n = -n'$

$n = n'$

이므로 f는 단사함수이다.

$ii)$ $\exists -n \in \mathbb{Z}$, $\exists n \in \mathbb{Z}$, $f(-n) = n$이므로 f는 전사함수이다.

$iii)$ $f(n+n') = -(n+n')$

$= -n-n'$

$= f(n)+f(n')$ 이므로

준동형사상이다.

따라서 f는 동형사상이다.

(2) $1 = f(n) = 2n$인 정수 n이 없으므로 전사가 아니다. 따라서 f는 동형사상이 아니다.

(별해) (1) $i) f(a+b) = -a-b$

$= (-a)+(-b)$

$= f(a)+f(b)$

$\therefore f$는 준동형사상

$ii) \ker(f) = \{a \in \mathbb{Z} \mid f(a) = -a = 0\} = \{0\}$

$\therefore f$는 단사함수

$iii) \forall a \in \mathbb{Z}$에 대해 $a = f(-a)$인 $-a \in \mathbb{Z}$가 존재한다.

$\therefore f$는 동형사상이다.

(2) $f(n) = 2n$ 이므로 $Imf = <2>$이다.

$1 \in \mathbb{Z}$이지만 $1 \notin <2>$이다.

$\therefore \mathbb{Z} \neq <2> = Im(f)$

$\therefore \mathbb{Z} \neq Im(f)$

3.2.13. (1) $\ker(\phi) = \left\{ f \in F \mid \phi(f) = \dfrac{d}{dx}f = 0 \right\} \supset \left\{ a \in \mathbb{R} \mid \dfrac{d}{dx}a = 0 \right\} = \mathbb{R} \neq \{0\}$

$\ker(\phi) \neq \{0\}$이므로 f는 단사함수가 아니다.

따라서 주어진 사상 ϕ는 동형사상이 아니다.

(2) $\phi(f) = \int_0^x f(t)dt = 1$인 $f(t)$가 존재하지 않으므로 전사함수가 아니다.

왜냐하면 $\phi(f)=\int_0^x f(t)dt=1$인 $f(t)$가 존재한다고 하자. 그러면 $F'(t)=f(t)$일 때 $F(x)-F(0)=1 \Rightarrow F(x)$는 상수함수이다. 그러면 $f(x)=F'(x)=0 \Rightarrow 1=\int_0^x f(t)dt=0$이 되어 모순이다.

따라서 주어진 사상 ϕ는 동형사상이 아니다.

(3) $\phi(f)=\frac{d}{dx}\left[\int_0^x f(t)d\right]=f(x)$이므로 ϕ는 항등함수이므로 전단사함수이다.

ϕ는 준동형사상이므로 ϕ는 동형사상이다.

3.2.14. 군 G 위수 p(소수)이므로 순환군이다. 따라서 생성원 $a\in G$가 존재하여 $G=\langle a\rangle$이다. 이때 함수

$$f:\langle a\rangle\to\langle a\rangle,\ f(a)=a^i(i=1,\ \cdots,\ p-1)$$

는 a^i가 G의 생성원(따름정리 2.3.12)이므로 자기동형사상이 된다. 따라서 자기동형사상은 $p-1$개다.

3.2.15. $f:\mathbb{Z}\to\mathbb{Z}$, $f(x)=x+1$이라 하자.

$$x=x' \Leftrightarrow x+1=x'+1 \Leftrightarrow f(x)=f(x')$$

이므로 함수의 잘 정의되고 단사함수이다.

$$\forall x\in\mathbb{Z},\ \exists\,(x-1)\in\mathbb{Z},\ f(x-1)=(x-1)+1=x$$

이므로 전사함수이다.

$$f(a+b)=a+b+1=(a+1)+(b+1)-1=f(a)+f(b)-1=f(a)*f(b)$$

가 되어 준동형사상이다.

따라서 f는 동형사상이다.

3.2.16. $f:(\mathbb{Q}-\{-1\},*)\to(\mathbb{Q}-\{1\},\circ),\ f(a)=-a$라 하자.

$$a,\ a'\in\mathbb{Q}-\{-1\},\ f(a)=f(a') \Rightarrow -a=-a' \Rightarrow a=a'$$

이므로 단사함수이다.

$$\forall\ a\in\mathbb{Q}-\{1\},\ f(-a)=-(-a)=a$$

이므로 전사함수이다.

$$\begin{aligned}\forall\ a,b\in(\mathbb{Q}-\{-1\}),\ f(a*b)&=f(a+b+ab)\\&=-a-b-ab\\&=f(a)+f(b)-f(a)f(b)\\&=f(a)\circ f(b)\end{aligned}$$

이므로 f는 준동형사상이다. 따라서 $(\mathbb{Q}-\{-1\},*)$와 $(\mathbb{Q}-\{1\},\circ)$는 동형사상이다.

3.2.17. (1) f가 준동형사상이 되려면 $f(a)*f(b)=f(a+b)=(a+b)+1$이어야 하므로

$$\forall\ x,y\in(\mathbb{Z},*)\text{에 대하여 } f(a)=x,\ f(b)=y\text{라 하면}$$

$$x=a+1,\ y=b+1 \Rightarrow a=x-1,\ b=y-1$$

가 된다. 따라서

$$x*y=f(a)*f(b)=a+b+1=(x-1)+(y-1)+1=x+y-1$$

따라서 $a*b=a+b-1$로 정의하면 f는 준동형사상이 된다.

(2) f가 준동형사상이 되려면 $f(a*b)=f(a)+f(b)=(a+1)+(b+1)=(a+b)+2$이어야 하므로

$$(a*b)+1=f(a*b)=(a+b)+2$$

$$a*b=a+b+1$$

따라서 $a*b=a+b+1$ 로 정의하면 f는 준동형사상이 된다.

3.2.18. (1) f가 준동형사상이 되려면 $f(a)*f(b)=f(a\cdot b)=ab+2$이어야 하므로

$$\forall\ x,y\in(\mathbb{Z},*)\text{에 대하여 } f(a)=x,\ f(b)=y\text{라 하면}$$

$$x=a+2,\ y=b+2 \Rightarrow a=x-2,\ b=y-2$$

가 된다. 따라서

$$x*y = f(a)*f(b) = ab+2 \ = (x-2)(y-2)+2$$

따라서 $a*b \equiv (a-2)(b-2)+2$로 정의하면 f는 준동형사상이 된다.

(2) $a = a*e = e*a = (a-2)(e-2)+2$ 이어야 하므로 $(e-2)=1$이고 $e=3$이다.

$$3 = 3*3^{-1} = (3-2)(3^{-1}-2)+2 = 3^{-1}$$

이므로 $3^{-1}=3$이다.

(별해) (1) $f(a)*f(b) = f(ab) = ab+2$

$(a+2)*(b+2) = ab+2$

$a+2 = x, b+2 = y$ 라 하자.

$x*y = (x-2)(y-2)+2$이다.

(2) $x*y = (x-2)(y-2)+\ 2 = x \Rightarrow (x-2)(y-2) = x-2 \Rightarrow y = 3$이다. 그러므로 항등원은 3이다.

$x*y = (x-2)(y-2)+\ 2 = 3$인 y를 구해보자. $y = \dfrac{1}{x-2}+2$ 이다.

$\mathbb{Z}$에서 역원이므로 1의 역원은 1이고 3의 역원은 3이다. 다른 정수에서는 유리수가 나오므로 역원이 존재하지 않는다.

3.2.19. $x \in G$에 대하여 함수 $\rho_x : G \to G, \rho_x(a) = ax^{-1}$가 전단사임을 보이자.

$$\rho_x(a) = \rho_x(a') \Rightarrow ax^{-1} = a'x^{-1} \Rightarrow a = a'$$

이므로 ρ_x는 단사함수이다. 그리고 임의의 $a \in G$에 대하여

$$\rho_x(ax) = (ax)x^{-1} = a$$

이므로 전사함수이다. 따라서 $\rho_x \in S_G$이다.

$$A = \left\{\rho_x \in S_G \mid \rho_x : G \to G,\ \rho_x(a) = ax^{-1},\ \forall a \in G\right\}$$라 하자.

함수 $f : G \to A, f(x) = \rho_x$가 동형사상임을 보이자.

$$f(x) = f(y) \Rightarrow \rho_x = \rho_y \Rightarrow \rho_x(e) = \rho_y(e) \Rightarrow ex^{-1} = ey^{-1} \Rightarrow x = y$$

f는 단사함수 이다. 정의에 의하여 f는 전사함수이다.

다음에 f가 준동형사상임을 보이기 위해 먼저 $\rho_{xy} = \rho_x\rho_y$임을 보이자. 임의의 $a \in G$에 대하여

$$\rho_{xy}(a) = a(xy)^{-1} = a(y^{-1}x^{-1}) = \rho_x(ay^{-1}) = \rho_x(\rho_y(a)) = \rho_x\rho_y(a)$$

이므로 $\rho_{xy} = \rho_x\rho_y$이다. 그러므로 임의의 $x, y \in G$에 대하여

$$f(xy) = \rho_{xy} = \rho_x\rho_y = f(x)f(y)$$

가 되어, f는 준동형사상이다. 그러므로 f는 동형사상이 되어 $G \cong A$이다.

3.2.20. G는 유한 가환군이고, $\gcd(n, |G|) = 1$일 때, 다음을 증명하라.

(1) G 위에서 함수 $f : G \to G, f(x) = x^n$는 군동형사상임을 보여라.

(2) 임의의 $x \in G$는 $x = y^n$을 만족시키는 $y \in G$가 존재함을 보여라.

(풀이) (1) 임의의 $x, y \in G$에 대하여

$$f(xy) = (xy)^n = x^ny^n = f(x)f(y)$$

이므로 f는 준동형이다.

$x \in Ker(f)$라 하자.

$$e = f(x) = x^n \Rightarrow |x|\text{는 } n\text{의 약수}$$

한편 라그람주 정리에 의하여 $|x|$는 $|G|$의 약수이다. 따라서 $|x|$는 $\gcd(n,|G|) = 1$의 약수가 되어 $x = e$가 되어야 한다. 따라서 f는 단사함수이다.

G는 유한 집합이므로 f는 전사함수가 되어야 하므로 f는 동형사상이다.

(2) (1)에 의하여 f가 전사함수이므로 임의의 $x \in G$는 $x = y^n$을 만족시키는 $y \in G$가 존재한다.

3.2.21. $i)$ $K = eKe$ ($\because e \in H \cap K$) 이므로 $K \sim K$이다. 따라서 반사관계가 성립한다.

$ii)$ $H \sim K$ 일 때, $\exists g \in G$, $K = gHg^{-1}$ 이다. 그러면 $H = g^{-1}Kg = g^{-1}K(g^{-1})^{-1}$이므로 $K \sim H$ 이다.
따라서 대칭관계가 성립한다.

$iii)$ $H \sim K$, $K \sim J$ 일 때, $\exists g, h \in G$, $K = gHg^{-1}$, $J = hKh^{-1}$를 만족한다.

$$J = hKh^{-1} = h(gHg^{-1})h^{-1} = (hg)H(hg)^{-1}$$

이므로 $H \sim J$ 이다. 따라서 추이관계가 성립한다.

그러므로 켤레관계 $\sim$는 A 위에서 동치관계이다.

3.2.22. f가 전단사함수이므로 $f^{-1}f = ff^{-1} = id$이다. 따라서 $\sigma, \delta \in S_A$에 대하여

$$\phi(\sigma\delta) = f(\sigma\delta)f^{-1} = f(\sigma f^{-1} f\delta)f^{-1} = (f\sigma f^{-1})(f\delta f^{-1}) = \phi(\sigma)\phi(\delta)$$

이므로 ϕ는 준동형사상이다. 다음에 $\sigma \in \ker(\phi)$라 하자.

$$id = \phi(\sigma) = f\sigma f^{-1} \Rightarrow f^{-1}f = \sigma \Rightarrow id = \sigma$$

이므로 ϕ는 단사함수 이다.

임의의 $\delta \in S_B$에 대하여 $f^{-1}\delta f \in S_A$이므로

$$\phi(f^{-1}\delta f) = f(f^{-1}\delta f)f^{-1} = \delta$$

가 되어 전사함수이다. 따라서 ϕ는 동형사상이다.

== 연습문제 (3.3) ==

3.3.1. (1) $|<3>| = |\{0, 3\}| = 2$이므로 잉여군의 위수는 $\frac{|\mathbb{Z}_6|}{|<3>|} = \frac{6}{2} = 3$이다.

(2) $|\langle (2,1) \rangle| = |\{(0,0),(2,1)\}| = 2$이므로 잉여군의 위수는 $|\mathbb{Z}_4 \times \mathbb{Z}_2| / |\langle (2,1) \rangle| = \frac{8}{2} = 4$이다.

(3) $|\langle (2,2) \rangle| = |\{(0,0), (2,2), (0,4), (2,6), (0,8), (2,10)\}| = 6$이고 $|\mathbb{Z}_4 \times \mathbb{Z}_{12}| = 48$이므로

$|\mathbb{Z}_4 \times \mathbb{Z}_{12}| / |\langle (2,2) \rangle| = \frac{48}{6} = 8$이다.

(4) $|\mathbb{Z}_4 \times \mathbb{Z}_{12}| = 48$, $|<2> \times <2>| = \mathrm{lcm}(|2|,|2|) = 2 \times 6 = 12$이므로 $\frac{|\mathbb{Z}_4 \times \mathbb{Z}_{12}|}{|<2> \times <2>|} = \frac{48}{12} = 4$이다.

3.3.2. $<(2,3)> = \{(0,0), (2,3), (4,0), (6,3), (8,0), (10,3)\}$이므로

$(5,5) + H$의 위수는 $|\mathbb{Z}_{12} \times \mathbb{Z}_6| / |<(2,3)>| = \frac{72}{6} = 12$의 약수 1, 2, 3, 4, 6, 12 중에 있다.

$(5,5) \notin <(2,3)>$, $2(5,5) = (10,4) \notin <(2,3)>$, $3(5,5) = (3,3) \notin <(2,3)>$,
$4(5,5) = (8,2) \notin <(2,3)>$, $6(5,5) = (6,0) \notin <(2,3)>$

이므로 위수는 12가 된다.

3.3.3. (1) $|<4>| = |\{0, 4, 8\}| = 3$이므로 잉여군의 위수는 $\frac{|\mathbb{Z}_{12}|}{|<4>|} = \frac{12}{3} = 4$이다. 따라서 $2 + \langle 4 \rangle$의 위수는 1, 2, 4 중에서 있다. $2 \cdot 2 = 4 \in \langle 4 \rangle$ 이므로 위수는 2이다.

(2) (1) 참조. $5 + \langle 4 \rangle$의 위수는 1, 2, 4 중에서 있다. $2 \cdot 5 = 10 \notin \langle 4 \rangle$ 이므로 위수는 4이다.

(3) $<(1,1)> = \{(0,0), (1,1), (2,2), (0,3), (1,4), (2,5)\}$이므로

$(2,1) + <(1,1)>$의 위수는 $|\mathbb{Z}_3 \times \mathbb{Z}_6| / |<(1,1)>| = \frac{18}{6} = 3$의 약수 1, 3 중에 있다. 따라서 위수는 3이 된다.

3.3.4. $<(1,0)>=\{(0,0),\ (1,0),\ (2,0),\ (3,0)\}$이므로

$(a,b)+<(1,0)>$의 위수는 $|\mathbb{Z}_4\times\mathbb{Z}_6|/|<(1,0)>|=\frac{24}{4}=6$의 약수 1, 2, 3, 6 중에 있다.

$(1,1)+<(1,0)>$의 위수는 6이므로 잉여군 $\mathbb{Z}_4\times\mathbb{Z}_6/<(1,0)>$은 순환군이다. 따라서 위수 6인 원소는 2개가 존재(따름정리 2.3.12)한다. 그러므로 위수 6인 원소는 $(a=0,1,\cdots,5)$

$(a,1)+<(1,0)>=(0,1)+<(1,0)>$과 $(a,5)+<(1,0)>=(0,5)+<(1,0)>$

인 2개이다.

3.3.5. (1) $f(x)=\cos x+i\sin x=e^{xi}$이므로 $f(x+y)=e^{(x+y)i}=e^{xi}e^{yi}=f(x)f(y)$

(2) $\ker f=\{x\in\mathbb{R}\mid 1=f(x)=\cos x+i\sin x\}=\{x\in\mathbb{R}\mid \sin x=0,\ \cos x=1\}=\{2n\pi\mid n\in\mathbb{Z}\}=<2\pi>$

$Imf=\{f(x)|x\in\mathbb{R}\}=\{\cos x+i\sin x\mid x\in\mathbb{R}\}$ 반지름이 1인 원상의 점집합이다.

(3) $\ker(g)=\{x\in\mathbb{R}\mid \sin(2\pi x)=0,\ \cos(2\pi x)=1\}=\{n\mid n\in\mathbb{Z}\}=\mathbb{Z}$

3.3.6. $\ker f=\{x\in\mathbb{Z}_8\mid f(x)\equiv 0(\mathrm{mod}\,4)\}=\{0,\ 4\}=<4>$

$\mathbb{Z}_8/\ker f=\{x+<4>\ \mid x\in\mathbb{Z}_8\}=\{<4>,\ 1+<4>,\ 2+<4>,\ 3+<4>\}$

$|\mathbb{Z}_8/\ker(f)|=4$

3.3.7. (1) $K=\ker f=\{n\in\mathbb{Z}_{18}\mid 0\equiv f(n)=10n\equiv 0(\mathrm{mod}\,12)\}=\{n\in\mathbb{Z}_{18}\mid 5n\equiv 0(\mathrm{mod}\,6)\}=\{0,\ 6,\ 12\}=<6>$

$Imf=\{10n(\mathrm{mod}\,12)|n\in\mathbb{Z}_{18}\}=\{0,2,4,6,8,10\}$

(2) $\mathbb{Z}_{18}/K=\{a+<6>|a\in\mathbb{Z}_{18}\}=\{<6>,\ 1+<6>,\ 2+<6>,\ 3+<6>,\ 4+<6>,\ 5+<6>\}$

(3) $\phi:\mathbb{Z}_{18}/K\to Im(f),\ \phi(a+K)=f(a)$라 정의하자.

$a+K=b+K\Leftrightarrow a-b\in K\Leftrightarrow f(a-b)=0\Leftrightarrow f(a-b)=0\Leftrightarrow f(a)=f(b)$

이므로 잘 정의되고 단사함수이다. 분명히 전사함수이다. 임의의 $a+K,\ b+K\in\mathbb{Z}_{18}/K$에 대하여

$\phi((a+K)+(b+K))=\phi(a+b+K)=f(a+b)=f(a)+f(b)=\phi(a+K)+\phi(b+K)$

이므로 준동형사상이다. 따라서 $\mathbb{Z}_{18}/K\cong Imf$이다.

3.3.8. (수정된 문제) 군 G의 원소 $a\in G$와 부분군 $C_G<Z(G)$에 대하여 $\theta:G\to G,\ \theta(x)=xax^{-1}a^{-1}$는 준동형사상임을 보여라. 또, $\ker(\theta)$를 구하여라.

(풀이) $x,\ y\in G$에 대하여 $xax^{-1}a^{-1},\ yay^{-1}a^{-1}\in C_G<Z(G)$이므로

$$\begin{aligned}\theta(xy)&=(xy)a(xy)^{-1}a^{-1}=xyay^{-1}x^{-1}a^{-1}=xyay^{-1}(a^{-1}x^{-1}xa)x^{-1}a^{-1}\\&=x(yay^{-1}a^{-1})x^{-1}(xax^{-1}a^{-1})\qquad=(yay^{-1}a^{-1})xx^{-1}(xax^{-1}a^{-1})\\&=(yay^{-1}a^{-1})(xax^{-1}a^{-1})\\&=(xax^{-1}a^{-1})(yay^{-1}a^{-1})\\&=\theta(x)\theta(y)\end{aligned}$$

이므로 θ는 준동형사상이다.

$\ker\theta=\{x\in G\mid e=\theta(x)=xax^{-1}a^{-1}\}=\{x\in G\mid ax=xa\}=Z(a)$이다.

3.3.9. (1) $\forall f(g)\in f(G),\ f(n)\in f(N)$에 대하여 $N\triangleleft G$이므로 $gng^{-1}\in N$이다. 그러므로

$$f(g)f(n)f(g)^{-1}=f(gng^{-1})\in f(N)$$

이므로 $f(N)\triangleleft f(G)$이다(정리 3.3.4).

(2) $\forall g\in G,\ n\in f^{-1}(N')$에 대하여 $f(n)\in N'$이다. 그리고 $N'\triangleleft f(G)$이므로 $f(g)f(n)f(g)^{-1}\in N'$이다. 그러므로

$$f(gng^{-1})=f(g)f(n)f(g)^{-1}\in N'\Rightarrow gng^{-1}\in f^{-1}(N')$$

이므로 $f^{-1}(N')\triangleleft G$이다(정리 3.3.4).

3.3.10. $\exists a\in G,\ G/Z(G)=<aZ(G)>=\{a^tZ(G)\mid t\in\mathbb{Z}\}$($G$의 분할)이다.

그러면 $G=\bigcup_{t\in Z} a^t Z(G)$이다. $\forall x, y\in G,\ \exists g, g'\in Z(G),\ t, s\in\mathbb{Z},\ x=a^t g,\ y=a^s g'$이다.

따라서 $xy=(a^t g)(a^s g')=a^t g a^s g'=a^{t+s}gg'=a^s a^t g' g=a^s g' a^t g=(a^s g')(a^t g)=yx$ 이므로 G는 가환군이다.

3.3.11. (1)과 S_3는 분명히 정규부분군이다. 위수 2인 부분군에 대해서는

$\{(1\,3),(1\,2\,3)\}=(1\,3)\langle(1\,2)\rangle\neq\langle(1\,2)\rangle(1\,3)=\{(1\,3),(1\,3\,2)\}$

$\{(1\,2),(1\,3\,2)\}=(1\,2)\langle(1\,3)\rangle\neq\langle(1\,3)\rangle(1\,2)=\{(1\,2),(1\,2\,3)\}$

$\{(1\,2),(1\,2\,3)\}=(1\,2)\langle(2\,3)\rangle\neq\langle(2\,3)\rangle(1\,2)=\{(1\,2),(1\,3\,2)\}$

으로 정규부분군이 아니다. 하지만 위수 3인 부분군 $\langle(1\,2\,3)\rangle=\langle(1\,3\,2)\rangle$의 원소는 모두 우치환이다. 그러므로

$$\forall\alpha\in\langle(1\,2\,3)\rangle=\langle(1\,3\,2)\rangle\ \Rightarrow\ \alpha\langle(1\,2\,3)\rangle=\langle(1\,2\,3)\rangle\alpha$$

이다. 한편 기치환 β에 대한 $\langle(1\,2\,3)\rangle$의 잉여류의 원소 3개 모두 기치환이므로

$$\beta\langle(1\,2\,3)\rangle=\langle(1\,2\,3)\rangle\beta$$

이다. 따라서 정규부분군은 (1)과 $\langle(1\,2\,3)\rangle$, S_3로 3개뿐이다.

3.3.12. 일반 선형군 $G=GL(2,\mathbb{R})$의 부분군 $H=\{\begin{pmatrix}a&b\\0&d\end{pmatrix}\in G\mid ad\neq 0\}$에 대하여 다음 물음에 답하라.

(1) H는 G의 정규부분군인가?

(2) (수정된 문제) $K=\{\begin{pmatrix}a&b\\0&d\end{pmatrix}\in G\mid ad=1\}$ 은 H의 정규부분군임을 보여라.

(풀이) (1) 연습문제 (2.2)절 7번 (1)에 의하여 G의 부분군이다.

$\begin{pmatrix}1&0\\1&1\end{pmatrix}\in G,\ \begin{pmatrix}1&1\\0&1\end{pmatrix}\in H$에 대하여

$$\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}^{-1}=\begin{pmatrix}1&1\\1&2\end{pmatrix}\begin{pmatrix}1&0\\-1&1\end{pmatrix}=\begin{pmatrix}0&1\\-1&2\end{pmatrix}\notin H$$

이므로 H는 G의 정규부분군이 아니다(정리 3.3.4).

(2) $\begin{pmatrix}1&0\\0&1\end{pmatrix}\in K$

$\forall\begin{pmatrix}a&b\\0&d\end{pmatrix}\in K,\quad \begin{pmatrix}a&b\\0&d\end{pmatrix}^{-1}=\begin{pmatrix}d&-b\\0&a\end{pmatrix}\in K\quad(ad\neq 0)$

$\forall\begin{pmatrix}a&b\\0&d\end{pmatrix},\begin{pmatrix}a'&b'\\0&d'\end{pmatrix}\in H,\quad \begin{pmatrix}a&b\\0&d\end{pmatrix}\begin{pmatrix}a'&b'\\0&d'\end{pmatrix}=\begin{pmatrix}aa'&ab'+bd'\\0&dd'\end{pmatrix}\in H\ ((aa')(dd')=ada'd'=1)$

$\therefore$ G의 부분군이다.

$\begin{pmatrix}a&b\\0&d\end{pmatrix}\in H,\ \begin{pmatrix}x&y\\0&w\end{pmatrix}\in K,\ ad\neq 0,\ xw=1$에 대하여

$$\begin{pmatrix}a&b\\0&d\end{pmatrix}\begin{pmatrix}x&y\\0&w\end{pmatrix}\begin{pmatrix}a&b\\0&d\end{pmatrix}^{-1}=\frac{1}{ad}\begin{pmatrix}ax&ay+bw\\0&dw\end{pmatrix}\begin{pmatrix}d&-b\\0&a\end{pmatrix}=\frac{1}{ad}\begin{pmatrix}adx&-abx+a(ay+bw)\\0&adw\end{pmatrix}=\begin{pmatrix}x&\frac{-abx+a(ay+bw)}{ad}\\0&w\end{pmatrix}\in K$$

이므로 K는 H의 정규부분군이다(정리 3.3.4).

3.3.13. (1) $H=\{A\in GL(n,\mathbb{R})\mid |A|=1\}$이라하자. $|I_n|=1$이므로 $I_n\in H$이다.

임의의 $A, B\in H$에 대하여

$$|AB^{-1}|=|A||B|^{-1}=1$$

이므로 H는 G의 부분군이다. 다음에 임의의 $X\in G, A\in H$에 대하여

$$|XAX^{-1}|=|X||A||X|^{-1}=|X||X|^{-1}=1$$

이므로 $XAX^{-1}\in H$가 되어 H는 G의 정규부분군이다(정리 3.3.4).

(2) (1)과 같은 방법으로 정규부분군임을 증명할 수 있다.

3.3.14. G는 실함수들의 집합이므로 가환군이다.

영함수 $g(x)\equiv 0$에 대하여 $g\in H$이다. $g,h\in H$라 하자.

$$(g+(-h))(0)=(g-h)(0)=g(0)-h(0)=0-0=0$$

이므로 $H<G$이다. 따라서 가환군의 부분군이므로 H는 G의 정규부분군이다.

3.3.15. $H<\mathbb{Q}/\mathbb{Z}, |H|<\infty$ 이라 하자. $\frac{q}{p}+\mathbb{Z}\in H$를 $\frac{q}{p}$라 하자.

$H=\left\{\frac{q_1}{p_1},\frac{q_2}{p_2},\cdots,\frac{q_n}{p_n}\right\}$이라 하자. $\mathrm{lcm}\{p_1,p_2,\cdots,p_n\}=l$이라 놓으면

$H=\left\{\frac{r_1}{l},\frac{r_2}{l},\cdots,\frac{r_n}{l}\right\}$인 $r_i\in\mathbb{Z}$가 존재한다.

① $H=\{0\}$이면 H는 순환부분군

② $H\neq\{0\}$인 경우, $H<\mathbb{Q}/\mathbb{Z}$이므로 $\frac{r}{l}(\neq 0)\in H$이면 $\frac{-r}{l}\in H$이고 양수$\frac{r}{l}$이 존재한다.

그러므로 $d=\min\{r_i\}, r_i>0$이라 하면 $H=\left\langle\frac{d}{l}\right\rangle$임을 보이자.

i) $\left\langle\frac{d}{l}\right\rangle\subset H$는 자명

ii) 임의의 $\frac{r_i}{l}\in H$에 대하여 나눗셈정리에 의해 $\exists q,s\in\mathbb{Z}, r_i=dq+s,\ 0\le s<d$이다.

$$\frac{s}{l}=\frac{r_i-dq}{l}=\frac{r_i}{l}-\frac{dq}{l}\in H$$

이므로 d의 최소성에 의하여 $s=0$이고 $r_i=dq$이므로 $\frac{r_i}{l}=\frac{dq}{l}\in\left\langle\frac{d}{l}\right\rangle$이다. 따라서 $H\subset\left\langle\frac{d}{l}\right\rangle$이다.

$\therefore H$는 생성원이 $\frac{d}{l}$인 순환부분군

3.3.16. $G/H=\langle aH\rangle\ (a\notin H)$라고 하자.($a\in H$이면 $G/H=H=\{e\}$이므로 유한 순환군)

① $K=\langle a\rangle<G, a\notin H, a\in G$라 하자.

$a^k\in H\cap K$이면 $a^k\in H$이고 $a^kH=H$이다.

이때 $k\neq 0$이면 $|aH|\le k$이므로 $|aH|=\infty$에 모순

따라서 $k=0$이고 $H\cap K=\{e\}$

② 임의의 원소 $g\in G$에 대하여

$gH\in G/H=\langle aH\rangle$

$gH=a^tH\subset KH=HK, \exists t\in\mathbb{Z}$ (G는 아벨군)

$g=hk, \exists h\in H, k\in K$

$g\in HK$

$\therefore G=HK$

3.3.17. 함수 $f: G/K\to H, f(hkK)=h, h\in H, k\in K$라 정의하자. 그러면 정리 3.1.7에 의하여

$$hkK=h'k'K\Leftrightarrow hK=h'K\Leftrightarrow h^{-1}h'\in K\cap H=\{e\}\Leftrightarrow h=h'$$

이므로 잘 정의되고 단사함수이다. 분명히 전사함수이므로 f는 전단사함수이다.

다음에 임의의 $hkK, h'k'K\in G/K$에 대하여 K는 G의 정규부분군이므로 적당한 $k''\in K$가 존재하여

$$f(hkK\cdot h'k'K)=f(hkh'k'K)=f(hh'k''k'K)=hh'=f(hk'K)f(h'k'K)$$

이다. 그러므로 f는 준동형사상이다. 따라서 $G/K\cong H$이다.

3.3.18. $|G/H|=\frac{|G|}{|H|}=[G:H]=20$이므로 임의의 $g\in G$에 대하여

$$H=(gH)^{20}=g^{20}H\ \Rightarrow\ g^{20}\in H$$

이다. 따라서 $H = x^{20}H = (x^7)^3 x^{-1}H = x^{-1}H$이다. 그러므로 $x^{-1} \in H$ 이고 $H < G$이므로 $x \in H$ 이다.

3.3.19. $|G/N| = |G:N| = a$, $|H| = b$라 하자. 그러면 적당한 정수 x, y가 존재해서 $1 = ax + by$이다. 그러면 $h \in H$에 대하여 $e = (hN)^a = h^a N \Rightarrow h^a \in N$이다. 따라서

$$h = h^1 = h^{ax+by} = h^{ax}h^{by} = (h^a)^x e^y = (h^a)^x \in N \ (\because h^a \in N)$$

이므로 $h \in N$이다. 그러므로 $H < N$이다.

3.3.20. 임의의 $n \in H \cap N$, $h \in H$에 대하여 N이 G의 정규부분군이므로 $hnh^{-1} \in N$이다. 그러므로

$$hnh^{-1} \in H \cap N$$

이다. 따라서 $H \cap N$ 는 H의 정규부분군이다.

(반례) $G = N = S_3$, $H = \{(1), (1\ 2)\}$이라 하자.

$N \triangleleft G$이지만 G의 부분군 $H \cap N = H$는 G의 정규부분군이 아니다(연습문제 3.3.11 참조).

3.3.21. $|G/H| = \frac{pq}{p} = q$, $|G/K| = \frac{pq}{q} = p$ 가 소수이므로 G/H, G/K는 순환군이다(정리 3.1.16). 그러므로 G/H, G/K는 가환군이고 정리 3.3.28에 의하여

$$C_G \subset H \cap K = \{e\} \Rightarrow C_G = \{e\} \Rightarrow G\text{는 가환군}$$

또한 p, q가 소수이므로 H, K는 순환군이다. 그러므로 적당한 원소 $a, b \in G$ 가 존재하여 $H = \langle a \rangle$, $K = \langle b \rangle$이다.
그러면 연습문제 2.3.11에 의하여 $|ab| = |a||b| = pq$이다. 따라서 $G = \langle ab \rangle$가 되어 G는 순환군이다.

3.3.22. $M < N = \langle a \rangle$라고 하자. $M < N < G$ 이다. N이 순환군이므로 M도 순환군이다.

이제 M이 G의 정규부분군이 됨을 보이자.

M이 N의 순환부분군이므로 $M = < a^m >, \exists m \in \mathbb{Z}$ 이다.

$\forall x \in M, \forall g \in G \Rightarrow gxg^{-1} \in M$ 임을 보이면 된다.

임의의 $x \in M$에 대하여 $x = a^{my}$인 $y \in \mathbb{Z}$가 존재한다.

$N \triangledown G$ 이므로 $gxg^{-1} \in N$ 이다. 이때 $gxg^{-1} = a^t\ (t \in \mathbb{Z})$라고 하자.

$$\begin{aligned} gxg^{-1} &= g(a^{my})g^{-1} \\ &= (gxg^{-1})^{my} \\ &= (a^t)^{my}\ (\because gxg^{-1} \in N) \\ &= a^{tmy} \\ &= (a^m)^{ty} \\ &\in M \end{aligned}$$

따라서 M 은 G 의 정규부분군이다.

3.3.23. 임의의 $g \in G$, $h \in H$에 대해 $ghg^{-1} \in H$임을 보이자.

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1}f(h) = f(h)$$

이므로, $f(ghg^{-1})f(h)^{-1} = f(ghg^{-1}h^{-1}) = e$이다. 따라서 $ghg^{-1}h^{-1} \in \ker(f)$이다.

$\ker(f) < H$이므로 적당한 $h' \in H$가 존재해서, $ghg^{-1}h^{-1} = h'$이다.

따라서 $ghg^{-1} = h'h \in H$이므로 H는 G의 정규부분군이다.

3.3.24. $H = \{g \in G \mid i_g : G \to G,\ x = i_g(x) = gxg^{-1},\ \forall x \in G\} = \{g \in G \mid xg = gx,\ \forall x \in G\}$라 하자.

정리 3.3.23(1)의 증명에서 H는 G의 부분군이다.

임의의 $y \in G$, $g \in H$에 대해 $ygy^{-1} \in H$임을 보이자. 이때 $g \in H$이므로 $y = gyg^{-1} \Rightarrow yg = gy$이다. 따라서

$$i_{ygy^{-1}}(x) = (ygy^{-1})x(ygy^{-1})^{-1} = (gyy^{-1})x(gyy^{-1})^{-1} = gxg^{-1} = x$$

이므로 $gyy^{-1} \in H$가 되어 H는 G의 정규부분군이다.

(별해) $H=\{g\in G\,|\,i_g: G\to G,\ x=i_g(x)=gxg^{-1},\ \forall x\in G\}=\{g\in G\,|\,xg=gx,\ \forall x\in G\}=Z(G)$가 되어 정리 3.3.23에 의하여 H는 G의 정규부분군이다.

3.3.25. $f^*: G/H\to G'/H'$, $f^*(aH)=f(a)H'$이라 정의하자. 잘 정의됨을 보이자.
원소 $aH, bH\in G/H$에 대하여

$$aH=bH \Rightarrow a^{-1}b\in H \Rightarrow f(a^{-1}b)\in f(H)\subset H' \Rightarrow f(a)^{-1}f(b)\in H' \Rightarrow f(a)H'=f(b)H'$$

이므로 f^*는 잘 정의된다. 임의의 원소 $aH, bH\in G/H$에 대하여

$$f^*(aH\cdot bH)=f^*(abH)=f(ab)H'=f(a)f(b)H'=f(a)H'f(b)H'=f^*(aH)f^*(bH)$$

이므로 f^*는 준동형사상이다.

3.3.26. 정수군 $G=H=\mathbb{Z}$, $K=2\mathbb{Z} \Rightarrow \mathbb{Z}\cong 2\mathbb{Z}$, $\mathbb{Z}/\mathbb{Z}\cong\{e\}\not\cong\mathbb{Z}_2\cong\mathbb{Z}/2\mathbb{Z}$,

3.3.27. G/N_1, G/N_2가 모두 가환군이면, 정리 3.3.28에 의하여 $C_G<N_1\cap N_2 \Rightarrow G/(N_1\cap N_2)$도 가환군이다.

3.3.28. $m=|G:H|=|G/H|$이므로 임의의 $a\in G$에 대하여 $H=(aH)^m=a^mH \Rightarrow a^m\in H$(정리 3.1.7)이다.

3.3.29. (1) 임의의 $A, B, C\in P(G)$에 대하여 $a\in A, b\in B, c\in C$에 대하여 $(ab)c=a(bc)$이므로

$$(ab)c\in(AB)C \Leftrightarrow a(bc)\in A(BC)$$
$$\therefore (AB)C=A(BC)$$

다음에 $\{e\}\in P(G)$에 대하여 분명히

$$\{e\}A=A\{e\}=A$$

이므로 $\{e\}$는 항등원이다. 따라서 $P(G)$는 단군이다.
하지만 항등원이 아닌 서로 다른 두 원소 집합 $\{a, b\}\in P(G)$에 대하여 $\{a, b\}A=\{e\}$인 $A\in P(G)$가 존재하려면 $a^{-1}, b^{-1}\in A$이어야 한다. 이때 $ab^{-1}\neq e \Rightarrow ab^{-1}\notin\{e\}$이므로 $ab^{-1}\in\{a, b\}A\neq\{e\}$이 되어 곱셈 역원이 존재하지 않는다. 따라서 $P(G)$는 군이 아니다.
(별해) 공집합 $\phi\in P(G)$는 역원이 존재하지 않으므로 군이 아니다.

(2) (참고: 두 집합 A, B의 곱에 대한 정리 3.3.11과 위 문제와의 차이점은 정리 3.3.11에서는 $AB=C$인 적당한 집합 C라 정의했지만 위 문제의 AB는 두 집합 A, B의 직접곱으로 정의된다.)
N이 G의 정규부분군이라 하자. $a, b\in G$에 대하여

$$anbn'\in(aN)(bN) \Rightarrow anbn'=abn''n'\in(ab)N \Rightarrow (aN)(bN)\subset(ab)N$$
$$abn\in(ab)N \Rightarrow abn=(ae)(bn)\in(aN)(bN) \Rightarrow (ab)N\subset(aN)(bN)$$

이므로 $(aN)(bN)=(ab)N$이다. 따라서 연산에 관하여 닫혀있다.

(3) 결합법칙은 (1)에서 증명했다. 항등원은

$$(aN)(eN)=(ae)N=aN$$
$$(eN)(aN)=(ea)N=aN$$

이므로 항등원 $eN=N$이 존재한다. 나머지 aN의 역원의 존재성을 증명하자. (2)에 의하여

$$(aN)(a^{-1}N)=(aa^{-1})N=eN=N$$
$$(a^{-1}N)(aN)=(a^{-1}a)N=eN=N$$

이므로 $(aN)^{-1}=a^{-1}N$이다. 그러므로 G에서 N의 잉여류들이 위의 연산아래서 군이 된다.
$P(G)$의 항등원은 $\{e\}$이고 잉여류의 항등원은 N으로 다르다.

3.3.30. (예 3.3.25와 예3.3.29, 정리 3.4.2 참조) $Z(\mathbb{Z}_3\times S_3)=\mathbb{Z}_3\times\{(1)\}$, $C_{\mathbb{Z}_3\times S_3}=\{1\}\times A_3$

3.3.31. (수정된 문제) 위수 $2n$(단, n은 소수)인 정이면체군 $D_n=<\sigma, \tau>$의 교환자부분군 C_{D_n}을 구하여라.
(풀이) 위수 n인 원소 $\sigma\in D_n$에 대하여 $\langle\sigma\rangle$은 순환부분군이고 $|D_n:\langle\sigma\rangle|=2$이므로 $\langle\sigma\rangle$은 정규부분군이다.

$D_n/\langle\sigma\rangle \cong \mathbb{Z}_2$은 가환군이고 D_n은 비가환군이므로 $\{e\} \neq C_{D_n} < \langle\sigma\rangle$이다(정리 3.3.28). n이 소수이므로 $C_{D_n} = \langle\sigma\rangle$이어야한다.

3.3.32. $|a| = n$, $\forall g \in G$에 대해서

$$a^n = e \Leftrightarrow e = gg^{-1} = ga^ng^{-1} = (gag^{-1})^n$$

이므로 $|a| = |gag^{-1}| \Rightarrow a = gag^{-1}$이다. 따라서 $ag = ga$ 이므로 $a \in Z(G)$ 이다.

(별해) $a \in Z(G)$임을 보이기 위해 $a = g^{-1}ag$, $\forall g \in G$임을 보이자. $|g^{-1}ag| = t$라 하자.

$a^n = e$이므로 $(g^{-1}ag)^n = g^{-1}a^ng = e \Rightarrow t|n$이다.

$(g^{-1}ag)^t = e \Rightarrow a^t = e \Rightarrow n|t$이다. 따라서 $n = t$이다.

이 때 위수가 n인 원소는 a뿐이므로 $a = g^{-1}ag$이다. 따라서 $a \in Z(G)$이다.

3.3.33. $|G| = pq$, p, q는 소수이다. G가 가환군인 아니면 $Z(G) = \{e\}$ 임을 보여라. [참조: 정리 3.3.27 이용]

(풀이) $Z(G) \triangleleft G$이므로 $|Z(G)| = 1, p, q, pq$이다.

$i)$ $|Z(G)| = p$ or q인 경우 $G/Z(G)$은 순환군이다. 따라서 G는 가환군이다(정리 3.3.24). 이는 가정에 모순이다.

$ii)$ $|Z(G)| = pq$인 경우 $Z(G) = G$이므로 $G/Z(G) \cong \{e\}$은 순환군이다. 따라서 G는 가환군이다(정리 3.3.24). 이는 가정에 모순이다.

따라서 $Z(G) = \{e\}$이다.

== 연습문제 (3.4) ==

3.4.1. 유한생성가환군의 정리에 의해

(1) $36 = 2^2 3^2$이므로 다음 4가지(지수의 수의 분할 (2,2), (1+1,2), (2,1+1), (1+1,1+1)의 종류와 일치)이다.

1) $\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \simeq \mathbb{Z}_{36}$,
2) $\mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3$,
3) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2}$,
40 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

(2) $72 = 2^3 \times 3^2$이므로 다음 6가지(지수의 수의 분할 (3,2), (3,1+1), (1+2,2), (1+2,1+1), (1+1+1,2), (1+1+1,1+1)의 종류와 일치)이다.

$\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \simeq \mathbb{Z}_{72}$,
$\mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_3$,
$\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2}$,
$\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3$,
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2}$,
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

(3) $100 = 2^2 \times 5^2$이므로 다음 4가지(지수의 수의 분할 (2,2), (1+1,2), (2,1+1), (1+1,1+1)의 종류와 일치)이다.

$\mathbb{Z}_{2^2} \times \mathbb{Z}_{5^2} \simeq \mathbb{Z}_{100}$,
$\mathbb{Z}_{2^2} \times \mathbb{Z}_5 \times \mathbb{Z}_5$,
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2}$,
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

(4) $250 = 2 \times 5^3$이므로 다음 3가지(지수의 수의 분할 (1,3), (1,1+2), (1,1+1+1)의 종류와 일치)이다.

$\mathbb{Z}_2 \times \mathbb{Z}_{5^3} \simeq \mathbb{Z}_{250}$,
$\mathbb{Z}_2 \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{5^2}$,
$\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

3.4.2. (수정된 문제) G가 위수 36인 가환군을 분류하고 각 가환군에 대하여 다음을 구하라.

(1) 각 G에서 위수 4인 원소의 개수를 구하라.

(2) 각 G에서 위수 6인 원소의 개수를 구하라.

(3) 각 G에서 위수 9인 원소의 개수를 구하라.

(풀이) 위 문제 3.4.1(1)에서 다음 4가지 경우가 존재한다.

1) $\mathbb{Z}_{2^2}\times\mathbb{Z}_{3^2}\simeq\mathbb{Z}_{36}$,

2) $\mathbb{Z}_{2^2}\times\mathbb{Z}_3\times\mathbb{Z}_3$,

3) $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_{3^2}$,

40 $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_3$

(1) 각 경우의 군에서 위수 4인 원소는 정리 3.4.8에 의하여 다음과 같다.

1) $(a,b)\in\mathbb{Z}_{2^2}\times\mathbb{Z}_{3^2}$에서 위수 4인 원소는 $4=\mathrm{lcm}(|a|,|b|)=\mathrm{lcm}(4,1)$인 경우를 구하면 된다.

따라서 위수 4인 원소는 (1,0), (3,0)로 2개이다.

2) $(a,b,c)\in\mathbb{Z}_{2^2}\times\mathbb{Z}_3\times\mathbb{Z}_3$에서 위수 4인 원소는 $4=\mathrm{lcm}(|a|,|b|,|c|)=\mathrm{lcm}(4,1,1)$인 경우를 구하면 된다.

따라서 위수 4인 원소는 (1,0,0), (3,0,0)로 2개이다.

3) $(a,b,c)\in\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_{3^2}$에서 위수 4인 원소는 $4=\mathrm{lcm}(|a|,|b|,|c|)$인 경우가 없으므로 0개이다.

4) $(a,b,c,d)\in\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_3$에서 위수 4인 원소는 $4=\mathrm{lcm}(|a|,|b|,|c|,|d|)$인 경우가 없으므로 0개이다.

(2) 각 경우의 군에서 위수 6인 원소는 정리 3.4.8에 의하여 다음과 같다.

1) $(a,b)\in\mathbb{Z}_{2^2}\times\mathbb{Z}_{3^2}$에서 위수 6인 원소는 $6=\mathrm{lcm}(|a|,|b|)=\mathrm{lcm}(2,3)$인 경우를 구하면 된다.

따라서 위수 4인 원소는 (2,3), (2,6)으로 2개이다.

2) $(a,b,c)\in\mathbb{Z}_{2^2}\times\mathbb{Z}_3\times\mathbb{Z}_3$에서 위수 6인 원소는 $6=\mathrm{lcm}(|a|,|b|,|c|)=\mathrm{lcm}(2,3,1)=\mathrm{lcm}(2,3,3)=\mathrm{lcm}(2,1,3)$인 경우를 구하면 된다.

따라서 위수 6인 원소는 (2,3,0), (2,6,0), (2,3,3), (2,3,6), (2,6,3), (2,6,6), (2,0,3), (2,0,6)로 8개이다.

3) $(a,b,c)\in\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_{3^2}$에서 위수 6인 원소는 $6=\mathrm{lcm}(|a|,|b|,|c|)=\mathrm{lcm}(2,1,3)=\mathrm{lcm}(2,2,3)=\mathrm{lcm}(1,2,3)$인 경우를 구하면 된다.

따라서 위수 6인 원소는 (1,0,3), (1,0,6), (1,1,3), (1,1,6), (0,1,3), (0,1,6)로 6개이다.

4) $(a,b,c,d)\in\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_3$에서 위수 6인 원소는

$6=\mathrm{lcm}(|a|,|b|,|c|,|d|)=\mathrm{lcm}(2,1,3,1)=\mathrm{lcm}(2,1,3,3)=\mathrm{lcm}(2,2,3,1)=\mathrm{lcm}(2,2,3,3)=\mathrm{lcm}(1,2,3,1)=\mathrm{lcm}(1,2,3,3)$인 경우를 구하면 된다.

따라서 위수 6인 원소는 (1,0,3,0), (1,0,6,0), (1,0,3,3), (1,0,3,6), (1,0,6,3), (1,0,6,6),
(1,1,3,0), (1,1,6,0), (1,1,3,3), (1,1,3,6), (1,1,6,3), (1,1,6,6),
(0,1,3,0), (0,1,6,0), (0,1,3,3), (0,1,3,6), (0,1,6,3), (0,1,6,6)
으로 18개이다.

3.4.3. **(1)** $|(4,9)|=\mathrm{lcm}(|4|,|9|)=\mathrm{lcm}\left(\frac{18}{\gcd(4,18)},\frac{18}{\gcd(9,18)}\right)=\mathrm{lcm}(9,2)=18$ **(정리 3.4.8)**

(2) $|(8,6,4)|=\mathrm{lcm}(|8|,|6|,|4|)=\mathrm{lcm}\left(\frac{18}{\gcd(8,18)},\frac{9}{\gcd(6,9)},\frac{8}{\gcd(4,8)}\right)=\mathrm{lcm}(9,3,2)=18$

(3) $|(8,6,4)|=\mathrm{lcm}(|8|,|6|,|4|)=\mathrm{lcm}\left(\frac{9}{\gcd(8,9)},\frac{17}{\gcd(6,17)},\frac{10}{\gcd(4,10)}\right)=\mathrm{lcm}(9,17,5)=765$

3.4.4. (1) $\mathbb{Z}_{24}$가 순환군이므로 $\frac{24}{\gcd(a,24)}=6$인 $\gcd(a,24)=4$인 $a\in\mathbb{Z}_{24}$를 구하면 된다.

따라서 $a=4,20$가 위수 6인 원소이다.

(2) $(a,b,c)\in\mathbb{Z}_{15}\times\mathbb{Z}_{18}\times\mathbb{Z}_{19}$에서 위수 18인 원소는 $18=\mathrm{lcm}(|a|,|b|,|c|)=\mathrm{lcm}(1,18,1)$인 경우를 구하면 된다.

따라서 위수 18인 원소는 $\phi(18)=6$개다(따름정리 2.3.12).

(3) $(a,b)\in\mathbb{Z}_2\times\mathbb{Z}_4$에서 위수 4인 원소는 $4=\mathrm{lcm}(|a|,|b|)=\mathrm{lcm}(1,4)=\mathrm{lcm}(2,4)$인 경우를 구하면 된다.

따라서 위수 4인 원소는 (0,1), (0,3), (1,1), (1,3)으로 4개이다.

위수 4인 부분군은 $\{0\}\times\mathbb{Z}_4$, $\mathbb{Z}_2\times 2\mathbb{Z}_4$, $\langle(1,1)\rangle$으로 3개이다.

(4) $\mathbb{Z}_2$와 $\mathbb{Z}_4$의 모든 원소는 유한 위수를 가진다. $\mathbb{Z}$에서 유한 위수를 가지는 원소는 0뿐이다.

따라서 $\mathbb{Z}_2\times\mathbb{Z}\times\mathbb{Z}_4$의 원소 중 유한 위수인 원소의 개수는 $2\times 1\times 4=8$(개) 이다.

$(a,b,c)\in\mathbb{Z}_2\times\mathbb{Z}\times\mathbb{Z}_4$에서 위수 4인 원소는 $4=\mathrm{lcm}(|a|,|b|,|c|)=\mathrm{lcm}(1,1,4)=\mathrm{lcm}(2,1,4)$인 경우를 구하면 된다.

따라서 위수 4인 원소는 (0,0,1), (0,0,3), (1,0,1), (1,0,3)으로 4개이다.

위수 4인 부분군은 $\{0\}\times\{0\}\times\mathbb{Z}_4$, $\mathbb{Z}_2\times\{0\}\times 2\mathbb{Z}_4$, $\langle(1,0,1)\rangle$으로 3개이다.

3.4.5. (1) $|\mathbb{Z}_2\times\mathbb{Z}_4|=8$이므로 라그랑주 정리에 의하여 위수 1, 2, 4, 8인 부분군이 존재한다(정리 3.4.15).

위수 1인 부분군 : $\{0\}\times\{0\}$으로 1개이다.

위수 2인 부분군 : $\mathbb{Z}_2\times\{0\}$, $\{0\}\times 2\mathbb{Z}_4$, $\langle(1,2)\rangle$으로 3개이다.

위수 4인 부분군은: $\{0\}\times\mathbb{Z}_4$, $\mathbb{Z}_2\times 2\mathbb{Z}_4$, $\langle(1,1)\rangle$으로 3개이다.

위수 8인 부분군은: $\mathbb{Z}_2\times\mathbb{Z}_4$으로 1개이다.

(2) $|\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2|=8$이므로 라그랑주 정리에 의하여 위수 1, 2, 4, 8인 부분군이 존재한다(정리 3.4.15).

위수 1인 부분군 : $\langle(0,0,0)\rangle$으로 1개이다.

위수 2인 부분군 : $\langle(1,0,0)\rangle$, $\langle(0,1,0)\rangle$, $\langle(0,0,1)\rangle$, $\langle(1,1,0)\rangle$, $\langle(1,0,1)\rangle$, $\langle(0,1,1)\rangle$, $\langle(1,1,1)\rangle$로 7개이다.

위수 4인 부분군은: $\{0\}\times\mathbb{Z}_2\times\mathbb{Z}_2$, $\mathbb{Z}_2\times\{0\}\times\mathbb{Z}_2$, $\mathbb{Z}_2\times\mathbb{Z}_2\times\{0\}$,

$\langle(1,1)\rangle\times\mathbb{Z}_2$, $\mathbb{Z}_2\times\langle(1,1)\rangle$, $\{(0,0,0),(1,0,1),(0,1,0),(1,1,1)\rangle$으로 6개이다.

위수 8인 부분군은: $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$으로 1개이다.

(3) $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_4$의 부분군 중 klein 4군과 동형인 군은 klein 4군과 대수적 구조가 같으면서 위수가 같아야 하므로 $\mathbb{Z}_2\times\mathbb{Z}_2$와 동형인 부분군이다. 따라서 klein 4원군과 동형인

$\mathbb{Z}_2\times\mathbb{Z}_2\times\{0\}$, $\mathbb{Z}_2\times\{0\}\times 2\mathbb{Z}_4$, $\{0\}\times\mathbb{Z}_2\times 2\mathbb{Z}_4$

$\langle(1,1)\rangle\times 2\mathbb{Z}_4$, $\mathbb{Z}_2\times\langle(1,2)\rangle$, $\{(0,0,0),(1,0,2),(0,1,0),(1,1,2)\rangle$

이다.

3.4.6. 따름정리 3.4.7을 이용하여 서로소인 인수로 분해하자.

(1) $\mathbb{Z}_2\times\mathbb{Z}_{12}\cong\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_4$이고 $\mathbb{Z}_4\times\mathbb{Z}_6\cong\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_3$이므로 동형이다.

(2) $\mathbb{Z}_8\times\mathbb{Z}_{10}\times\mathbb{Z}_{24}\cong\mathbb{Z}_8\times\mathbb{Z}_2\times\mathbb{Z}_5\times\mathbb{Z}_3\times\mathbb{Z}_8$이고

$\mathbb{Z}_4\times\mathbb{Z}_{12}\times\mathbb{Z}_{40}\cong\mathbb{Z}_4\times\mathbb{Z}_3\times\mathbb{Z}_4\times\mathbb{Z}_5\times\mathbb{Z}_8$이므로 동형이 아니다. 위수 8인 원소의 개수가 다르다.

3.4.7. $d=\gcd(m,n)$, $l=\mathrm{lcm}(m,n)$이라 하자. 그리고 $m=dm'$, $n=dn'$이라고 하면 $l=dm'n'$이고 $m\,||G|$, $n\,||G|$이다. $|G|=nx$라 하자. 그러면

$$dm'|dn'x \Rightarrow m'|n'x \Rightarrow m'|x\,(\because \gcd(m',n')=1)$$

이다. 그러므로

$$|G|=nxdn'x=dn'm'x'=lx' \Rightarrow l\,||G|$$

이므로 정리 3.4.15에 의하여 위수가 $\mathrm{lcm}(m,n)$인 G의 부분군 존재한다.

(별해) $d=\gcd(m,n)$, $l=\mathrm{lcm}(m,n)$이라 하자. $|H|=m$, $|K|=n$이라 하자.

G가 가환군이므로 $H\triangleleft G, K\triangleleft G$이다. 정리 3.3.6에 의하여 $HK\triangleleft G$이다. $|H\cap K|\,||H|$이고 $|H\cap K|\,||K|$이므로 $|H\cap K|\mid\gcd(m,n)\Rightarrow d=|H\cap K|d'$이다. 한편 정리 3.1.14에 의하여

$$|HK|=\frac{|H||K|}{|H\cap K|}=\frac{mn}{\frac{d}{d'}}=\frac{dm'dn'd'}{d}=dm'n'd'=ld'$$

이다. 그러므로

$$l \mid |HK|,\ |HK| \mid |G| \Rightarrow l \mid |G|$$

이므로 정리 3.4.15에 의하여 위수가 $\mathrm{lcm}(m,n)$인 G의 부분군 존재한다.

3.4.8. 유한생성 가환군의 기본 정리에 의하여 위수 m인 동형이 아닌 가환군을 $H_1, \cdots, H_r$이라 하고 위수 n인 동형이 아닌 가환군을 $K_1,\cdots,K_s$라 하자. 그러면 $H_i \times K_j$는 위수 mn인 가환군이다. $\gcd(m,n)=1$이므로 위수가 mn이고 $H_i \times K_j$와 동형인 것은 rs개가 존재한다.

3.4.9. (1) 임의의 $(h,k) \in G$에 대하여 $(h,k)=(h,e)(e,k) \in HK$이다.
(2) $(h,e)(e,k)=(h,k)=(e,k)(h,e)$
(3) $(h,e)=(e,k) \in H \cap K \Rightarrow h=k=e \Rightarrow H \cap K=\{(e,e)\}$

3.4.10. $\gcd(m,n)=1 \Leftrightarrow \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$(정리 3.4.6)을 이용하자.
($\Rightarrow$) 유한가환군 G이 순환군이 아니라 하자. 유한생성가환군의 정리에 의하여
$G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$이고 $\gcd(m_1,m_2)=d>1$인 m_1, m_2가 존재한다.
d의 소인수 p를 생각하면 $p|d, p|m, p|n$이다. 그러므로 $\mathbb{Z}_p < \mathbb{Z}_{m_1}$, $\mathbb{Z}_p < \mathbb{Z}_{m_2}$이므로
G는 $\mathbb{Z}_p \times \mathbb{Z}_p$와 동형인 부분군을 포함한다.
($\Leftarrow$) G는 $\mathbb{Z}_p \times \mathbb{Z}_p$와 동형인 부분군을 포함한다고 하자.
G가 순환군이면 부분군도 순환군이다(정리 2.3.5). 하지만 $\mathbb{Z}_p \times \mathbb{Z}_p$는 순환부분군이 아니므로 G는 순환군이 아니다.
(별해) G가 순환군이면 서로 다른 위수 p인 순환부분군 $\mathbb{Z}_p \times \{0\}, \{0\} \times \mathbb{Z}_p$을 가지므로 순환부분군의 유일성(정리 2.3.11)에 모순이다. 따라서 G는 순환군이 아니다.

3.4.11. 유한 생성가환군의 기본 정리에 의하여 $G \times K$와 $H \times K$는 동형인 순환군의 같은 개수의 직접곱으로 이루어져있다. 따라서 부분군으로 같은 K를 가지고 있으므로 G와 H는 동형이어야 한다.

3.4.12. 유한생성가환군의 정리에 의해
$G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_r^{a_r}}$, p_i는 소수, $a_i > 0$이고
$H < G$이므로 $H \cong \mathbb{Z}_{p_1^{b_1}} \times \mathbb{Z}_{p_2^{b_2}} \times \cdots \times \mathbb{Z}_{p_r^{b_r}}$, $0 \le b_i \le a_i$ 이다. (정리 3.5.6 참조)

$$G/H = \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_r^{a_r}} / \mathbb{Z}_{p_1^{b_1}} \times \mathbb{Z}_{p_2^{b_2}} \times \cdots \times \mathbb{Z}_{p_r^{b_r}} \simeq \mathbb{Z}_{p_1^{a_1}}/\mathbb{Z}_{p_1^{b_1}} \times \mathbb{Z}_{p_2^{a_2}}/\mathbb{Z}_{p_2^{b_2}} \times \cdots \times \mathbb{Z}_{p_r^{a_r}}/\mathbb{Z}_{p_r^{b_r}}$$

이 때 $\mathbb{Z}_{p_r^{a_i}}$와 $\mathbb{Z}_{p_r^{b_i}}$는 순환군이고 $\left|\mathbb{Z}_{p_i^{a_i}}/\mathbb{Z}_{p_i^{b_i}}\right| = \dfrac{\left|\mathbb{Z}_{p_r^{a_i}}\right|}{\left|\mathbb{Z}_{p_r^{b_i}}\right|} = \left|\mathbb{Z}_{p_i^{a_i-b_i}}\right|$이므로 $\mathbb{Z}_{p_i^{a_i}}/\mathbb{Z}_{p_i^{b_i}} \cong \mathbb{Z}_{p_i^{a_i-b_i}}$이다.

$$G/H \simeq \mathbb{Z}_{p_1^{a_1-b_1}} \times \cdots \times \mathbb{Z}_{p_i^{a_r-b_r}} = K < G$$

3.4.13. $36=4 \cdot 9$이므로 $\mathbb{Z}_{36}=4\mathbb{Z}_{36} \oplus 9\mathbb{Z}_{36}$이다.

== 연습문제 (3.5) ==

3.5.1. (1) $K=\{a \in \mathbb{Z}_{12} \mid 0=f(a)=2a(\mathrm{mod}\ 3)\}=\{a \in \mathbb{Z}_{12} \mid 0=a(\mathrm{mod}\ 3)\}=\{0, 3, ,6, 9\}$이다.
(2) $0+K=\{0, 3, 6, 9\}$, $1+K=\{1, 4, 7, 10\}$, $2+K=\{2, 5, 8, 11\}$
(3) $|\mathbb{Z}_{12}/K|=3 \Rightarrow \mathbb{Z}_{12}/K \cong \mathbb{Z}_3$(예 2.1.15(3))이므로 제1동형정리가 성립한다.

3.5.2. (1) $H=\langle 4 \rangle=\{0,4,8,12,16,20\}$, $N=\langle 6 \rangle=\{0,6,12,18\}$이므로

$HN = \langle 2 \rangle = \{0,2,4,6,8,10,12,14,16,18,20,22\}$, $H \cap N = \langle 12 \rangle = \{0,12\}$

(2) $HN/N = \{0+N, 2+N, 4+N\}$

(3) $H/(H \cap N) = \{0+H \cap N,\ 4+H \cap N,\ 8+H \cap N\}$

(4) 위수 3인 가환군은 $\mathbb{Z}_3$과 동형이다. 따라서 $HN/N \cong \mathbb{Z}_3 \cong H/(H \cap N)$이다. 따라서 제2동형정리가 성립한다.

3.5.3. $H = \langle 4 \rangle = \{0,4,8,12,16,20\}$, $N = \langle 8 \rangle = \{0,8,16\}$이므로

(1) $G/H = \{H,\ 1+H,\ 2+H,\ 3+H\}$

(2) $G/N = G = \{N,\ 1+N,\ 2+N,\ 3+N,\ 4+N,\ 5+N,\ 6+N,\ 7+N\}$

(3) $H/N = \{0+N,\ 4+N\}$

(4) $(G/N)/(H/N) = \{0+N+H/N,\ 1+N+H/N,\ 2+N+H/N,\ 3+N+H/N\}$

(5) $|G/H| = |(G/N)/(H/N)| = 4$이고 모두 순환군이므로 $G/H \cong \mathbb{Z}_4 \cong (G/N)/(H/N)$이다.

따라서 제3동형정리가 성립한다.

3.5.4. 임의의 $x, y \in U$에 대하여

$$f(xy) = (xy)^n = x^n y^n = f(x)f(y)$$

이므로 준동형사상이다. 또한 임의의 $x \in U$에 대하여 $f\left(x^{\frac{1}{n}}\right) = x$이므로 전사함수이다. 그리고

$$\ker(f) = \{x \in U \mid 1 = f(x) = x^n\} = \left\{ e^{\frac{2\pi i}{n}} \;\middle|\; n = 0,1,\cdots,n-1 \right\} = U_n$$

이므로 제1동형정리에 의하여 $U/U_n = U/\ker(f) \cong Im(f) = U$이다.

3.5.5. 정리 3.2.23에 의하여 $K \triangleleft G$이다. 그러면 정리 3.5.10에 의하여 $(H \cap K) \triangleleft H$이다. f의 H로의 제한 사상

$$f|_H : H \to f(H),\ f|_H(h) = f(h)$$

를 생각하면 $\ker(f|_H) = \{h \in H \mid e = f|_H(h) = f(h)\} = H \cap K$이고 분명히 전사함수이므로 제1동형정리에 의하여

$$H/(H \cap K) = H/\ker(f|_H) \cong Im(f|_H) = f(H)$$

이다.

3.5.6. 함수 $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_3,\ f(a,b) = (2a-b,\ [a]_3)$이라 정의하자. 그러면 임의의 $(a,b) \in \mathbb{Z} \times \mathbb{Z}_3$에 대하여 $f(b, 2b-a) = (2b-(2b-a), [b]_3) = (a,b)$이므로 전사함수이다.

$\ker(f) = \{(a,b) \mid (0,0) = f(a,b) = (2a-b, [a]_3)\} = \{(a,b) \mid a = 3x,\ 2a = b\} = \{(3x,6x) \mid x \in \mathbb{Z}\} = \langle (3,6) \rangle$

이다. 다음에 임의의 (a,b), $(a',b') \in \mathbb{Z} \times \mathbb{Z}$에 대하여

$f((a,b)+(a',b')) = f(a+a', b+, b') = (2(a+a') - (b+b'),\ [a+a']_3) = (2a-b,\ [a]_3) + (2a'-b',\ [a']_3) = f(a,b) + f(a',b')$

이므로 준동형사상이다. 따라서 제1동형정리에 의하여

$$(\mathbb{Z} \times \mathbb{Z})/N = (\mathbb{Z} \times \mathbb{Z})/\ker(f) \cong Im(f) = \mathbb{Z} \times \mathbb{Z}_3$$

이다.

3.5.7. 함수 $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},\ f(x,y) = bx - ay$라 정의하자. 그러면 a, b가 서로소인 정수이므로 $ar + bs = 1$인 정수 $r, s \in \mathbb{Z}$가 존재한다. 임의의 $x \in \mathbb{Z}$에 대하여 $arx + bsx = x$이므로 $f(sx,\ -rx) = b(sx) - a(-rx) = arx + bsx = x$이므로 전사함수이다.

$$\ker(f) = \{(x,y) \mid 0 = f(x,y) = bx - ay\} = \{(x,y) \mid bx = ay\} = \{(ax,bx) \mid x \in \mathbb{Z}\} = \langle (a,b) \rangle$$

이다. 다음에 임의의 (x,y), $(x',y') \in \mathbb{Z} \times \mathbb{Z}$에 대하여

$$f((x,y)+(x',y')) = f(x+x', y+, y') = b(x+x') - a(y+y') = (bx-ay) + (bx'-ay') = f(x,y) + f(x',y')$$

이므로 준동형사상이다. 따라서 제1동형정리에 의하여

$$(\mathbb{Z} \times \mathbb{Z})/N = (\mathbb{Z} \times \mathbb{Z})/\ker(f) \cong Im(f) = \mathbb{Z}$$

이다.

== 연습문제 (3.6) ==

3.6.1. 함수 $f:\mathbb{Z}_4\times\mathbb{Z}_8\to\mathbb{Z}_2\times\mathbb{Z}_8,\ f(a,b)=([a]_2,\ 2a-b)$이라 정의하자. 그러면 임의의 $(a,b)\in\mathbb{Z}_2\times\mathbb{Z}_8$에 대하여 $f(a,\ 2a-b)=([a]_2,\ 2a-(2a-b))=(a,b)$이므로 전사함수이다.

$$\ker(f)=\{(a,b)\mid(0,0)=f(a,b)=([a]_2,\ 2a-b))\}=\{(a,b)\mid a=2x,\ 2a=b\}=\{(2x,4x)\mid x\in\mathbb{Z}\}=\langle(2,4)\rangle$$

이다. 다음에 임의의 $(a,b),\ (a',b')\in\mathbb{Z}\times\mathbb{Z}$에 대하여

$$f((a,b)+(a',b'))=f(a+a',b+,b')=([a+a']_2,\ 2(a+a')-(b+b'))=([a]_2,2a-b)+([a']_2,2a'-b')=f(a,b)+f(a',b')$$

이므로 준동형사상이다. 따라서 제1동형정리에 의하여

$$(\mathbb{Z}\times\mathbb{Z})/\langle(2,4)\rangle=(\mathbb{Z}\times\mathbb{Z})/\ker(f)\cong Im(f)=\mathbb{Z}_2\times\mathbb{Z}_8$$

이다.

3.6.2. 함수 $f:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}_2,\ f(a,b)=(2a-b,\ [a]_2)$이라 정의하자. 그러면 임의의 $(a,b)\in\mathbb{Z}\times\mathbb{Z}_2$에 대하여 $f(b,\ 2b-a)=(2b-(2b-a),[b]_2)=(a,b)$이므로 전사함수이다.

$$\ker(f)=\{(a,b)\mid(0,0)=f(a,b)=(2a-b,[a]_2)\}=\{(a,b)\mid a=2x,\ 2a=b\}=\{(2x,4x)\mid x\in\mathbb{Z}\}=\langle(2,4)\rangle$$

이다. 다음에 임의의 $(a,b),\ (a',b')\in\mathbb{Z}\times\mathbb{Z}$에 대하여

$$f((a,b)+(a',b'))=f(a+a',b+,b')=(2(a+a')-(b+b'),\ [a+a']_2)=(2a-b,\ [a]_2)+(2a'-b',\ [a']_2)=f(a,b)+f(a',b')$$

이므로 준동형사상이다. 따라서 제1동형정리에 의하여

$$(\mathbb{Z}\times\mathbb{Z})/\langle(2,4)\rangle=(\mathbb{Z}\times\mathbb{Z})/\ker(f)\cong Im(f)=\mathbb{Z}\times\mathbb{Z}_2$$

이다.

3.6.3. 유한생성 가환군의 기본정리에 따라 다음 주어진 군을 분류하라.

(1) $|<(0,\ 1)>|=4\ \Rightarrow\ |(\mathbb{Z}_2\times\mathbb{Z}_4)/<(0,\ 1)>|=2$이고 $|(1,1)+<(0,1)>|=2$이므로 $(\mathbb{Z}_2\times\mathbb{Z}_4)/<(0,\ 1)>\cong\mathbb{Z}_2$

(2) $|<(1,2)>|=2\ \Rightarrow\ |(\mathbb{Z}_2\times\mathbb{Z}_4)/<(1,\ 2)>|=4$이고 $|(1,1)+<(1,2)>|=4$이므로 $(\mathbb{Z}_2\times\mathbb{Z}_4)/<(1,\ 2)>\cong\mathbb{Z}_4$

(3) $|<(1,2)>|=12\ \Rightarrow\ |(\mathbb{Z}_4\times\mathbb{Z}_6)/<(1,\ 2)>|=2$이고 $|(1,1)+<(1,2)>|=2$이므로 $(\mathbb{Z}_4\times\mathbb{Z}_6)/<(1,\ 2)>\cong\mathbb{Z}_2$

(4) $<(1,\ 2)>\cong\mathbb{Z}$을 참조(연습문제 3.5.7)하면 $(\mathbb{Z}\times\mathbb{Z})/<(1,\ 2)>\cong\mathbb{Z}$

(5) (문제 수정) $|<(1,2)>|=4\ \Rightarrow\ |(\mathbb{Z}_4\times\mathbb{Z}_8)/<(1,\ 2)>|=8$이고

$|(1,1)+<(1,2)>|=8$이므로 $(\mathbb{Z}_4\times\mathbb{Z}_8)/<(1,\ 2)>\cong\mathbb{Z}_8$

(6) $|<(1,3)>|=8\ \Rightarrow\ |(\mathbb{Z}_4\times\mathbb{Z}_8)/<(1,\ 3)>|=4$이고 $|(0,1)+<(1,3)>|=4$이므로 $(\mathbb{Z}_4\times\mathbb{Z}_8)/<(1,\ 3)>\cong\mathbb{Z}_4$

(7) $|<(1,\ 2,\ 3)>|=8\ \Rightarrow\ |(\mathbb{Z}_4\times\mathbb{Z}_4\times\mathbb{Z}_8)/<(1,\ 2,\ 3)>|=16$이고 위수 8, 16인 원소가 없고 $|(1,1,1)+<(1,2,3)>|=4$이므로 잉여군은 $\mathbb{Z}_4\times\mathbb{Z}_4,\ \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_4$중의 하나와 동형이다. 잉여군의 위수가 2인 것이 $\mathbb{Z}_4\times\mathbb{Z}_4$는 3개 $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_4$는 4개 이상이다. 잉여군의 원소 중

$$|(2,0,0)+<(1,2,3)>|=|(2,2,0)+<(1,2,3)>|=|(2,2,4)+<(1,2,3)>|=|(0,2,0)+<(1,2,3)>|=2$$

의 위수가 2이므로 $(\mathbb{Z}_4\times\mathbb{Z}_4\times\mathbb{Z}_8)/<(1,\ 2,\ 3)>\cong\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_4$이다.

(8) $<(3,3,3)>\cong 3\mathbb{Z}$을 참조.

함수 $f:\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}_3,\ f(x,y,z)=(x-y,\ x-z,\ [x]_3)$라 정의하자. 그러면 임의의 $(a,b,c)\in\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}_3$에 대하여 $f(c,\ c-a,\ c-b)=(c-(c-a),\ c-(c-b),\ [c]_3)=(a,b,c)$이므로 전사함수이다.

$$\ker(f)=\{(a,b,c)\mid(0,0,0)=f(a,b,c)=(a-b,a-c,[a]_3)\}=\{(a,b,c)\mid a=3x,\ a=b=c\}=\{(3x,3x.3x)\mid x\in\mathbb{Z}\}=\langle(3,3,3)\rangle$$

이다. 다음에 임의의 $(a,b,c),\ (a',b',c')\in\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$에 대하여

$$f((a,b,c)+(a',b',c'))=f(a+a',b+,b',c+c')=((a+a')-(b+b'),\ (a+a')-(c+c'),\ [a+a']_3)$$
$$=(a-b,\ a-c,\ [a]_3)+(a'-b',\ a'-c',\ [a']_3)=f(a,b,c)+f(a',b',c')$$

이므로 준동형사상이다. 따라서 제1동형정리에 의하여

$$(\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z})/\langle(3,3,3)\rangle=(\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z})/\ker(f)\cong Im(f)=\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}_3$$

이다.

== 연습문제 (4.1) ==

4.1.1. $G_y \subseteq gG_xg^{-1}$, $G_y \supseteq gG_xg^{-1}$ 임을 보이자.

$a \in G_y$ 이면

$$ay = y \implies agx = gx \implies (g^{-1}ag)x = (g^{-1}g)x = ex = x \implies g^{-1}ag \in G_x \implies a \in g^{-1}G_xg$$

이다. 따라서 $G_y \subseteq gG_xg^{-1}$

$b \in gG_xg^{-1}$ 이면 $b = gag^{-1}$, 적당한 $a \in G_x$가 존재하여 $ax = x$이다.

$$bg = ga \implies bgx = gax = gx \implies by = y$$

이다. $b \in G_y$이다. 따라서 $G_y \supseteq gG_xg^{-1}$이므로 $G_y = gG_xg^{-1}$이다.

4.1.2. 항등원$e \in G$는 모든$y \in Y$에 대해 $ey = y$를 만족하므로 $e \in G_Y$이고,

모든$g, h \in G_Y$에 대해 ($gy = y$이면 $y = g^{-1}y$이다) $(gh^{-1})y = g(h^{-1}y) = gy = y$이므로 $gh^{-1} \in G_Y$이다. 따라서 G_Y는 G의 부분군이다.

4.1.3.

$(D_4)_C = D_4$,
$(D_4)_1 = \{\rho_0, \delta_1\}$
$(D_4)_2 = \{\rho_0, \delta_2\}$
$(D_4)_3 = \{\rho_0, \delta_1\}$
$(D_4)_4 = \{\rho_0, \delta_2\}$

$(D_4)_{P_1} = \{\rho_0, y\}$
$(D_4)_{P_2} = \{\rho_0, x\}$
$(D_4)_{P_3} = \{\rho_0, y\}$
$(D_4)_{P_4} = \{\rho_0, x\}$

$(D_4)_{x'} = \{\rho_0, \rho_2, x, y\}$
$(D_4)_{y'} = \{\rho_0, \rho_2, x, y\}$
$(D_4)_{\delta_1} = \{\rho_0, \rho_2, \delta_1, \delta_2\}$
$(D_4)_{\delta_2} = \{\rho_0, \rho_2, \delta_1, \delta_2\}$

$(D_4)_{s_1} = \{\rho_0, y\}$
$(D_4)_{s_2} = \{\rho_0, x\}$
$(D_4)_{s_3} = \{\rho_0, y\}$
$(D_4)_{s_4} = \{\rho_0, x\}$

4.1.4. (수정된 문제) 유한군 G에서 원소 x를 포함하는 켤레류 $C_x = \{gxg^{-1} \mid g \in G\}$에 꼭 두 개의 원소가 존재하면, $G_x \triangleleft G$, $\{e\} \subsetneq G_x \subsetneq G$임을 밝혀라.

(풀이) $C_x = \{gxg^{-1} \mid g \in G\}$이고 $G_x = \{g \in G \mid gxg^{-1} = x\}$이므로 정리 4.1.10에 의하여

$$|G : G_x| = |C_x| = 2$$

이다. 따라서 $G_x \triangleleft G$이다.

또한 $G_e = \{g \in G \mid geg^{-1} = e\} = G \neq G_x$이므로 $x \neq e$이다. 그리고 $x \in G_x$이므로 $\{e\} \subsetneq G_x \subsetneq G$이다.

4.1.5. 유한군 G가 두 개의 켤레류 $C_1 = \{e\}$, C_2를 가진다고 하자. 그러면 따름정리 4.1.15에 의하여

$$|G| = |C_1| + |C_2| = 1 + |C_2| \implies |C_2| = |G| - 1$$

이다. 또한 정리 4.1.10에 의하여 $|C_2| \mid |G|$이므로 $|C_2| = 1$이고 $|G| = 2$이다.

4.1.6. (1) (예 4.1.16(2)번 참조) 모든 $x \in S_4$에 대하여, x가 우치환(기치환)이면, gxg^{-1}도 우치환(기치환)이므로, S_4-궤도(켤레류)는 다음과 같은 5가지이고, 각각의 원소수는 $|S_4| = 24$의 약수이다.

$C_{(1)} = \{(1)\}$
$C_{(a\,b)} = \{(12),(13),(14),(23),(24),(34)\}$, $a \neq b$
$C_{(a\,b\,c)} = \{(123),(132),(124),(142),(134),(143),(234),(243)\}$, a,b,c는 서로다름
$C_{(a\,b)(c\,d)} = \{(12)(34),(13)(24),(14)(23)\}$, $a \neq b$, $c \neq d$
$C_{(a\,b\,c\,d)} = \{(1234),(1324),(1342),(1423),(1432)\}$, a,b,c,d는 서로다름

(2)
$C_1 = \{1\}$
$C_{-1} = \{-1\}$
$C_i = C_{-i} = \{i, -i\}$
$C_j = C_{-j} = \{j, -j\}$
$C_k = C_{-k} = \{k, -k\}$

(3) $D_4 = \langle \sigma = (1234), \tau = (24) \rangle = \langle 1, \sigma, \sigma^{2,} \sigma^{3,} \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau \rangle$라 할 때 켤레류는 다음과 같다.

$C_1 = \{1\}$
$C_{\sigma^2} = \{\sigma^2\}$
$C_\sigma = C_{\sigma^3} = \{\sigma, \sigma^3\}$
$C_\tau = C_{\sigma^2\tau} = \{\tau, \sigma^2\tau\}$
$C_{\sigma\tau} = C_{\sigma^3\tau} = \{\sigma\tau, \sigma^3\tau\}$

== 연습문제 (4.2) ==

4.2.1. S_4, S_5의 실로우 2-부분군과 실로우 3-부분군을 각각 구하여라.

(풀이) $|S_4| = 24 = 2^3 \cdot 3$이므로 S_4의 실로우 2-부분군의 위수는 8이고, 다음 3개(실로우 3정리에 의해 1개 또는 3개 존재가능)의 실로우2-부분군이 존재한다.

$D_4 = \langle \sigma = (1234), \tau = (13) \rangle = \langle (1), (1234), (13)(24), (1432), (12)(34), (13), (14)(23), (24) \rangle$
$(12)D_4(12)^{-1} = \langle (1342), (14) \rangle$
$(14)D_4(14)^{-1} = \langle (1423), (12) \rangle$

S_4의 실로우 3-부분군은 위수가 3이므로 다음과 같은 4개(실로우 3정리에 의해 1개 또는 4개 존재가능)가 존재한다.

$P_1 = \langle (123) \rangle = \langle (1), (123), (132) \rangle$
$P_1 = \langle (124) \rangle = \langle (1), (124), (142) \rangle$
$P_2 = \langle (134) \rangle = \langle (1), (134), (143) \rangle$
$P_1 = \langle (234) \rangle = \langle (1), (234), (243) \rangle$

$|S_5| = 120 = 2^3 \cdot 3 \cdot 5$이므로 S_5의 실로우 2-부분군의 위수는 8이고, 다음 15개(실로우 3정리 1개 또는 3개, 5개, 15개 존재가능)의 실로우2-부분군이 존재한다.

$\langle (1234), (13) \rangle, \langle (1342), (14) \rangle, \langle (1423), (12) \rangle,$
$\langle (1235), (13) \rangle, \langle (1352), (15) \rangle, \langle (1523), (12) \rangle,$
$\langle (1245), (14) \rangle, \langle (1452), (15) \rangle, \langle (1524), (12) \rangle,$
$\langle (1345), (14) \rangle, \langle (1453), (15) \rangle, \langle (1534), (13) \rangle,$
$\langle (2345), (24) \rangle, \langle (2453), (25) \rangle, \langle (2534), (23) \rangle$

S_5의 실로우 3-부분군은 위수가 3이고 다음 10개(실로우 3정리 1개 또는 4개, 10개, 40개 존재가능)의 실로우2-부분군이 존재한다. 실로우 3-부분군이 40개이면 실로우 2-부분군, 실로우 5-부분군과의 원소수의 합이 120을 초과하므로 실로우 3-부분군이 40개는 불가능.

$\langle (123) \rangle, \langle (124) \rangle, \langle (125) \rangle, \langle (134) \rangle, \langle (135) \rangle, \langle (145) \rangle, \langle (234) \rangle, \langle (235) \rangle, \langle (245) \rangle, \langle (345) \rangle$

4.2.2. (1) $|S_3 : H| = 2 \Rightarrow H \lhd S_3 \Rightarrow S_3 \subset N_{S_4}(H)$이다. 그리고

$$(421)(123)(421)^{-1} = (421)(123)(412) = (134) \notin H$$

이므로 $S_4 \not\subset N_{S_4}(H)$이다. 한편 정리 4.2.10에 의하여

$$|N_{S_4}(H) : H| \equiv |S_4 : H| \equiv 8 \equiv 2 (\mathrm{mod}\ 3)$$

이므로

$$|N_{S_4}(H)| = |H| \cdot 2 = 6 \ \text{ or } \ |H| \cdot 5 = 15 \ \text{ or } \ |H| \cdot 8 = 24$$

이다. 이중 가능한 경우는 $|N_{S_4}(H)| = |H| \cdot 2 = 6$이다. 따라서 $N_{S_4}(H) = S_3$이다.

(2) 연습문제 4.2.1에 의하여 S_4의 실로우-3부분군은 (123), (124), (134), (234)이다.

$(1)(123)(1)^{-1}=(12)(123)(12)^{-1}=(123)$ 이므로 $(12)H(12)^{-1}=\langle(123)\rangle$
$(34)(123)(34)^{-1}=(124)$ $(34)H(34)^{-1}=\langle(124)\rangle$
$(24)(123)(24)^{-1}=(134)$ $(24)H(24)^{-1}=\langle(134)\rangle$
$(14)(123)(14)^{-1}=(234)$ $(14)H(14)^{-1}=\langle(234)\rangle$

4.2.3. $45=3^2\times5$이고 sylow 3-부분군의 개수를 r개라 하자. sylow 3정리에 의하여

$$\begin{cases} r\equiv 1(\mathrm{mod}\,3) \\ r\mid 45 \end{cases}$$ 이므로 $r=1$

따라서 sylow 3-부분군은 1개 존재하므로 정규부분군이 된다(정리 4.2.14). 또한 실로우3-부분군은 위수가 9이므로 위수가 9인 정규부분군이 존재한다.

4.2.4. $(35)^3=5^3\cdot 7^3$이므로 위수 125인 실로우 5-부분군이 존재한다. 실로우 3정리에 의하여 실로우 5-부분군은 1개가 존재하여 정리 4.2.14에 의하여 실로우 5-부분군은 정규부분군이다.

4.2.5. (1) $|G|=36=2^2\times3^2$ 이고 $\forall g\in G, |g|=2^r3^s\ (r,s=0,1,2)$

$\gcd(2^r,3^s)=1\Leftrightarrow 2^rx+3^sy=1$인 $\exists x,y\in\mathbb{Z}$ 그러면 $g=g^1=g^{2^rx+3^sy}=g^{2^r}\cdot g^{3^s}$이고

$$\left|g^{2^rx}\right|=\frac{2^r3^r}{\gcd(2^rx,2^r3^s)}=\frac{2^r3^s}{2^r}=3^s\ (\because \gcd(x,3)=1)$$

$$\left|g^{3^sy}\right|=\frac{2^r3^r}{\gcd(3^sy,2^r3^s)}=\frac{2^r3^s}{3^s}=2^r\ (\because \gcd(y,2)=1)$$

$a=g^{2^r}$, $b=g^{3^s}$라 하면, $g=ab$이고 $|a||9, |b||4$이다.

(2) 실로우 3정리에 의하여 실로우 2, 3-부분군 A, B가 존재한다. 그러면

$|A\cap B|\,|\gcd(|A|,|B|)=\gcd(4,9)=1\Rightarrow |A\cap B|=1\Rightarrow A\cap B=\{e\}$

이다. 그리고 정리 3.1.14에 의하여

$$36=|G|\geq|AB|=\frac{|A||B|}{|A\cap B|}=|A||B|=4\times9=36$$

이므로 $|G|=|AB|$이고 $G=AB$이다.

4.2.6. 실로우 1정리에 의하여 H는 sylow p-군 임을 알 수 있다.

sylow 3정리에 의해 sylow p-군의 개수는 1개이다. ($\because p>n$이므로, $\gcd(p,n)=1$)

따라서 $H\lhd G$이다(정리 4.2.14).

4.2.7. 실로우 1정리에 의해 실로우 p-부분군 H가 존재해서 $|H|=p^n$이고 $|G:H|=q$이다. 이 때 실로우 p-부분군의 개수는 실로우 3정리에 의해 $p>q$이므로 1개로 유일하게 존재한다. 따라서 $H\lhd G$이다(정리 4.2.14). 따라서 지수 q인 정규부분군이 유일하게 존재한다.

4.2.8. ($\Rightarrow$) 유한군 G가 p-군이고 $|G|=p^rm$(단, $\gcd(p,m)=1$)이라 하자. 만약 $m>1$이면 m의 소인수 $(p\neq)q$가 존재하여 $q|G$이다. 그러면 코시정리 (4.2.3)에 의하여 위수 q인 부분군이 존재한다. 이는 위수가 p가 아닌 원소가 존재하므로 가정에 모순이다. 따라서 $m=1$이고 G의 위수는 p^r이어야 한다.

($\Leftarrow$) G의 위수는 p^r이면 라그랑주의 정리에 의하여 G의 모든 원소의 위수는 p^r의 약수이다. 따라서 G는 p-군이다.

4.2.9. (1) 정리 3.2.21에 의하여 $H\cong gHg^{-1}$이므로 $|H|=|gHg^{-1}|$이다.

(2) 임의의 $g\in G$에 대하여, H의 켤레부분군 gHg^{-1}에 대하여 $|H|=|gHg^{-1}|$이므로 유일성의 의하여 $H=gHg^{-1}$이

다. 따라서 $H \triangleleft G$이다.

4.2.10. $|N| = p^a, |G/N| = p^b$라 하자. $N < G$이므로

$$p^b = |G/N| = \frac{|G|}{|N|} = \frac{|G|}{p^a} \Rightarrow |G| = p^{a+b}$$

이다. 따라서 $|G| = p^{a+b}$이므로 G는 $p-$군이다(따름정리 4.2.4).

4.2.11. p가 소수일 때 위수가 p^2인 군은 항상 아벨군이 됨을 실로우정리를 써서 증명하여라.
(풀이)
실로우 1정리에 의하여 위수 p인 정규부분군 H가 존재한다. 그러면 $b \in G - H$를 생성원으로 갖는 군 $K = \langle b \rangle$는 위수가 p이고 역시 실로우 1정리에 의하여 정규부분군이다. 그러면 정리 3.3.6에 의하여 HK는 G의 정규부분군이다. 또한 $H \neq HK$이므로 $|HK| = p^2$이다. 따라서 $G = HK$이어야하고 $H \cap K = \{e\}$이다. 정리 3.3.8에 의하여

$$G \cong H \times K$$

이다. 이때 $|H| = |K| = p$(소수)이므로 H, K는 순환부분군이고 가환부분군이다. 따라서 G는 가환군이다.

(별해) G가 순환군이면 G는 가환군이다.

G가 순환군이 아니라고 하자. 그러면 $a(\neq e) \in G$에 대해 라그랑주 정리에 의해 $|\langle a \rangle| = p$이다. ($\because |\langle a \rangle| = p^2$이면 $\langle a \rangle = G$는 순환군이므로 모순)
$b \in G - \langle a \rangle$에 대해 $|\langle b \rangle| = p$이고 p가 소수이므로 $\langle a \rangle \cap \langle b \rangle = \{e\}$이다. 그리고 $\langle a \rangle \vee \langle b \rangle$를 $\langle a \rangle$와 $\langle b \rangle$를 포함하는 가장 작은 G의 부분군이라 하면 $\langle a \rangle \vee \langle b \rangle < G$이다. 이 때 $\langle a \rangle \subset \langle a \rangle \vee \langle b \rangle$이고 $\langle b \rangle \subset \langle a \rangle \vee \langle b \rangle$이므로 $|\langle a \rangle \vee \langle b \rangle| > p$이다. 따라서 $|\langle a \rangle \vee \langle b \rangle| = p^2$이므로 $G = \langle a \rangle \vee \langle b \rangle$이고 $\langle a \rangle \triangleleft G, \langle b \rangle \triangleleft G$이다. ($\because$ 실로우 1정리) 그리고 $\langle a \rangle \cap \langle b \rangle = \{e\}$이므로 $\langle a \rangle \times \langle b \rangle \cong G$이다(정리 3.3.8). 따라서 G는 가환군이다.

4.2.12. 유한 $p-$군 $G(\neq \{e\})$이면 따름정리 4.2.4에 의하여 $|G| = p^r$이다. 그러면 실로우 1정리에 의하여 위수 p^{r-1}인 부분군은 정규부분군이다. 따라서 단순군이 되려면 $r = 1$이어야 한다. 즉, G의 위수는 p일 때 단순군이다.

4.2.13. (1) 유한 $p-$군 $G(\neq \{e\})$이면 따름정리 4.2.4에 의하여 $|G| = p^r$이다. $H \subsetneq G$이므로 $|H| = p^a (a < r)$이다. 그러면 실로우 1정리에 의하여 위수 p^{a+1}인 부분군 $(H \subset) K$가 존재하고 $H \triangleleft K$이므로 $K \subset N_G(H)$이다. 따라서 $H \subsetneq N_G(H)$이다.

(2) $|G : H| = p$이면 $|H| = p^{r-1}$이므로 실로우 1정리에 의하여 $H \triangleleft G$이다.

== 연습문제 (4.3) ==

4.3.1. ⅰ) 위수 12인 군은 $12 = 2^2 \cdot 3$이므로 실로우 1과 3정리에 의하여 실로우 2-부분군은 1개 또는 3개 존재한다. 실로우 3-부분군은 1개 또는 4개 존재한다. 만약 실로우 2-부분군이 3개, 실로우 3-부분군이 4개 존재한다면 적어도 실로우 2-부분군의 원소는 적어도 $2 \cdot 3 = 6$개 존재하고, 실로우 3-부분군의 원소는 적어도 $2 \cdot 4 = 8$가 존재하여 원소가 14개 이상이 되어 모순이다. 따라서 실로우 2-부분군이 1개이거나 실로우 3-부분군이 1개이다. 1개인 실로우 2-부분군 또는 실로우 3-부분군이 정규부분군(정리 4.2.14)이 되므로 단순군이 아니다.

ⅱ) 위수 $56 = 2^3 \cdot 7$인 군은 실로우 1과 3정리에 의하여 실로우 2-부분군이 1개 또는 7개 존재하고, 실로우 7-부분군은 1개 또는 8개 존재한다. 만약 실로우 2-부분군이 7개, 실로우 7-부분군이 8개 존재한다면 적어도 실로우 2-부분군의 원소는 적어도 $4 \cdot 7 = 28$개 존재하고, 실로우 7-부분군의 원소는 적어도 $6 \cdot 8 = 48$가 존재하여 군의 원소가 76개 이상이 되어 모순이다. 따라서 실로우 2-부분군이 1개이거나 실로우 7-부분군이 1개이다. 1개인 실로우 2-부분군 또

는 실로우 7-부분군이 정규부분군(정리 4.2.14)이 되므로 단순군이 아니다.

iii) 위수 $96=2^5\cdot 3$인 군 G는 실로우 1과 3정리에 의하여 위수 32인 실로우 2-부분군이 1개 또는 3개 존재한다. 실로우 2-부분군이 1개이면 정규부분군(정리 4.2.14)이 되므로 단순군이 아니다.

만약 실로우 2-부분군이 3개 존재한다. 그 중 서로 다른 실로우 2-부분군을 H, K라 하자. 그러면 $|H\cap K|=1, 2, 4, 8, 16$의 중에서 하나이다. 이때

$$96 \geqq |HK|=\frac{32\cdot 32}{|H\cap K|} \Rightarrow |H\cap K|=16$$

이다. 또한 실로우 1정리에 의하여 위수가 16인 $H\cap K$는 위수가 32인 H, K의 정규부분군이다. 따라서 $H\cup K\subset N_G(H\cap K)$이다. 그러므로 $|N_G(H\cap K)|$은 32보다 크고 16의 배수이며 96의 약수이어야 한다. 즉,

$$|N_G(H\cap K)|=96 \Rightarrow N_G(H\cap K)=G$$

가 되어 $H\cap K$는 G의 정규부분군이 되어 G는 단순군이 아니다.

iv) 위수 $160=2^5\cdot 5$인 군 G는 실로우 1과 3정리에 의하여 위수 32인 실로우 2-부분군이 1개 또는 5개 존재한다. 실로우 2-부분군이 1개이면 정규부분군(정리 4.2.14)이 되므로 단순군이 아니다.

만약 실로우 2-부분군이 3개 존재한다. 그 중 서로 다른 실로우 2-부분군을 H, K라 하자. 그러면 $|H\cap K|=1, 2, 4, 8, 16$의 중에서 하나이다. 이때2

$$160 \geqq |HK|=\frac{32\cdot 32}{|H\cap K|} \Rightarrow |H\cap K|=8, 16$$

이다.

먼저 $|H\cap K|=8$인 경우에는 $|HK|=128$이므로 위수가 2^r인 원소가 128개이다. 이때 실로우 5-부분군은 1개 또는 16개이므로 실로우 5-부분군이 16이면 위수 5인 원소가 적어도 $4\cdot 16=64$개가 되어 G의 원소는 적어도 192개가 되어 모순이다. 즉 실로우 5-부분군이 1개가 되어 정규부분군이다. 따라서 G는 단순군이다.

다음에 $|H\cap K|=16$인 경우에는 $H\cap K$는 위수가 32인 H, K의 정규부분군이다. 따라서 $H\cup K\subset N_G(H\cap K)$이다. 그러므로 $|N_G(H\cap K)|$은 32보다 크고 16의 배수이며 160의 약수이어야 한다. 즉,

$$|N_G(H\cap K)|=160 \Rightarrow N_G(H\cap K)=G$$

가 되어 $H\cap K$는 G의 정규부분군이 되어 G는 단순군이 아니다.

v) 위수 $200=2^3\cdot 5^2$인 군 G는 실로우 1과 3정리에 의하여 위수 125인 실로우 5-부분군이 1개 존재한다. 실로우 5-부분군이 1개이면 정규부분군(정리 4.2.14)이 되므로 단순군이 아니다.

4.3.2. $39=3\cdot 13$이므로 실로우 1과 3정리에 의하여 실로우 3-부분군이 1개 또는 13개 존재하고, 실로우 13-부분군은 1개 존재한다.

G가 가환군이면 $\mathbb{Z}_3\times\mathbb{Z}_{13}\cong\mathbb{Z}_{39}$와 동형이 되어 순환군이다. 따라서 실로우 3부분군은 1개 존재한다(정리 2.3.11). 실로우 13-부분군은 1개 존재한다.

G가 비가환군일 때 실로우 3부분군 H가 1개 존재한다면 실로우 13-부분군 K가 1개 존재하므로 둘 다 정규부분군이 된다(정리 2.3.11). 한편 정리 3.3.28(3)에 의하여

$$G/H\cong\mathbb{Z}_{13},\quad G/K\cong\mathbb{Z}_3 \Rightarrow\quad C_G<H\cap K=\{e\}$$

가 되어 정리 3.3.28(2)에 의하여 G가 가환군이 되어 모순이다. 따라서 실로우 3-부분군은 13개이다. 실로우 13-부분군은 1개 존재한다.

4.3.3. (1) 위수 $70=2\cdot 5\cdot 7$인 군 G는 실로우 1과 3정리에 의하여 실로우 7-부분군이 1개 존재하므로 정규부분군(정리 4.2.14)이다.

(2) 위수 $70=2\cdot 5\cdot 7$인 군 G는 실로우 1과 3정리에 의하여 실로우 5-부분군이 1개 존재하므로 정규부분군(정리 4.2.14)이다.

실로우 5-부분군을 H, 실로우 7-부분군을 K라 하면 $H\cap K=\{e\}$이다. 따라서

$$|HK| = \frac{5 \cdot 7}{|H \cap K|} = 35$$

이므로 정리 3.3.6(2)에 의하여 HK는 위수 35인 G의 정규부분군이다.

4.3.4. (1) 위수 $5 \cdot 7 \cdot 13$인 군 G는 실로우 1과 3정리에 의하여 실로우 13-부분군이 1개 존재하므로 정규부분군(정리 4.2.14)이다.

(2) 위수 $5 \cdot 7 \cdot 13$인 군 G는 실로우 1과 3정리에 의하여 실로우 7-부분군이 1개 존재하므로 정규부분군(정리 4.2.14)이다.

(3) 실로우 13-부분군 H와 실로우 7-부분군 K가 정규부분군이므로 잉여군 G/H, G/K가 존재하고 각각의 위수는 35와 65이다. 다시 실로우 1과 3정리에 의하여 잉여군 G/H는 실로우 5-부분군 H_5과 실로우 7-부분군 H_7이 1개씩 존재하므로 G/H의 정규부분군이다. 그러면 정리 3.3.28(3)에 의하여

$$|(G/H)/H_5| = 7, \quad |(G/H)/H_7| = 5 \;\Rightarrow\; (G/H)/H_5 \cong \mathbb{Z}_7,\ (G/H)/H_7 \cong \mathbb{Z}_5 \;\Rightarrow\; C_{G/H} < H_5 \cap H_7 = \{eH\}$$

가 되어 정리 3.3.28(2)에 의하여 G/H는 가환군이다. 같은 방법으로 G/K도 가환군임을 증명할 수 있다. 따라서

$$C_G < H \cap K = \{e\}$$

가 되어 정리 3.3.28(2)에 의하여 G가 가환군이다.

(4) G가 가환군이므로 유한생성 가환군의 기본정리 3.4.12와 따름정리 3.4.7에 의하여

$$G \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{13} \cong \mathbb{Z}_{5 \cdot 7 \cdot 13}$$

이 되어 G는 순환군이다.

4.3.5. 위수 $33 = 3 \cdot 11$인 군은 실로우 1과 3정리에 의하여 실로우 3-부분군 H와 실로우 11-부분군 K가 각각 1개씩 존재하므로 정규부분군이다. 따라서 잉여군 G/H, G/K가 존재하고 각각의 위수는 11과 3이다.
그러면 정리 3.3.28(3)에 의하여

$$|G/H| = 11, \quad |G/K| = 3 \;\Rightarrow\; G/H \cong \mathbb{Z}_{11},\ G/K \cong \mathbb{Z}_3 \;\Rightarrow\; C_G < H \cap K = \{e\}$$

가 되어 정리 3.3.28(2)에 의하여 G는 가환군이다. 유한생성 가환군의 기본정리 3.4.12와 따름정리 3.4.7에 의하여

$$G \cong \mathbb{Z}_3 \times \mathbb{Z}_{11} \cong \mathbb{Z}_{33}$$

이 되어 G는 순환군이다.

4.3.6. 위수 $30 = 2 \cdot 3 \cdot 5$인 군은 실로우 1과 3정리에 의하여 실로우 3-부분군이 1개 또는 10개 존재하고, 실로우 5-부분군은 1개 또는 6개 존재한다. 예 4.3.3에 의하여 실로우 3-부분군 또는 실로우 5-부분군이 정규부분군이 된다. 실로우 3-부분군을 H라 하고, 실로우 5-부분군을 K라 하면 $H \cap K = \{e\}$이다. 따라서

$$|HK| = \frac{3 \cdot 5}{|H \cap K|} = 15$$

이므로 정리 3.3.6(1)에 의하여 HK는 위수 15인 G의 부분군이다.

4.3.7. 위수 $28 = 2^2 \cdot 7$인 군은 실로우 1과 3정리에 의하여 실로우 7-부분군이 1개 존재한다. 그러면 위수가 7이므로 순환부분군이 되어 위수 7인 원소는 $\phi(7) = 6$개다(따름정리 2.3.12).

4.3.8. 위수 $44 = 2^2 \cdot 11$인 군은 실로우 1과 3정리에 의하여 실로우 11-부분군이 1개 존재한다. 그러면 위수가 11이므로 순환부분군이 되어 위수 11인 원소는 $\phi(11) = 10$개다(따름정리 2.3.12).

4.3.9. 위수가 $168 = 2^3 \cdot 3 \cdot 7$인 군은 실로우 1과 3정리에 의하여 실로우 7-부분군이 1개 또는 8개 존재한다.
단순군이므로 실로우 7-부분군은 정규부분군이 아니므로 8개 존재해야 한다. 따라서
그러면 위수가 7이므로 순환부분군이 되어 위수 7인 원소는 $\phi(7) \cdot 8 = 6 \cdot 8 = 48$개다(따름정리 2.3.12).

4.3.10. 위수가 $231 = 3 \cdot 7 \cdot 11$인 군 G의 실로우 11-부분군 H는 실로우 1과 3정리에 의하여 1개 존재하므로 정규부분군이다. 즉, $H = \langle a \rangle$라 하자. 그러면 임의의 $g \in G$에 대하여 $gag^{-1} = a^t (0 \leq t < 11)$이다. $gag^{-1} = a$임을 보이면 $\langle a \rangle \subset Z(G)$가 되어 증명이 완료된다.

한편 $gag^{-1} = a^t (0 \leq t < 11) \Rightarrow (gag^{-1})^{10} = (a^t)^{10} \Rightarrow ga^{10}g^{-1} = a^{t^{10}} \Rightarrow \ t^{10} = 1$이므로 다음이 성립한다.

$$a = g^{231}ag^{-231} = g^{230}(gag^{-1})g^{-230} = g^{230}(a^t)g^{-230} = (g^{230}ag^{-230})^t = \ \cdots \ = a^{t^{231}}$$

$|a| = 11$이므로 $t^{231} = 1 (\mathrm{mod}\ 11)$이다. 그러므로 $t \neq 0$이고 페르마 정리에 의하여 $t^{10} = 1 (\mathrm{mod}\ 11)$이다. 따라서

$$a = a^{231} = a^{(t^{10})^{23}t^1} = a^t = gag^{-1} \Rightarrow ga = ag$$

그러므로 $\langle a \rangle \subset Z(G)$이다.

4.3.11. 위수 $45 = 3^2 \times 5$인 군은 실로우 1과 3정리에 의하여 실로우 3-부분군과 실로우 5-부분군 각각 1개씩 존재하므로 정규부분군이다. 실로우 3-부분군을 P라 하고, 실로우 5-부분군을 Q라 하면 $P \cap Q = \{e\}$이다. 따라서

$$45 = |G| \geq |PQ| = \frac{9 \cdot 5}{|P \cap Q|} = 45$$

이므로 정리 3.3.6(1)에 의하여 PQ는 위수 45인 G의 부분군이므로 $G = PQ$이고 정리 3.3.7에 의하여 G는 가환군이다.

(별해) $G/P \cong \mathbb{Z}_5$은 가환군이고 $|G/Q| = 9 = 3^2$이므로 정리 4.3.1에 의하여 가환군이다. 따라서 정리 3.3.28(3)에 의하여

$$C_G < P \cap Q = \{e\}$$

가 되어 정리 3.3.28(2)에 의하여 G는 가환군이다.

4.3.12. $p = q$인 경우에는 실로우 1정리에 의하여 위수 p^2인 정규부분군이 존재하여 단순군이 아니다.
$p > q$인 경우에는 실로우 p-부분군이 1개 존재하여 정규부분군이 되므로 단순군이 아니다.
마지막으로 $p < q$인 경우에는 $p = 2$이고 $q = 3$이면 위수 12인 군은 연습문제 4.3.1에 의하여 단순군이 아니다.
$p = 2$이고 $q > 3$인 경우에는 실로우 q-부분군이 1개 존재하므로 정규부분군이 되어 단순군이 아니다.
다음에 $p > 2$인 경우에는

$$p^2 - 1 \equiv 0 (\mathrm{mod}\ q) \Rightarrow (p+1)(p-1) \equiv 0 (\mathrm{mod}\ q) \Rightarrow p + 1 \equiv 0 (\mathrm{mod}\ q) \Rightarrow p + 1 = qt$$

이므로 $q \geq p + 1 = qt \Rightarrow p + 1 = q$($p$, q 둘 다 홀수)가 되어 모순이다.
따라서 $p^2 \not\equiv 1 (\mathrm{mod}\ q)$이므로 실로우 q-부분군이 1개 존재하므로 정규부분군이 되어 단순군이 아니다.

(별해) $|G| = p^2q$이므로 sylow p-부분군의 개수는 1개 또는 q개
sylow q-부분군의 개수는 1개 또는 p개 또는 p^2개 존재한다.
이때 실로우 p-부분군 또는 실로우 q-부분군이 1개 존재하면 정규부분군이 되어 단순군이 아니다.
한편 실로우 p-부분군이 q개이고 sylow q-부분군이 p개 이상인 경우는 다음과 같다.
sylow p-부분군을 $H_1, \cdots, H_q$라 하면 $|H_i| = p^2$이고 $|H_i \cap H_j| = 1$ 또는 p $(i \neq j)$이므로

$$|H_1 \cup H_2 \cup \cdots \cup H_q| \geq p + (p^2 - p)q = p^2q - pq + p \ \cdots\cdots\cdots ①$$

sylow q-부분군을 J_i라 할 때 p개인 경우, $|J_1 \cup J_2 \cup \cdots \cup J_p| = pq - p + 1$이고 $\cdots\cdots\cdots ②$

$① + ② > p^2q$ 이므로 모순

p^2개인 경우, $|J_1 \cup J_2 \cup \cdots \cup J_{p^2}| = p^2q - p^2 + 1$이고 $\cdots\cdots\cdots ③$

$$\begin{aligned} ① + ③ &= 2p^2q - pq - p^2 + p + 1 \qquad \text{이므로 모순} \\ &= p^2q + p^2q - pq - p^2 + p + 1 \\ &= p^2q + (p-1)(pq-1) + 1 > p^2q \end{aligned}$$

따라서 sylow p-부분군 또는 sylow q-부분군의 개수는 1개이므로 정규부분군이 존재하여 G는 단순군이 아니다.

4.3.13. 실로우 1과 3정리에 의하여 실로우 p-부분군이 1개 존재하므로 정규부분군이다. 따라서 단순군이 아니다.

4.3.14.(문항 삭제) 유한 단순군 G의 위수가 60보다 클 때, G에는 $1<|G:H|\le 5$인 부분군 H가 존재하지 않음을 증명하여라.
(풀이) 생략. 참조: 박승안 대수학 8판. 연습문제 (6.2) 7번 문제.

== 연습문제 (4.4) ==

4.4.1. G가 가환군이면 유한생성 가환군의 기본정리에 의하여 $G\cong \mathbb{Z}_2\times\mathbb{Z}_7\cong\mathbb{Z}_{14}$이다.
G가 비가환군이면 $6^2\equiv 1(\mathrm{mod}\ 7)$이므로 정리 4.3.1(4)에 의하여 $G\cong\langle a,\ b\,|\,|a|=7,\ |b|=2,\ ba=a^6b\rangle\cong D_7$이다.

4.4.2. G가 가환군이면 유한생성 가환군의 기본정리에 의하여 $G\cong\mathbb{Z}_3\times\mathbb{Z}_7\cong\mathbb{Z}_{21}$이다.
G가 비가환군이면 $2^3\equiv 4^3\equiv 1(\mathrm{mod}\ 7)$이므로 정리 4.3.1(4)에 의하여
$G\cong\langle a,\ b\,|\,|a|=7,\ |b|=3,\ ba=a^2b\rangle$ 또는 $\langle a,\ b\,|\,|a|=7,\ |b|=3,\ ba=a^4b\rangle$
이다. 하지만 $c=a^2$이라면 $|c|=|a^2|=7$이고 $ba=a^4b=c^2b$이므로 다음과 같은 동형군을 얻는다.
$G\cong\langle a,\ b\,|\,|a|=7,\ |b|=3,\ ba=a^4b\rangle\cong\langle c,\ b\,|\,|c|=7,\ |b|=3,\ ba=c^2b\rangle\cong\langle a,\ b\,|\,|a|=7,\ |b|=3,\ ba=a^2b\rangle$

4.4.3. (1) $a^2ba^2=a^2(ba)a=a^2(a^3b)a=a^5ba=a(a^3b)=a^4b=b$
(2) $(ba^2)^2=(ba^2)(ba^2)=ba^2(ba)a=ba^2(a^3b)a=ba(ba)=ba(a^3b)=b^2=e$이므로 위수는 2이다.

== 연습문제 (5.1) ==

5.1.1. $\forall\, a+b\sqrt{2},\ a'+b'\sqrt{2},\ a''+b''\sqrt{2}\in\mathbb{Q}(\sqrt{2})$에 대하여
① $(a+b\sqrt{2}+a'+b'\sqrt{2})+a''+b''\sqrt{2}=(a+a'+(b+b')\sqrt{2})+a''+b''\sqrt{2}=a+a'+a''+(b+b'+b'')\sqrt{2})$
$a+b\sqrt{2}+(a'+b'\sqrt{2}+a''+b''\sqrt{2})=a+b\sqrt{2}+(a''+a'')+(b'+b'')\sqrt{2}=a+a'+a''+(b+b'+b'')\sqrt{2})$
$\therefore (a+b\sqrt{2}+a'+b'\sqrt{2})+a''+b''\sqrt{2}=a+b\sqrt{2}+(a'+b'\sqrt{2}+a''+b''\sqrt{2})$
나머지 생략 (참조 예 7.3.5)

$-(a+b\sqrt{2})=-a-b\sqrt{2}$이고 $(a+b\sqrt{2})^{-1}=\dfrac{a}{a^2-2b^2}-\dfrac{b}{a^2-2b^2}\sqrt{2}$

5.1.2. $2^{-1}=\dfrac{1}{2}\notin\mathbb{Z}(\sqrt{2})$이므로 (R_9)가 성립하지 않으므로 체가 아닌 단위원을 갖는 가환환이다.

5.1.3. $(R,+)$이 가환군이므로 곱셈에 대한 분배법칙과 결합법칙이 성립함을 보이자.
$\forall\, a,b,c\in R,\ a\cdot(b+c)=0=0+0=a\cdot b+a\cdot c$이고 $(a+b)\cdot c=0=0+0=a\cdot c+b\cdot c$
이므로 곱셈에 대한 분배법칙 성립.
$\forall\, a,b,c\in R,\ (a\cdot b)\cdot c=0\cdot c=0=a\cdot 0=a\cdot(b\cdot c)$
이므로 곱셈에 대한 결합법칙 성립.
$\therefore (R,+,\cdot)$은 환이다.

5.1.4. 유리수체 $\mathbb{Q}$의 원소 a,b 에 대하여 $a*b=a+b-1,\ a\cdot b=a+b-ab$ 라 할 때, $(\mathbb{Q},*,\cdot)$는 체가 되는가?
(풀이) $\forall\, a,b,c\in\mathbb{Q}$ 에 대하여
① $(a*b)*c=(a+b-1)*c=a+b+c-2$
$a*(b*c)=a*(b+c-1)=a+b+c-2$
$\therefore (a*b)*c=a*(b*c)$

② $a = a * e = e * a = a + e - 1$
$\therefore e = 1 \in \mathbb{Q}$

③ $1 = a * (-a) = (-a) * a = a + (-a) - 1$
$\therefore (-a) = -a + 2 \in \mathbb{Q}$

④ $a * b = a + b - 1 = b + a - 1 = b * a$

⑤ $(a \cdot b) \cdot c = (a + b - ab) \cdot c$
$= a + b - ab + c - ac - bc + abc$
$= a + b + c - bc - ab - bc + abc$
$= a \cdot (b + c - bc)$
$= a \cdot (b \cdot c)$

$(R_1)\ \forall a, b, c \in \mathbb{Q},\ (a * b) * c = (a + b - 1) * c = a + b + c - 2 = a + (b + c - 1) - 1 = a * (b + c - 1) = a * (b * c)$
$\therefore (a * b) * c = a * (b * c)$

$(R_2)\ \exists e (= 1) \in \mathbb{Q},\ \forall a \in \mathbb{Q},\ a = a * e = e * a = a + e - 1 \quad \therefore e = 1$

$(R_3)\ \forall a \in \mathbb{Q},\ \exists x (= 2 - a) \in \mathbb{Q},\ 1 = x * a = a * x = a + x - 1 \quad \therefore x = 2 - a$

$(R_4)\ \forall a, b \in \mathbb{Q},\ a * b = a + b - 1 = b + a - 1 = b * a \quad \therefore a * b = b * a$

$(R_5)\ (a * b) \bullet c = (a + b - 1) \bullet c = a + b + c - 1 - ac - bc + c$
$= (a + c - ac) + (b + c - bc) - 1 = (a + c - ac) * (b + c - bc)$
$= (a \bullet c) * (b \bullet c)$
$\therefore (a * b) \bullet c = (a \bullet c) * (b \bullet c)$
$a \bullet (b * c) = (a \bullet b) * (a \bullet c)$도 위와 같은 방법으로 성립

$(R_6)\ \forall a, b, c \in \mathbb{Q},\ (a \bullet b) \bullet c = (a + b - ab) \bullet c = a + b + c - ab - bc - abc$
$= a + (b + c - bc) - (ab + ac - abc) = a \bullet (b + c - bc) = a \bullet (b \bullet c)$
$\therefore (a \bullet b) \bullet c = a \bullet (b \bullet c)$

$(R_7)\ \exists e (= 0) \in \mathbb{Q},\ \forall a \in \mathbb{Q},\ a = a \bullet e = e \bullet a = a + e - ae \Rightarrow e = 0$

$(R_8)\ \forall a, b \in \mathbb{Q},\ a \bullet b = a + b - ab = b + a - ba = b \bullet a$
$\therefore a \bullet b = b \bullet a$

$(R_9)\ \forall a (\neq 1) \in \mathbb{Q},\ \exists x \left(= \frac{a}{a-1}\right) \in \mathbb{Q},\ a \bullet x = a + x - ax = 0,\ x = \frac{a}{a-1}$ 이므로
$(\mathbb{Q}, *, \bullet)$는 체이다.

5.1.5. 유클리드 호제법이용

$3a \equiv 1 \equiv 27 \equiv 3 \cdot 9 \pmod{26},\quad 3^{-1} = a = 9$
$5a \equiv 1 \equiv -25 \equiv 5 \cdot (-5) \pmod{26},\quad 5^{-1} = a = -5 = 21$
$11a \equiv 1 \equiv -77 \equiv 11 \cdot (-7) \pmod{26},\ 11^{-1} = a = -7 = 19$

5.1.6. $x = 1 \cdot x = (ya) \cdot x = y \cdot (ax) = y \cdot 1 = y$

5.1.7. 임의의 $a, b \in U(R)$에 대하여

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$

이므로 $ab \in U(R)$이다. 또한 R이 환이므로 곱셈에 대한 결합법칙이 성립하고, 정의에 의하여 곱셈항등원 1과 곱셈역원은 분명히 $U(R)$의 원소이다. 그러므로 $U(R)$은 곱셈군이다.

5.1.8.

(1) a가 단원이므로 $aa^{-1} = 1$이 성립한다. $a^2 = a$의 양변에 a의 역원을 곱하면 $a = 1$이다.
(2) $a = 0$이면 분명히 멱등원이다.

$a \neq 0$ 이면, 나눗셈환이므로 $a(a-1)=0 \Rightarrow a^{-1}a(a-1)=a^{-1}0=0 \Rightarrow a-1=0 \Rightarrow a=1$

$\therefore a=0,1$

(3) $\forall a,b \in R$, $(ab)^2=abab=aabb=a^2b^2=ab$이므로 곱셈에 관해 닫혀 있다.

(4) $\mathbb{Z}_6$의 멱등원: $\{0,1,3,4\}$, $\mathbb{Z}_{12}$의 멱등원:$\{0,1,4,9\}$

5.1.9.

(1) (R_1) $f,g,h \in F^F$에 대하여

$$[(f+g)+h](x)=(f+g)(x)+h(x)=(f(x)+g(x))+h(x)$$
$$=f(x)+(g(x)+h(x))=f(x)+(g+h)(x)=[f+(g+h)](x)$$
$$\therefore (f+g)+h=f+(g+h)$$

(R_2) 영함수 $0(x)=0$와 $\forall f \in F^F$에 대하여

$$(f+0)(x)=f(x)+0(x)=f(x)+0=f(x)$$
$$(0+f)(x)=0(x)+f(x)=0+f(x)=f(x)$$
$$\therefore f+0=0+f=f$$

(R_3) $\forall f \in F^F$에 대하여 $\exists -f \in F^F$

$$(f+(-f))(x)=f(x)+(-f(x))=0$$
$$((-f)+f)(x)=-f(x)+f(x)=0$$
$$\therefore f+(-f)=(-f)+f=0$$

(R_4) $\forall f,g \in F^F$에 대하여

$$(f+g)(x)=f(x)+g(x)=g(x)+f(x)=(g+f)(x)$$
$$\therefore f+g=g+f$$

(R_5) $\forall f,g,h \in F^F$에 대하여

$$[f \bullet (g+h)](x)=f(x)(g+h)(x)=f(x)(g(x)+h(x))$$
$$=f(x)g(x)+f(x)h(x))=(f \bullet g)(x)+(f \bullet h)(x)=[(f \bullet g)+(f \bullet h)](x)$$
$$\therefore f \bullet (g+h)=(f \bullet g)+(f \bullet h)$$

같은 방법으로 $(f+g) \bullet h=(f \bullet h)+(g \bullet h)$이 성립함을 증명할 수 있다.

(R_6) $\forall f,g,h \in F^F$에 대하여

$$[(f \bullet g) \bullet h](x)=(f \bullet g)(x)h(x)=(f(x)g(x))h(x)$$
$$=f(x)(g(x)h(x))=f(x)(g \cdot h)(x)=[f \cdot (g \cdot h)](x)$$
$$\therefore (f \bullet g) \bullet h=f \cdot (g \cdot h)$$

(R_7) $\forall f \in F^F$에 대하여 $1(x)=1$(상수함수)이라 하면

$$(f \bullet 1)(x)=f(x)1(x)=f(x)=1(x)f(x)=(1 \bullet f)(x)$$
$$\therefore f \cdot 1=1 \cdot f=f$$

(R_8) $\forall f,g \in F^F$에 대하여

$$(f \bullet g)(x)=f(x)g(x)=g(x)f(x)=(g \bullet f)(x)$$
$$\therefore f \cdot g=g \cdot f$$

이 성립하므로 $(F^F,+,\bullet)$은 단위원 1을 가진 가환환이 된다.

(2) $f \in F^F$, $f^2=f \Rightarrow f^2(x)=f(x) \Rightarrow \{f(x)\}^2=f(x) \Rightarrow f(x)\{f(x)-1\}=0 \Rightarrow f(x)=0,\ f(x)=1 \Rightarrow f=0,\ 1$

$\therefore F^F$에서 모든 멱등원 : $\{0,1\}$

5.1.10.

(1) (R_1) $f,g,h \in End(A)$에 대하여

$$[(f+g)+h](x)=(f+g)(x)+h(x)=(f(x)+g(x))+h(x)$$
$$=f(x)+(g(x)+h(x))=f(x)+(g+h)(x)=[f+(g+h)](x)$$
$$\therefore (f+g)+h=f+(g+h)$$

(R_2) 영함수 $0(x)=0$와 $\forall f \in End(A)$에 대하여

$$(f+0)(x)=f(x)+0(x)=f(x)+0=f(x)$$
$$(0+f)(x)=0(x)+f(x)=0+f(x)=f(x)$$
$$\therefore f+0=0+f=f$$

$(R_3)\ \forall f\in End(A)$에 대하여 $\exists -f\in End(A)$

$$(f+(-f))(x)=f(x)+(-f(x))=0$$
$$((-f)+f)(x)=-f(x)+f(x)=0$$
$$\therefore f+(-f)=(-f)+f=0$$

$(R_4)\ \forall f,g\in End(A)$에 대하여

$$(f+g)(x)=f(x)+g(x)=g(x)+f(x)=(g+f)(x)$$
$$\therefore f+g=g+f$$

$(R_5)\ \forall f,g,h\in End(A)$에 대하여 군 준동형사상이므로

$$[f\circ(g+h)](x)=f((g+h)(x))=f(g(x)+h(x))=f(g(x))+f(h(x))$$
$$=(f\circ g)(x)+(f\circ h)(x)=[(f\circ g)+(f\circ h)](x)$$
$$\therefore f\circ(g+h)=(f\circ g)+(f\circ h)$$

같은 방법으로 $(f+g)\circ h=(f\circ h)+(g\circ h)$이 성립함을 증명할 수 있다.

$(R_6)\ \forall f,g,h\in End(A)$에 대하여 정리 1.4.8에 의하여 합성은 결합법칙이 성립한다.

$$(f\circ g)\circ h=f\circ(g\circ h)$$

$(R_7)\ \forall f\in End(A)$에 대하여 $1(x)=x$(항등함수)라 하면

$$(f\circ 1)(x)=f(1(x))=f(x)=1(f(x))=(1\circ f)(x)$$
$$\therefore f\circ 1=1\circ f=f$$

예 1.4.7에 의하여 비가환환이다.

이 성립하므로 $(End(A),+,\circ)$은 단위원 1을 가진 환이 된다.

5.1.11.

(1) $\mathbb{Z}$: 0, $\mathbb{Z}_{12}$: 0, 6, $\mathbb{Z}_{32}$: 0, 2, 4, 6, 8, 10, ... , 30

(2) n의 약수 중 소수들 모두를 약수로 가지는 수

$n=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$(표준분해)일 때 $x=p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r}, 0<b_i\le a_i$은 멱영원이고

$S=\left\{x\in\mathbb{Z}\mid x=p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r}, 0<b_i\le a_i\right\}$는 멱영원들의 집합.

($\Rightarrow$) $x\in\mathbb{Z}_n$을 멱영원이라 하면 $\exists t\in\mathbb{N}, x^t=0\ (\mathrm{mod}\ \mathbb{Z}_n)$이다.

$n\mid x^t$이고 $p_i\mid n$이므로 $p_i\mid x^t$이고 p_i가 소수이므로 $p_i\mid x$이다.

즉, $\mathrm{lcm}(p_1,p_2,\cdots,p_r)=p_1p_2\cdots p_r\mid x$

그러므로 $\mathbb{Z}_n$의 원소 중 멱영원은 $p_1p_2\cdots p_r$의 배수이다.

따라서 $S=\{x\in\mathbb{Z}_n\mid p_1p_2\cdots p_r\mid x\}=\left\{x\in\mathbb{Z}\mid x=p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r}, 0<b_i\le a_i\right\}$

($\Leftarrow$) $\forall y\in S$가 $\mathbb{Z}_n$의 멱영원임을 보이자.

$y=p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r}, 0<b_i\le a_i$

$b_it-a_i\ge 0$인 t를 선택하면

$$y^t=(p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r})^t$$
$$=p_1^{b_1t}p_2^{b_2t}\cdots p_r^{b_rt}$$
$$=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}(p_1^{b_1t-a_1}p_2^{b_2t-a_2}\cdots p_r^{b_rt-a_r})$$
$$=n\cdot(p_1^{b_1t-a_1}p_2^{b_2t-a_2}\cdots p_r^{b_rt-a_r})$$
$$=0$$

이므로 y는 $\mathbb{Z}_n$의 멱영원

5.1.12.

a, b는 멱영원이므로 a^m=0, b^n=0이 되는 자연수 m, n이 존재한다. 가환환이므로 이항정리를 적용하면

$$(a+b)^{m+n} = {}_{m+n}C_0 a^{m+n} + {}_{m+n}C_1 a^{m+n-1}b + \cdots + {}_{m+n}C_i a^{m+n-i}b^i + \cdots + {}_{m+n}C_{m+n} b^{m+n}$$

이다. 이때

$$\begin{cases} {}_{m+n}C_i a^{m+n-i}b^i = 0, \text{ if } i \leqq n, \text{ then } a^{m+n-i} = a^m a^{n-i} = 0 \\ {}_{m+n}C_i a^{m+n-i}b^i = 0, \text{ if } i > n, \text{ then } b^i = b^{i-n}b^n = 0 \end{cases}$$

이므로 $(a+b)^{m+n} = 0$이다. 따라서 $a+b$도 멱영원이다.

5.1.13. x가 멱영원이므로 $x^n = 0 (\exists\, n \in \mathbb{N})$이다.

먼저 n이 홀수인 경우

$$u^n = x^n + u^n = (x+u)(x^{n-1} - x^{n-2}u + \cdots - xu^{n-2} + u^{n-1})$$

이므로 $x+u$는 단원이다. 다음에 n이 짝수인 경우

$$-u^n = x^n - u^n = (x+u)(x^{n-1} - x^{n-2}u + \cdots + xu^{n-2} - u^{n-1})$$

이므로 $x+u$는 단원이다.

5.1.14. (문제 수정) 환 R에 대하여 다음 물음에 답하라.

(1) R이 영이 아닌 멱영원을 가지지 않을 필요충분조건은 $x^2 = 0$의 해가 0뿐임을 보여라.

(2) 특히 R이 영이 아닌 멱영원을 가지지 않을 때 원소 $a, b \in R$에 대하여 다음을 증명하라.

(2-1) $ab = 0$이면 $ba = 0$이다.

(2-2) $aba = 0$이면 $ab = 0$이다.

(2-3) $ab = 0$이면 임의의 $x \in R$에 대하여 $axb = 0$이다.

(풀이) (1) ($\Rightarrow$) 원소 $a(\neq 0) \in R$에 대하여 가정에 의하여 a^n=0인 자연수 n이 존재하지 않는다. 특히 $a^2 \neq 0$이다. 따라서 x^2=0의 해는 0뿐이다.

(별해) 0이 아닌 해 $a(\neq 0) \in R$가 존재한다면 $a^2 = 0$이 되어 a는 0이 아닌 멱영원이 되어 모순이다. 따라서 x^2=0의 해는 0뿐이다.

($\Leftarrow$) $x \in$R, x^2=0의 해가 0뿐이라 하자. 만약 0이 아닌 멱영원 x가 존재한다고 하면 적당한 최소 자연수 n에 대하여 $x^n = 0$이다. 이때 n이 홀수이면 $x^{n+1} = 0$이므로 n을 짝수라 해도 좋다. 그러면 가정에서 x^2=0의 해가 0뿐이므로

$$0 = x^n = \left(x^{\frac{n}{2}}\right)^2 \Rightarrow 0 = x^{\frac{n}{2}}$$

이다. 이것은 n의 최소성$\left(\frac{n}{2} < n\right)$에 모순이다. 따라서 R은 0이 아닌 멱영원을 가지지 않는다.

(2)

(2-1) $(ba)^2 = b(ab)a = 0$이므로 (1)에 의하여 $ba = 0$이다.

(2-2) $(ab)^2 = (aba)b = 0$이므로 (1)에 의하여 $ab = 0$이다.

(2-3) $ab = 0$이면 (2-1)에 의하여 $ba = 0$이다. 따라서 $(axb)^2 = ax(ba)xb = 0$이므로 (1)에 의하여 $axb = 0$이다.

5.1.15.

(1) ($\Rightarrow$) $(a+b)(a-b) = a^2 - ab + ba - b^2 = a^2 - ab + ab - b^2 = a^2 - b^2$

($\Leftarrow$) $\forall\, a, b \in R$에 대하여

$$(a+b)(a-b) = a^2 - b^2 \Rightarrow a^2 - ab + ba - b^2 = (a+b)(a-b) = a^2 - b^2 \Rightarrow -ab + ba = 0 \Rightarrow ab = ba$$

$\therefore$ R은 가환환이다.

(2) ($\Rightarrow$) $(ab)^2 = abab = aabb = a^2b^2$

($\Leftarrow$) 위 문제 5.1.14 (2-1)에 의하여

$$(ab)^2 = a^2b^2 \Rightarrow abab - aabb = 0 \Rightarrow a[(ba-ab)b] = 0 \Rightarrow [(ba-ab)b]a = (ba-ab)ba = 0$$

위와 같은 방법으로 a, b를 바꾸어도 성립하므로 $(ab-ba)ab=0$이다. 따라서

$$(ba-ab)^2=(ba-ab)(ba-ab)=(ba-ab)ba-(ba-ab)ab=(ba-ab)ba+(ab-ba)ab=0$$

이므로 위 문제 5.1.14(1)에 의하여 $ba-ab=0,\quad ba=ab$이다. 따라서 R은 가환환이다.

5.1.16. 덧셈에 대한 교환법칙만 성립하면 가정에 의해 나눗셈환이 된다.

$\forall a,b\in S$

$$a+a+b+b=(1+1)a+(1+1)b=(1+1)(a+b)=(a+b)+(a+b)=a+b+a+b(\because \text{분배법칙})$$
$$\Rightarrow\ a+b=b+a(\because \text{덧셈에 대한 소거법칙})$$

그러므로 S는 나눗셈 환이다.

5.1.17.

(1) 임의의 $a, b\in S$에 대하여 $ab\neq 0$임을 보이면 된다. $a\neq 0,\ b\neq 0$이다. 이때 $ab=0$이라면 D가 정역이므로

$$ab=0\ \Rightarrow\ a=0\text{이거나 }b=0$$

이 되어 모순이다. 따라서 $ab\neq 0$이고 $ab\in S$이다. 그러므로 S는 곱셈집합이다.

(2) 1= $b^0\in$S 이므로 $1\in$S 이다.

$b^m,\ b^n\in S$에 대하여 $b^m\cdot b^n=b^m\cdot b^n=b^{m+n}\in S$이므로 S는 $\mathbb{Z}$의 곱셈집합이다.

5.1.18. $\mathbb{Z}[i]=\{a+bi\mid a, b\in\mathbb{Z}, i^2=-1\}$ 이라면 $\mathbb{Z}[i]$는 $\mathbb{C}$ 의 부분집합이다.

(1) $(\mathbb{Z}[i],\ +,\ \cdot\ )$은 1을 가진 가환환이 됨을 보여라.
(이 환을 가우스의 정수환이라 한다.)

(2) $N(a+bi)=a^2+b^2$ 라고 하면, $x, y\in\mathbb{Z}[i]$일 때 $N(xy)=N(x)N(y)$ 임을 보여라.

(3) $x=a+bi$가 단원일 필요충분조건은 $N(x)=1$임을 보여라.

(4) $\mathbb{Z}[i]$ 의 모든 단원을 구하여라.

(5) $\mathbb{Z}[i]$ 의 단원들의 군은 무엇과 같은가?

(풀이) (1) $0=0+0\cdot i,\ 1=1+0\cdot i\in\mathbb{Z}[i]$이고 $a+bi, c+di\in\mathbb{Z}[i]$에 대하여

$$(a+bi)+(c+di)=a+c+(b+d)i\in\mathbb{Z}[i]$$
$$(a+bi)(c+di)=ac-bd+(ad+bc)i\in\mathbb{Z}[i]$$

이고 나머지 성질은 복소수는 단위원을 가진 가환환을 이용하면 $(\mathbb{Z}[i],\ +,\ \cdot\ )$은 1을 가진 가환환임을 알 수 있다.

(2) $a+bi, c+di\in\mathbb{Z}[i]$에 대하여

$$N((a+bi)(c+di))=N(ac-bd+(bc+ad)i)=(ac-bd)^2+(bc+ad)^2$$
$$=a^2c^2+b^2d^2+b^2c^2+a^2d^2=(a^2+b^2)(c^2+d^2)=N(a+bi)N(c+di)$$

이므로 $N((a+bi)(c+di))=N(a+bi)N(c+di)$이다.

(3) ($\Rightarrow$) $(a+bi)$가 단원이라 하자. $(a+bi)(a'+b'i)=1\in\mathbb{Z}[i]$인 $a'+b'i\in\mathbb{Z}[i]$가 존재한다. 그러면 (2)에 의하여

$$(a+bi)(a'+b'i)=1\ \Rightarrow\ 1=N(1)=N((a+bi)(a'+b'i))=N(a+bi)N(a'+b'i)$$

이다. 그리고 $N(a+bi)\geq 0$이므로 $N(a+bi)=1$이다.

(별해) $(a+bi)$가 단원이라 하자. $(a+bi)^{-1}=\dfrac{a-bi}{a^2+b^2}\in\mathbb{Z}[i]$ 이므로 $\dfrac{a}{a^2+b^2}$, $\dfrac{b}{a^2+b^2}\in\mathbb{Z}$ 이어야 하는데

$a\leq a^2+b^2,\ b\leq a^2+b^2$ 이고, $a^2+b^2|a$, $a^2+b^2|b$ 가 되기 위해선 $a^2+b^2=1$일 수 밖에 없다. $\therefore N(a+bi)=1$

($\Leftarrow$) $N(a+bi)=1$이므로

$$1=N(a+bi)=a^2+b^2\ \Rightarrow\ a+bi=\pm 1,\ \pm i$$

이다. $a+bi=1,\ -1,\ i,\ -i$의 곱셈 역원은 각각 $1, -1,\ -i,\ i$이므로 $a+bi$는 단원이다.

(4) (3)에 의하여 단원은 $1, -1,\ -i,\ i$이다.

(5) 단원집합 $\{1, -1,\ -i,\ i\}$은 곱셈군으로 i의 위수가 4이므로 $\mathbb{Z}_4$와 동형이다.

5.1.19.

(1) $(i+j)(1+2j-k)=i+2ij-ik+j+2j^2-jk=i+2k+j+j-2-i=-2+2j+2k$

(2) $j^3i^2kji^5=(-j)(-1)kji=(jk)(ji)=i(-k)=j$

(3) $[(1+3i)(4j+3k)]^{-1}=(4j+3k)^{-1}(1+3i)^{-1}=\frac{-4j-3k}{25}\cdot\frac{1-3i}{10}=\frac{5j-15k}{250}$

(별해) $[(1+3i)(4j+3k)]^{-1}=[4j+3k+12ij+9ik]^{-1}=[4j+3k+12k-9j]^{-1}=[-5j+15k]^{-1}=\frac{5j-15k}{250}$

== 연습문제 (5.2) ==

5.2.1.

(1) 단원군 : $\{\overline{1},\overline{5},\overline{7},\overline{11},\overline{13},\overline{17}\}$

영인자 : $\{\overline{2},\overline{3},\overline{4},\overline{6},\overline{8},\overline{9},\overline{10},\overline{12},\overline{14},\overline{15},\overline{16}\}$

(2) 단원군 : $\{1,5,7,11,13,17\}$

영인자 : $\{2,3,4,6,8,9,10,12,14,15,16\}$

(3) 단원군 : $\{(1,1)\}$

영인자 : $\{(0,1),(1,0)\}$

5.2.2.

단원 : $\{(1,1),(1,2)\}$

영인자 : $\{(0,1),(0,2),(1,0)\}$

멱등원 : $\{(0,0),(0,1),(1,0),(1,1)\}$

멱영원 : $\{(0,0)\}$

5.2.3.

(1) $U(\mathbb{Z}^2)=\{(1,1),(-1,-1),(1,-1),(-1,1)\}$

$Zero(\mathbb{Z}^2)=\{(a,0),(0,b)\,|\,a,b\in\mathbb{Z}-\{0\}\}$

(2) $(1,2),(2,1)$

5.2.4. ab가 영인자이므로 $\begin{cases}(ab)x=0\\x(ab)=0\end{cases}$ $(ab\neq 0, x\neq 0)$이다.

a가 영인자가 아니라 하자. $0=(ab)x=a(bx)$이므로 $bx=0$이 된다. $b\neq 0, x\neq 0$이므로 b는 영인자이다.

5.2.5. R의 영인자 a가 단원이라 하자. 그러면 적당한 $b(\neq 0)\in R$이 존재하여 $ab=0$이다. 한편 a가 단원이므로

$$ab=0 \Rightarrow a^{-1}(ab)=a^{-1}0=0 \Rightarrow b=0$$

이 되어 $b\neq 0$이라는 가정에 모순이다. 따라서 R의 영인자는 단원이 아니다.

5.2.6. $a0=0$이므로 $0\in I_a$이다.

$$\forall x,y\in I_a,\ a(x-y)=ax-ay=0-0=0$$

이므로 $(x-y)\in I_a$이다.

$$\forall x,y\in I_a,\ a(xy)=(ax)y=0y=0$$

이므로 $xy\in I_a$이다. 부분환의 판정조건(정리 5.2.12)에 의하여 $I_a<R$이다.

5.2.7.

(1) $(1-r)^2 = 1-2r+r^2 = 1-2r+r = 1-r$이므로 $1-r$도 멱등원이다.

(2) $r^2 = r \Rightarrow r-r^2 = 0 \Rightarrow r(1-r) = 0$

가정에 의하여 $r \neq 0$이고 $1-r \neq 0$이므로 r과 $1-r$은 영인자이다.

5.2.8. 정역 D의 부분정역들의 공통집합을 $S = \cap_{i \in I, A_i < D} A_i$(단, I는 첨자집합)이라 하자.

모든 $i \in I$에 대하여 A_i가 정역 D의 부분정역이므로 $0, 1 \in A_i$이다. 따라서 $0, 1 \in S$ 이다.

임의의 $a, b \in S$ 일 때, 모든 $i \in I$에 대하여 $a-b, ab \in A_i$ 이므로 $a-b, ab \in S$ 이다. 그러므로 S는 부분환이다. 그리고 각 A_i가 가환환이므로 S도 가환환이다. 따라서 S는 단위원을 가진 가환환이다. 마지막으로 D가 정역이므로

$$a, b \in S,\ ab = 0 \Rightarrow a = 0 \text{ 또는 } b = 0$$

이다. 따라서 S는 D의 부분정역이다.

5.2.9. 단위원 1을 갖고, 영인자가 없는 유환환을 R이라하자.

$R = \{a_1, a_2, \cdots, a_n\}$이라 하면, 임의의 $a(\neq 0) \in R$에 대하여 $aR = \{aa_1, aa_2, \cdots, aa_n\} \subset R$이다.

R은 영인자가 없으므로 $aa_i = aa_j$이면 $a_i = a_j$이다(소거법칙 정리 5.2.8). 그러므로

$$|aR| = n \text{이고, } |aR| = n = |R|$$

이다. 따라서 $aR = R$이다. 그러면 $1 \in R = aR$이므로 적당한 $a_i \in R$가 존재하여 $aa_i = 1$이다.

같은 방법으로 Ra를 생각하면 적당한 $a_j \in R$가 존재하여 $a_j a = 1$이다. 그러므로

$$a_i = 1a_i = (a_j a)a_i = a_j(aa_i) = a_j 1 = a_j$$

이므로 $a^{-1} = a_i$가 되어 R은 나눗셈환이다.

5.2.10. $\mathbb{Z}_6$의 부분환 $3\mathbb{Z}_6 = \{0, 3\}$의 곱셈항등원은 3이고 $\mathbb{Z}_6$의 곱셈항등원은 1이다.

$\mathbb{Z} \times \mathbb{Z}$의 부분환 $\mathbb{Z} \times \{0\}$의 곱셈항등원은 $(1,0)$이고 $\mathbb{Z} \times \mathbb{Z}$의 곱셈항등원은 $(1,1)$이다.

5.2.11. 부분정역 D'의 영이 아닌 원소 $a(\neq 0) \in D'$에 대하여

$$a1_D = a = a1_{D'}$$

이다. 정역은 소거법칙이 성립하므로 $1_D = 1_{D'}$이다.

5.2.12. 부분환은 부분군이 되므로 부분군에서 부분환이 되는 것을 구하면 된다. 모두 순환군이므로 부분군은 모두 순환부분군이다.

(1) $0\mathbb{Z}_{14}$, $2\mathbb{Z}_{14}$, $7\mathbb{Z}_{14}$, $\mathbb{Z}_{14}$

(2) $0\mathbb{Z}_{18}$, $2\mathbb{Z}_{18}$, $3\mathbb{Z}_{18}$, $6\mathbb{Z}_{18}$, $9\mathbb{Z}_{18}$, $\mathbb{Z}_{18}$

5.2.13. (1) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$이다. 그리고 $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \in R$에 대하여

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} a-a' & b-b' \\ 0 & c-c' \end{pmatrix} \in R,\ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix} \in R$$

이므로 R은 $M_2(\mathbb{R})$의 부분환이다.

(2) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$이다. 그리고 $\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}, \begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix} \in R$에 대하여

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} - \begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} a-a' & 2(b-b') \\ b-b' & a-a' \end{pmatrix} \in R,\ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa'+2bb' & 2(ab'+ba') \\ ab'+ba' & aa'+2bb' \end{pmatrix} \in R$$

이므로 R은 $M_2(\mathbb{R})$의 부분환이다.

5.2.14. (1) $0 \in R_b$이다. 임의의 $\frac{x}{b^n}, \frac{y}{b^m} \in R_b$에 대하여

$$\frac{x}{b^n} - \frac{y}{b^m} = \frac{xb^m - yb^n}{b^{n+m}} \in R_b, \quad \frac{x}{b^n}\frac{y}{b^m} = \frac{xy}{b^{n+m}} \in R_b$$

이므로 R_b는 부분환이다.

한편 $b \nmid y$이면 $\frac{x}{b^n}\left(\frac{y}{b^m}\right)^{-1} = \frac{x}{b^n}\frac{b^m}{y} = \frac{x}{y}b^{m-n} \notin R_b$이므로 부분체가 아니다.

(2) $a \in \mathbb{Z}$에 대하여 $n = 0$일 때, $a = \frac{a}{b^0} \in R_b$이므로 $\mathbb{Z} \subset R_b$이다.

$a = 3, b = 2$이라하면, $\frac{3}{2} \in R_2$이지만 $\frac{3}{2} \notin \mathbb{Z}$이므로 $\mathbb{Z} \subsetneq R_b$이다.

임의의 $\frac{a}{b^n} \in R_b$에 대하여 $\frac{a}{b^n} \in \mathbb{Q}$이므로 $R_b \subset \mathbb{Q}$이다.

$a = 3, b = 2$이라하면 $\frac{2}{3} \in \mathbb{Q}$인데 $\frac{2}{3} \notin R_b$이므로 $R_b \subsetneq \mathbb{Q}$이다.

그러므로 $\mathbb{Z} \subsetneq R_b \subsetneq \mathbb{Q}$이다.

5.2.15. (1) $r + r = (r+r)^2 = r^2 + r + r + r^2 = r + r + r + r \Rightarrow r + r = 0$. 특히 $r = -r$이다.

(2) 임의의 $a, b \in R$에 대하여 $a + b = (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b \Rightarrow ab = -ba = ba$이다((1) 참조).

그러므로 R은 가환환이다.

5.2.16.

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(0,1)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

·	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,0)	(0,1)
(1,0)	(0,0)	(0,0)	(1,0)	(1,0)
(1,1)	(0,0)	(0,1)	(1,0)	(1,1)

5.2.17.

(1) 단원을 a라 하자. 임의의 $a \in R, a \neq 0$에 대하여 $a^2 = a$이므로

$$a^2 - a = 0 \Rightarrow a(a-1) = 0 \Rightarrow a - 1 = 0 \Rightarrow a = 1$$

(2) 임의의 $a(\neq 0,1) \in R$에 대하여, $a^2 = a$이므로

$$a^2 - a = 0 \Rightarrow a(a-1) = 0$$

이다. $a \neq 0, a - 1 \neq 0$이므로 a는 영인자이다.

====연습문제 (5.3)===========

5.3.1. $\phi : \mathbb{Z}_3 \to \mathbb{Z}_6$를 환준동형 사상이면

$$\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$$

이므로 $2 = \phi(1) = \phi(1)^2 = 4$ (모순)이다. 그러므로 $\phi : \mathbb{Z}_3 \to \mathbb{Z}_6$는 환준동형 사상이 아니다.

(별해) $\phi : \mathbb{Z}_3 \to \mathbb{Z}_6$를 환준동형 사상이면

$$\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) \Rightarrow \phi(1)(\phi(1) - 1) = 0 \Rightarrow \phi(1) = 0, 1, 3, 4$$

이어야 한다. 하지만 $\phi(1) = 1 + 1 = 2$가 되어 환 준동형사상이 아니다.

다음에 $\forall x, y \in \mathbb{Z}_3$에 대하여

$$\phi(x+y)=4(x+y)=4x+4y=\phi(x)+\phi(y)$$
$$\phi(xy)=\phi(xy)=4xy=4^2xy=4x4y=\phi(x)\phi(y)$$

이므로 ϕ는 환 준동형사상이다.

5.3.2. $\ker(\phi_5)=\{f(x)\in\mathbb{Q}[x]\mid 0=\phi(f(x))=f(5)\}$이므로

$x-5,\ 2(x-5),\ 3(x-5),\ 4(x-5),\ 5(x-5),\ x(x-5)$를 들 수 있다.

5.3.3. $a,\ b\in\mathbb{R}$일 때, 함수 $\phi:\ \mathbb{C}\to M_2(\mathbb{R}),\ \phi(a+bi)=\begin{pmatrix} a & b\\ -b & a\end{pmatrix}$

는 단사 환준동형사상임을 보여라.

(풀이) $\forall\, a+bi,\ c+di\in\mathbb{C}$에 대하여

$$\phi(a+bi+c+di)=\phi((a+c)+(b+d)i)=\begin{pmatrix} a+c & b+d\\ -(b+d) & a+c\end{pmatrix}=\begin{pmatrix} a & b\\ -b & a\end{pmatrix}+\begin{pmatrix} c & d\\ -d & c\end{pmatrix}=\phi(a+bi)+\phi(c+di)$$

$$\phi((a+bi)\cdot(c+di))=\phi(ac-bd+(bc+ad)i)=\begin{pmatrix} ac-bd & bc+ad\\ -(bc+ad) & ac-bd\end{pmatrix}=\begin{pmatrix} a & b\\ -b & a\end{pmatrix}\cdot\begin{pmatrix} c & d\\ -d & c\end{pmatrix}=\phi(a+bi)\cdot\phi(c+di)$$

이므로 ϕ는 환 준동형 사상이다.

$$\ker(\phi)=\left\{a+bi\in\mathbb{C}\;\middle|\;\begin{pmatrix} 0 & 0\\ 0 & 0\end{pmatrix}=\phi(a+bi)=\begin{pmatrix} a & b\\ -b & a\end{pmatrix}\right\}=\{0\}$$

이므로 ϕ는 단사 환 준동형 사상이다.

5.3.4. (1) 0, 1

(2) (예 5.3.13 참조) (1)에서 $\mathbb{Z}_9$의 멱등원이 2개이므로 환준동형 사상을 $f(1)=0,1$인 2개이다.

5.3.5. $\phi:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$를 환준동형 사상이라 하자.

$\forall\,(a,b)\in\mathbb{Z}\times\mathbb{Z}$에 대하여

$$\phi(a,b)=\phi(a(1,0)+b(0,1))=a\phi(1,0)+b\phi(0,1)$$

이므로 $(1,0),(0,1)$의 상에 의해 결정된다.

$\phi(1,0)=(a,b),\ \phi(0,1)=(c,d)$라 하자. 그러면

$$(a,b)=\phi(1,0)=\phi(1,0)^2=(a^2,b^2),\ (c,d)=\phi(0,1)=\phi(0,1)^2=(c^2,d^2)\ \Rightarrow\ a=0,\ 1,\ b=0,\ 1,\ c=0,\ 1,\ d=0,\ 1$$

이므로 $\phi(1,0)=(0,0),\ (1,0),\ (0,1),\ (1,1)$이다.

$\phi(0,1)=(0,0),\ (1,0),\ (0,1),\ (1,1)$

이때 $(0,0)=\phi((1,0)\cdot(0,1))=\phi(1,0)\phi(0,1)$이므로

$\phi(1,0)=(0,0)$이면 $\phi(0,1)=(0,0),\ (1,0),\ (0,1),\ (1,1)$이어야 하고

$\phi(1,0)=(1,0)$이면 $\phi(0,1)=(0,0),\ (0,1)$이어야 하고

$\phi(1,0)=(0,1)$이면 $\phi(0,1)=(0,0),\ (1,0)$이어야 하고

$\phi(1,0)=(1,1)$이면 $\phi(0,1)=(0,0)$이어야 한다.

그러므로 환준동형 사상은

$$\begin{aligned}\phi(a,b)&=a\phi(1,0)+b\phi(0,1)\\ &=(0,0),\ (b,0),\ (0,b),\ (b,b)\\ &\quad(a,0),\ (a,b),\ (0,a),\ (b,a),\ (a,a)\end{aligned}$$

로 9가지이다.

5.3.6. 환 준동형사상에서는 반드시 정의역의 덧셈 항등원과 상의 멱등원을 조사해 보아야 한다. 정의역의 생성원이 결정되면 준동형사상이 결정(정리 3.2.25)되므로 생성원에 대한 상만 조사하면 된다.

(1) f가 환 준동형 사상일 때 1의 상 $f(1)$에 의하여 결정된다.

$$f(1)=f(1^2)=f(1)^2\ \Rightarrow\ f(1)=0,1$$

이므로 $f(a)=0, f(a)=a$가 환준동형사상이 될 수 있다.

$f(a)=a$일 때, $\forall\, a,b\in\mathbb{Z}\ \ f(a+b)=[a+b]_7=[a]_7+[b]_7=f(a)+f(b)$

$f(ab)=[ab]_7=[a]_7[b]=f(a)f(b)$

이므로 f의 환 준동형 사상은 2가지이다.

(2) $\mathbb{Z}_{12}$에서 멱등원은 0,1,4,9 $f(x)=0,\ x,\ 4x,\ 9x$의 4가지 경우가 환준동형사상이 된다.

(3) f가 환 준동형 사상이라 하자.

$$(a,b)=f(1)=f(1^2)=f(1)^2=(a^2,b^2),\ \ a=0,\ 1,\ \ b=0,\ 1$$

이므로 $f(1)=(0,0),(0,1),(1,0),(1,1)$이다.

$\forall\, a,b\in\mathbb{Z},\ f(1)=(0,1)$일 때,

$$f(a+b)=(0,a+b)=(0,a)+(0,b)=f(a)+f(b)$$
$$f(ab)=(0,ab)=(0,a)(0,b)=f(a)f(b)$$

이다.

$f(1)=(1,0)$도 위와 같은 방법으로 하면 된다.

$f(1)=(1,1)$일 때, $f(a+b)=(a+b,a+b)=(a,a)+(b,b)=f(a)+f(b)$

$$f(ab)=(ab,ab)=(a,a)(b,b)=f(a)f(b)$$

$\therefore f$의 환 준동형 사상은 $f(1)=(0,0),\ (0,1),\ (1,0),\ (1,1)$인 4가지이다.

(4) f가 환 준동형 사상이라 하자.

$\mathbb{Z}$에서 멱등원은 $f(1,0)=f(0,1)^2,\ f(0,1)=f(0,1)^2$이므로 $f(1,0)=0\text{ or}1,\ f(0,1)=0\text{or}1$이다.

한편 $f(1,0)f(0,1)=f((1,0)(0,1))=f(0,0)=0$이다. $\mathbb{Z}$에선 영인자가 없으므로 $f(1,0)=0$이거나 $f(0,1)=0$이어야 한다.

$f(1,0)=0$이면 $f(0,1)=0,\ 1$이어야 하고,

$f(1,0)=1$이면 $f(0,1)=0$이어야 한다.

환준동형 사상은

$$\phi(a,b)=a\phi(1,0)+b\phi(0,1)=0,\ b,\ a$$

로 3가지이다.

(5) f가 환 준동형 사상이라 하자.

$\mathbb{Q}$에선 영인자가 없고 $f(1)=f(1^2)=f(1)^2$이므로 $f(1)$은 멱등원이다. $f(1)=0\text{or}1$이다.

$f(1)=0\text{or}1$인 경우, $f(a+b)=(a+b)f(1)=af(1)+bf(1)=f(a)+f(b)$,

$$f(ab)=abf(1)=abf(1^2)=af(1)bf(1)=f(a)f(b)$$

이다. 환 준동형 사상은 $f(a)=0\text{or}a$로 2가지이다.

(6) f가 환 준동형 사상이라 하자.

$\mathbb{Z}$에서 $f(1)=f(1^2)=f(1)^2$이므로 $f(1)=0\text{or}1$이다.

$f(1)=1$이면 $1=f(1)=f\left(\frac{2}{2}\right)=2f\left(\frac{1}{2}\right)$이 되어 모순이다. 따라서 환 준동형 사상은 $f(a)=0$으로 1가지이다.

5.3.7. 1) $f:2\mathbb{Z}\to3\mathbb{Z}$가 환 동형 사상이라 하자.

2가 $2\mathbb{Z}$의 생성원이므로 $f(2)=3a\ (\exists\, a\in\mathbb{Z})\Rightarrow f(2x)=3ax$가 성립한다.

f가 동형이므로 $f\neq0,\ \therefore a\neq0$이다.

$$3a2=f(2\cdot2)=f(2)f(2)=3a3a$$

인데 $a\neq0$이므로 $6=9a$ (모순)

$\therefore f$는 환 동형사상이 아니다.

(별해) 환 동형사상 $\phi:2\mathbb{Z}\to3\mathbb{Z}$라 하자.

2는 $2\mathbb{Z}$의 생성원이고, $\phi(2)=a\in3\mathbb{Z}$라 하면

$$\phi(4)=\phi(2+2)=\phi(2)+\phi(2)=2a$$
$$\phi(4)=\phi(2\cdot 2)=\phi(2)\cdot\phi(2)=a^2$$

이므로

$$2a=a^2 \Rightarrow a^2-2a=0 \Rightarrow a(a-2)=0$$

이므로 $a=0$또는 2이다.

$a=0$이면 전단사에 모순($\because \phi(0)=0$)

$a=2$이면 $a=2\notin 3\mathbb{Z}$

그러므로 $2\mathbb{Z}$에서 $3\mathbb{Z}$로의 환 동형사상은 존재하지 않는다.

2) $f:\mathbb{C}\to\mathbb{R}$가 환 동형사상이라 하자. 그럼 f가 전단사 함수여야 하므로 $f\neq 0$이다.

$f(1)$는 멱등원이므로 $f(1)=0$ or 1이다.

$f(i)$의 경우, $-f(1)=f(-1)=f(i^2)=f(i)f(i)=f(i)^2$이다.

만약 $f(1)=1$이라면 $f(i)^2=-1$인 $f(i)$가 $\mathbb{R}$에 존재하지 않으므로 모순이다. 따라서 $f(1)\neq 1$이다.

그러므로 $f(1)=0$이고 $f(i)^2=f(i^2)=0$이 되어, $f(i)=0$이 된다. 이는 $f=0$이 되어 모순이다. 따라서 f는 환 동형사상이 아니다.

(별해1) $f:\mathbb{C}\to\mathbb{R}$가 동형사상이라 하자. $f(i)=a\in\mathbb{R}$이라 하자. 그러면

$$-1=f(-1)=f(i^2)=f(i)^2=a^2$$

이 되어 $a\notin\mathbb{R}$이 되어 모순이다. 그러므로 동형사상이 존재하지 않는다.

(별해2) $f:\mathbb{R}\to\mathbb{C}$가 동형사상이라 하자. 그러면 $f(a)=i(\exists\, a\in\mathbb{R})$이다. f는 단사함수이므로

$$f(-1)=-1=i^2=f(a^2) \Rightarrow a^2=-1$$

이 되어 $a\notin\mathbb{R}$이 되어 모순이다. 그러므로 동형사상이 존재하지 않는다.

5.3.8. $f:\mathbb{Z}[\sqrt{2}]\to\mathbb{Z}[\sqrt{2}]$가 환 준동형사상이라 하자.

$$\forall\, x+y\sqrt{2}\in\mathbb{Z}[\sqrt{2}],\ f(x+y\sqrt{2})=xf(1)+yf(\sqrt{2})$$

이므로 $f(1), f(\sqrt{2})$의 상만 결정 되면 f가 결정된다. 이때

$$f(\sqrt{2})^2=f(\sqrt{2}^{\,2})=f(2)=2f(1)$$

이다. $f(1)$은 멱등원이므로 $f(1)=0$ or 1이다.

$i)\, f(1)=0$인 경우 $f(\sqrt{2})=0$이므로 f가 영사상이 되어 준동형사상이다.

$ii)\, f(1)=1$인 경우 $f(\sqrt{2})^2=2 \Rightarrow f(\sqrt{2})=\pm\sqrt{2}$이다.

ii-1) $f(\sqrt{2})=\sqrt{2}$이면 $f(x+y\sqrt{2})=x+y\sqrt{2}$이므로 f가 항등사상이므로 준동형사상이다.

ii-2) $f(\sqrt{2})=-\sqrt{2}$이면 $f(x+y\sqrt{2})=x-y\sqrt{2}$이다.

$\forall\, a+b\sqrt{2}, c+d\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$

$$\begin{aligned} f((a+b\sqrt{2})+(c+d\sqrt{2})) &= f((a+c)+(b+d)\sqrt{2}) \\ &= a+c-(b+d)\sqrt{2} \\ &= f(a+b\sqrt{2})+f(c+d\sqrt{2}), \end{aligned}$$

$$\begin{aligned} f((a+b\sqrt{2})(c+d\sqrt{2})) &= f((ac+2bd)+(ad+bc)\sqrt{2}) \\ &= ac+2bd-(ad+bc)\sqrt{2} \\ &= (a-b\sqrt{2})(c-d\sqrt{2})=f(a+b\sqrt{2})f(c+d\sqrt{2}) \end{aligned}$$

이므로 준동형사상이다. 따라서 총 환 준동형사상이 되는 f는 3가지이다.

5.3.9. $\forall\, a+bi, c+di\in\mathbb{C}$,

$$\begin{aligned} f(a+bi+c+di) &= f(a+c+bi+di)=a+c-(b+d)i \\ &= a-bi+c-di=f(a+bi)+f(c+di) \end{aligned}$$

$$\begin{aligned} f((a+bi)(c+di)) &= f(ac-bd+(ad+bc)i)=ac-bd-(ad+bc)i \\ &= (a-bi)(c-di)=f(a+bi)f(c+di) \end{aligned}$$

그러므로 f는 환 준동형사상이다. 분명히 전사함수이다.

$$\ker(f)=\{a+bi\mid 0=f(a+bi)=a-bi\}=\{0\}$$

이므로 f는 단사함수가 되어 동형사상이다.

5.3.10. (문제수정) 환 동형사상이 되는 다음 함수를 구하라.

(1) $f:\mathbb{Z}_{10}\to\mathbb{Z}_2\times\mathbb{Z}_5$

(2) $f:\mathbb{Z}_{12}\to\mathbb{Z}_3\times\mathbb{Z}_4$

(풀이) (1) $f:\mathbb{Z}_{10}\to\mathbb{Z}_2\times\mathbb{Z}_5$에 대하여 $f(a)=([a]_2,[a]_5)$라 하자.

임의의 $a,b\in\mathbb{Z}_{10}$에 대하여

$$f(a+b)=([a+b]_2,[a+b]_5)=([a]_2+[b]_2,[a]_5+[b]_5)$$
$$=([a]_2,[a]_5)+([b]_2,[b]_5)=f(a)+f(b)$$
$$f(ab)=([ab]_2,[ab]_5)=([a]_2[b]_2,[a]_5[b]_5)=([a]_2,[a]_5)([b]_2,[b]_5)=f(a)f(b)$$

이므로 환 준동형사상이다.

$$\ker(f)=\{a\mid f(a)=([a]_2,[a]_5)=(0,0)\}$$
$$=\{a\mid a=\mathrm{lcm}(2,5)m=10m,\ m\in\mathbb{Z}\}=\{0\}$$

이다. 따라서 f는 단사함수이다. $|\mathbb{Z}_{10}|=|\mathbb{Z}_2\times\mathbb{Z}_5|$이고, f가 단사이므로 f는 전사이다.

따라서, f는 환 동형사상이다.

(2) $f:\mathbb{Z}_{12}\to\mathbb{Z}_3\times\mathbb{Z}_4$에 대하여 $f(a)=([a]_3,[a]_4)$라 하면, (1)과 같은 방법으로 증명 가능하다.

5.3.11. $\phi\neq0$이므로 $\exists a\in R,\ \phi(a)\neq0$이다. 그리고 $\phi(a)=\phi(a\cdot1)=\phi(a)\phi(1)$이다. 임의의 $r'\in R'$에 대하여 영인자가 없으므로 소거법칙(정리 5.2.8)을 사용하면

$$\phi(a)r'=\phi(a)\phi(1)r'\ \Rightarrow\ r'=\phi(1)r'$$

이다. 또한 $\phi(a)=\phi(1\cdot a)=\phi(1)\phi(a)$이므로 위와 같은 방법으로 $r'=r'\phi(1)$이 성립한다. 그러므로 $\phi(1)=1_{R'}$이다.

5.3.12. ($\Rightarrow$) $\phi(u)$가 S의 단원이므로 $\phi(u)\neq0$이다. 따라서 $u\notin\ker\phi$이다.

($\Leftarrow$) $u\notin\ker\phi$라 하자.

$\phi(a)\neq0$이고 $u\in U(R)$이므로 $\exists u^{-1}\in R,\ u\cdot u^{-1}=1$이다.

$$\phi(1)=\phi(u\cdot u^{-1})=\phi(u)\phi(u^{-1})$$

이고 ϕ가 전사이므로 $Im(\phi)=S$이다. $\phi(1)$이 $Im(\phi)=S$의 단위원이므로 $\phi(1)=1_S$이다. 그러므로 $\phi(u)$는 S의 단원이다.

5.3.13. (문제수정) 체 F와 환 R에 대하여 함수 $\phi:F\to R$가 환 준동형사상이면, $\phi=0$이거나 단사임을 보여라.

(풀이) $\phi\neq0$일 때, ϕ가 단사임을 보이자.

$\exists a\in F,\phi(a)\neq0$이다. 이때 $\ker(\phi)\neq\{0\}$이면 $\exists b(\neq0)\in\ker\phi$이고, $\exists b^{-1}\in F,\ bb^{-1}=1$이다. 그러면

$$0\neq\phi(a)=\phi(a1)=\phi(abb^{-1})=\phi(a)\phi(b)\phi(b^{-1})=0$$

이므로 모순이다. 따라서 $\ker(\phi)=\{0\}$이 되어 ϕ는 단사함수이다.

5.3.14. (문제수정) 체 F에서 환 $R(\neq\{0\})$로의 환 준동형사상 $f:F\to R$이 전사이면, f는 동형사상임을 보여라.

(풀이) f가 전사이므로 $f(1)$은 $Im(f)=R$의 단위원이다.

이때 $\ker(f)\neq\{0\}$이면 $\exists b(\neq0)\in\ker(f)$이고, $\exists b^{-1}\in F,\ bb^{-1}=1$이다. 그러면

$$1_R=f(1)=f(bb^{-1})=f(b)f(b^{-1})=0$$

이므로 $R(\neq\{0\})$에 모순이다. 따라서 $\ker(\phi)=\{0\}$이 되어 ϕ는 단사함수이다. 그러므로 f는 동형사상이다.

(별해) $R(\neq\{0\})$이고 f가 전사이므로 $f\neq0$이다. 위 문제 5.3.13에 의하여 f는 단사함수이다. 그러므로 f는 동형사상이다.

5.3.15. $f(x)=a_0+a_1x+\cdots+a_nx^n,\ g(x)=b_0+b_1x+\cdots+b_nx^n\in R[x]$(필요하면 계수를 0으로 하여 $n+1$개항을 만듦)

$$
\begin{aligned}
&\phi_\sigma(f(x)+g(x))\\
&=\phi_\sigma((a_0+a_1x+\cdots+a_nx^n)+(b_0+b_1x+\cdots+b_nx^n))\\
&=\phi_\sigma((a_0+b_0)+(a_1+b_1)x+\ \cdots\ +(a_n+b_n)x^n)\\
&=\sigma(a_0+b_0)+\sigma(a_1+b_1)x+\cdots+\sigma(a_n+b_n)x^n\\
&=\sigma(a_0)+\sigma(b_0)+\sigma(a_1)x+\sigma(b_1)x+\cdots+\sigma(a_n)x^n+\sigma(b_n)x^n\\
&=[\sigma(a_0)+\sigma(a_1)x+\cdots+\sigma(a_n)x^n]+[\sigma(b_0)+\sigma(b_1)x+\cdots+\sigma(b_n)x^n]\\
&=\phi_\sigma(f(x))+\phi_\sigma(g(x)),
\end{aligned}
$$

$$
\begin{aligned}
&\phi_\sigma(f(x)g(x))\\
&=\phi_\sigma((a_0+a_1x+\cdots+a_nx^n)(b_0+b_1x+\cdots+b_nx^n))\\
&=\phi_\sigma((\Sigma_{i+j=0}^{i+j=n}\,a_ib_j)x^{i+j}\\
&=\sigma(\Sigma_{i+j=0}^{i+j=n}\,a_ib_j)x^{i+j}\\
&=(\Sigma_{i+j=0}^{i+j=n}\,\sigma(a_i)\sigma(b_j))x^{i+j}\\
&=\phi_\sigma(f(x))\phi_\sigma(g(x))
\end{aligned}
$$

이므로 ϕ_σ는 환 준동형사상이다.

5.3.16. (1) $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$, $g(x)=b_0+b_1x+b_2x^2+\cdots+b_nx^n$(필요하면 계수를 0으로 하여 $n+1$개항을 만듦)라 하자.

$$
\begin{aligned}
(f(x)+g(x))' &= (a_0+a_1x+a_2x^2+\cdots+a_nx^n+b_0+b_1x+b_2x^2+\cdots+b_nx^n)'\\
&= \{(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_n+b_n)x^n\}'\\
&= (a_1+b_1)+2(a_2+b_2)x+\cdots+n(a_n+b_n)x^{n-1}\\
&= (a_1+2a_2x+\cdots+nb_nx^{n-1})+(b_1+2b_2x+\cdots+nb_nx^{n-1})\\
&= f'(x)+g'(x)
\end{aligned}
$$

$$
\begin{aligned}
(af(x))' &= (a(a_0+a_1x+a_2x^2+\cdots+a_nx^n))' = (aa_0+aa_1x+aa_2x^2+\cdots+aa_nx^n)'\\
&= aa_1+2aa_2x+\cdots+naa_nx^{n-1} = a(a_1+2a_2x+\cdots+na_nx^{n-1}) = af'(x)
\end{aligned}
$$

$$
\begin{aligned}
(f(x)g(x))' &= ((a_0+a_1x+a_2x^2+\cdots+a_nx^n)(b_0+b_1x+b_2x^2+\cdots+b_nx^n))'\\
&= (a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\cdots+(a_nb_n)x^{2n})'\\
&= (a_0b_1+a_1b_0)+2(a_0b_2+a_1b_1+a_2b_0)x+\cdots+2n(a_nb_n)x^{2n-1}\\
&= (a_0b_1+(2a_0b_2+a_1b_1)x+\cdots+n(a_nb_n)x^{2n-1})+(a_2b_0+(2a_2b_0+a_1b_1)x+\cdots+n(a_nb_n)x^{2n-1})\\
&= f(x)g'(x)+f'(x)g(x)
\end{aligned}
$$

(2) $D(F[x])=f[x]$

5.3.17. (문제 수정) 함수 $\phi:\mathbb{H}\to M_2(\mathbb{C})$를

$$\phi(a+bi+cj+dk)=a\begin{pmatrix}1&0\\0&1\end{pmatrix}+b\begin{pmatrix}0&1\\-1&0\end{pmatrix}+c\begin{pmatrix}0&i\\i&0\end{pmatrix}+d\begin{pmatrix}i&0\\0&-i\end{pmatrix}$$

로 정의하면 ϕ가 단사 환 준동형사상임을 보여라

(풀이)
$$
\begin{aligned}
&\phi((a+bi+cj+dk)+(a'+b'i+c'j+d'k))\\
&=\phi((a+a')+(b+b')i+(c+c')j+(d+d')k)\\
&=(a+a')\begin{pmatrix}1&0\\0&1\end{pmatrix}+(b+b')\begin{pmatrix}0&1\\-1&0\end{pmatrix}+(c+c')\begin{pmatrix}0&i\\i&0\end{pmatrix}+(d+d')\begin{pmatrix}i&0\\0&-i\end{pmatrix}\\
&=\phi(a+bi+cj+dk)+\phi(a'+b'i+c'j+d'k)
\end{aligned}
$$

다음에 $A=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$, $B=\begin{pmatrix}0&i\\i&0\end{pmatrix}$, $C=\begin{pmatrix}i&0\\0&-i\end{pmatrix}$라 하면

$$A^2=B^2=C^2=-I_2,\quad AB=C=-BA,\ BC=A=-CB,\ CA=B=-AC$$

이므로

$$\begin{aligned}
&\phi((a+bi+cj+dk)(a'+b'i+c'j+d'k))\\
&=\phi((aa'-bb'-cc'-dd')+(ab'+ba'+cd'-dc')i+(ac'-bd'+ca'+db')j+(ad'+bc'-cb'+da')k)\\
&=(aa'-bb'-cc'-dd')\begin{pmatrix}1&0\\0&1\end{pmatrix}+(ab'+ba'+cd'-dc')\begin{pmatrix}0&1\\-1&0\end{pmatrix}\\
&\quad+(ac'-bd'+ca'+db')\begin{pmatrix}0&i\\i&0\end{pmatrix}+(ad'+bc'-cb'+da')\begin{pmatrix}i&0\\0&-i\end{pmatrix}\\
&=\left[a\begin{pmatrix}1&0\\0&1\end{pmatrix}+b\begin{pmatrix}0&1\\-1&0\end{pmatrix}+c\begin{pmatrix}0&i\\i&0\end{pmatrix}+d\begin{pmatrix}i&0\\0&-i\end{pmatrix}\right]\left[a'\begin{pmatrix}1&0\\0&1\end{pmatrix}+b'\begin{pmatrix}0&1\\-1&0\end{pmatrix}+c'\begin{pmatrix}0&i\\i&0\end{pmatrix}+d'\begin{pmatrix}i&0\\0&-i\end{pmatrix}\right]\\
&=\phi(a+bi+cj+dk)\phi(a'+b'i+c'j+d'k)
\end{aligned}$$

이다. 따라서 환 준동형사상이다.

그리고 $a+bi+cj+dk\in\ker(\phi)$라 하면

$$\begin{pmatrix}0&0\\0&0\end{pmatrix}=\phi(a+bi+cj+dk)=a\begin{pmatrix}1&0\\0&1\end{pmatrix}+b\begin{pmatrix}0&1\\-1&0\end{pmatrix}+c\begin{pmatrix}0&i\\i&0\end{pmatrix}+d\begin{pmatrix}i&0\\0&-i\end{pmatrix}=\begin{pmatrix}a+di&b+ci\\-b+ci&a-di\end{pmatrix}$$

에서 $a=b=c=d=0$이므로 단사함수이다.

5.3.18. (1) 임의의 $x, y\in R$에 대하여

$$\lambda_a(x+y)=a(x+y)=axay=\lambda_a(x)+\lambda_a(y)$$

이므로 $\lambda_a\in End(R)$이다.

(2) 분명히 $\lambda_e\in R'$이다. 다음에 임의의 $\lambda_a, \lambda_b\in R'$와 $x\in R$에 대하여

$$\begin{aligned}
&(\lambda_a+\lambda_b)(x)=\lambda_a(x)+\lambda_b(x)=ax+bx=(a+b)x=\lambda_{a+b}(x),\\
&\lambda_a\circ\lambda_b(x)=\lambda_a(\lambda_b(x))=\lambda_a(bx)=a(bx)=(ab)x=\lambda_{ab}(x)
\end{aligned}$$

이므로 $\lambda_a+\lambda_b=\lambda_{a+b}\in R'$, $\lambda_a\circ\lambda_b=\lambda_{ab}\in R'\Rightarrow\ \lambda_a+\lambda_b, \lambda_a\circ\lambda_b\in R'$가 되어 R'은 $(End(R),+,\circ)$의 부분환이다.

(3) 함수 $f:R\to R'$, $f(a)=\rho_a$가 동형사상임을 보이자.

$$f(a)=f(b)\Rightarrow\ \rho_a=\rho_b\Rightarrow\ \rho_a(1)=\rho_b(1)\Rightarrow\ a=b$$

f는 단사함수이다. 정의에 의하여 f는 전사함수이다.

다음에 (2)에 의하여

$$f(a+b)=\rho_{a+b}=\rho_a+\rho_b=f(a)+f(b),\quad f(ab)=\rho_{ab}=\rho_a\rho_b=f(a)f(b)$$

이므로 f는 환 준동형사상이다. 그러므로 f는 동형사상이 되어 $R\cong R'$이다.

5.3.19. $End(\mathbb{Z},+)=\{\rho_m\mid m\in\mathbb{Z}\}$, $End(\mathbb{Z}_n,+)=\{\rho_m\mid m\in\mathbb{Z}_m\}$이다. 하지만 $End(\mathbb{Z}_2\times\mathbb{Z}_2,+)\neq\{\rho_m\mid m\in\mathbb{Z}_2\times\mathbb{Z}_2\}$이다. 따라서 다음이 성립한다.

(1)과 (2)는 위 연습문제 5.3.18의 특수한 경우이다.

(3) $\mathbb{Z}_2\times\mathbb{Z}_2$의 생성원이 (1,0), (0,1)이므로 $|End(\mathbb{Z}_2\times\mathbb{Z}_2,+)|=16$이고 $|(\mathbb{Z}_2\times\mathbb{Z}_2,+,\cdot)|=4$이므로 동형이 아니다.

== 연습문제 (5.4) ==

5.4.1.

(1) $(2x+1)+(x+2)=0$

(2) $(x+1)-(2x+2)=-x-1$

(3) $(2x+1)(x+2)=2x^2+2x+2$

(4) $(2x^2+x+1)(2x+1)=x^3+x^2+1$

5.4.2. (문제수정) (4) $\mathbb{Z}_{12}$

(풀이)

(1) $\mathbb{Z}$는 정역이므로 $\mathbb{Z}[x]$도 정역이고, $U(\mathbb{Z}[x])=U(\mathbb{Z})$이므로 $U(\mathbb{Z}[x])=U(\mathbb{Z})=\{\pm1\}$

(2) $\mathbb{Q}$가 체이므로, $\mathbb{Q}[x]$는 정역이다. 따라서 $U(\mathbb{Q}[x]) = U(\mathbb{Q}) = \mathbb{Q} - \{0\}$

(3) $\mathbb{Z}_7$가 체이므로, $\mathbb{Z}_7[x]$는 정역이다. 따라서 $U(\mathbb{Z}_7[x]) = U(\mathbb{Z}_7) = \mathbb{Z}_7 - \{0\}$

(4) $\mathbb{Z}_{12}$는 정역이 아니므로 $U(\mathbb{Z}_{12}) = \{1,5,7,11\}$

5.4.3. 필요하면 계수를 0으로 하여 항의 개수를 $n+1$개로 맞춘 임의의 다항식

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \, (a_i \in R)$$
$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0 \, (b_i \in R)$$
$$h(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 \, (c_i \in R)$$

에 대하여

(R_1) $\forall f(x), g(x), h(x) \in R[x]$, $(f(x)+g(x))+h(x) = f(x)+(g(x)+h(x))$

$$\begin{aligned}(f(x)+g(x))+h(x) &= (a_n x^n + \cdots + a_1 x + a_0 + b_n x^n + \cdots + b_1 x + b_0) + c_n x^n + \cdots + c_1 x + c_0 \\ &= (a_n + b_n) x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0) + c_n x^n + \cdots + c_1 x + c_0 \\ &= (a_n + b_n + c_n) x^n + \cdots + (a_1 + b_1 + c_1)x + (a_0 + b_0 + c_0) \\ &= a_n x^n + \cdots + a_1 x + a_0 + (b_n + c_n) x^n + \cdots + (b_1 + c_1)x + (b_0 + c_0) \\ &= a_n x^n + \cdots + a_1 x + a_0 + (b_n x^n + \cdots + b_1 x + b_0 + c_n x^n + \cdots + c_1 x + c_0) \\ &= f(x) + (g(x) + h(x))\end{aligned}$$

(R_2) $\exists 0 \in R[x], \forall f(x) \in R[x], 0 + f(x) = f(x) + 0 = f(x)$

$$\begin{aligned}0 + f(x) &= 0 + a_n x^n + \cdots + a_1 x + a_0 \\ &= a_n x^n + \cdots + a_1 x + a_0 = f(x) \\ &= a_n x^n + \cdots + a_1 x + a_0 + 0 = f(x) + 0\end{aligned}$$

(R_3) $\forall f(x) \in R[x], \exists -f(x) \in R[x], f(x) + (-f(x)) = (-f(x)) + f(x) = 0$

$\exists -a_n, -a_{n-1}, \cdots, -a_0 \in R$, $\exists -f(x) = (-a_n)x^n + (-a_{n-1})x^{n-1} + \cdots + (-a_1)x + (-a_0) \in R[x]$

$$\begin{aligned}f(x) + (-f(x)) &= a_n x^n + \cdots + a_1 x + a_0 + (-a_n)x^n + (-a_{n-1})x^{n-1} + \cdots + (-a_1)x + (-a_0) \\ &= \{a_n + (-a_n)\}x^n + \cdots + \{a_1 + (-a_1)\}x + \{a_0 + (-a_0)\} \\ &= 0x^n + \cdots + 0x + 0 = 0 \\ &= \{(-a_n) + a_n\}x^n + \cdots + \{(-a_1) + a_1\}x + \{(-a_0) + a_0\} \\ &= (-a_n)x^n + (-a_{n-1})x^{n-1} + \cdots + (-a_1)x + (-a_0) + a_n x^n + \cdots + a_1 x + a_0 \\ &= (-f(x)) + f(x)\end{aligned}$$

(R_4) $\forall f(x), g(x) \in R[x]$, $f(x) + g(x) = g(x) + f(x)$

$$\begin{aligned}f(x) + g(x) &= a_n x^n + \cdots + a_1 x + a_0 + b_n x^n + \cdots + b_1 x + b_0 \\ &= (a_n + b_n) x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0) \\ &= (b_n + a_n) x^n + \cdots + (b_1 + a_1)x + (b_0 + a_0) \\ &= b_n x^n + \cdots + b_1 x + b_0 + a_n x^n + \cdots + a_1 x + a_0 \\ &= g(x) + f(x)\end{aligned}$$

(R_5) $\forall f(x), g(x), h(x) \in R[x]$, $\begin{cases} f(x)(g(x)+h(x)) = f(x)g(x) + f(x)h(x) \\ (f(x)+g(x))h(x) = f(x)h(x) + g(x)h(x) \end{cases}$을 보이자.

$$f(x)g(x) = d_{n+n}x^{n+n} + \cdots + d_1 x + d_0, \;\; d_i = \Sigma_{k=0}^{i} a_k b_{i-k} = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0,$$
$$f(x)h(x) = e_{n+n}x^{n+n} + \cdots + e_1 x + e_0, \;\; e_i = \Sigma_{k=0}^{i} a_k c_{i-k} = a_0 c_i + a_1 c_{i-1} + \cdots + a_i c_0,$$

$f(x)(g(x))+h(x)) = (a_n x^n +\cdots+ a_1 x + a_0)(b_n x^n +\cdots+ b_1 x + b_0 + c_n x^n +\cdots+ c_1 x + c_0)$

$= (a_n x^n +\cdots+ a_1 x + a_0)\{(b_n + c_n)x^n +\cdots+ (b_1 + c_1)x + (b_0 + c_0)\}$

$= r_{n+n}x^{n+n} + \cdots + r_1 x + r_0,\ r_i = \Sigma_{k=0}^{i} a_k (b_{i-k} + c_{i-k}),$

$= (d_{n+n}x^{n+n} + \cdots + d_1 x + d_0) + (e_{n+n}x^{n+n} + \cdots + e_1 x + e_0),\ d_i = \Sigma_{k=0}^{i} a_k b_{i-k},\ e_i = \Sigma_{k=0}^{i} a_k c_{i-k}$

$= f(x)g(x) + f(x)h(x)$

같은 방법으로 $(f(x)+g(x))h(x) = f(x)h(x)+g(x)h(x)$이 성립한다.

(R_6) 위와 같은 방법으로 $\forall f(x), g(x), h(x) \in R[x],\ (f(x)g(x))h(x) = f(x)(g(x)h(x))$이 성립한다.
따라서 $(R[x], +, \bullet)$은 환이다.

5.4.4. $(3x^{3+}2x)y^3 + (x^2 - 6x + 1)y^2 + (x^4 - 2x)y + (x^4 - 3x^2 + x)$

$= 3x^3 y^3 + 2xy^3 + x^2 y^2 - 6xy^2 + y^2 + x^4 y - 2xy + x^4 - 3x^2 + x$

$= (y+1)x^{4+}(3y^3)x^{3+}(y^2 - 3)x^2 + (2y^3 - 6y^2 - 2y + 1)x + y^2$

5.4.5. (1) 필요하면 계수를 0으로 하여 항의 개수를 $n+1$개로 맞춘 임의의 다항함수

$f(x) = a_n x^n + a_{n-1}x^{n-1} +\cdots+ a_1 x + a_0\ (a_i \in R)$

$g(x) = b_n x^n + b_{n-1}x^{n-1} +\cdots+ b_1 x + b_0\ (b_i \in R)$

$h(x) = c_n x^n + c_{n-1}x^{n-1} +\cdots+ c_1 x + c_0\ (c_i \in R)$

에 대하여 $(R_1) \sim (R_4)$의 증명은 위 문제 5.4.3과 같다.

(R_5) $\forall f(x), g(x), h(x) \in R[x], \begin{cases} f(x)(g(x))+h(x)) = f(x)g(x)+f(x)h(x) \\ (f(x)+g(x))h(x) = f(x)h(x)+g(x)h(x) \end{cases}$을 보이자.

$f(x)(g(x))+h(x)) = (a_n x^n +\cdots+ a_1 x + a_0)(b_n x^n +\cdots+ b_1 x + b_0 + c_n x^n +\cdots+ c_1 x + c_0)$

$= (a_n x^n +\cdots+ a_1 x + a_0)\{(b_n + c_n)x^n +\cdots+ (b_1 + c_1)x + (b_0 + c_0)\}$

$= a_n(b_n + c_n)x^{2n} +\cdots+ \{a_0(b_1 + c_1) + a_1(b_0 + c_0)\}x + a_0(b_0 + c_0)$

$= (a_n b_n + a_n c_n)x^{2n} +\cdots+ \{(a_0 b_1 + a_0 c_1) + (a_1 b_0 + a_1 c_0)\}x + a_0 b_0 + a_0 c_0)$

$= a_n b_n x^{2n} + a_n c_n x^{2n} +\cdots+ a_0 b_1 x + a_0 c_1 x + a_1 b_0 x + a_1 c_0 x + a_0 b_0 + a_0 c_0$

$= a_n b_n x^{2n} +\cdots+ a_0 b_1 x + a_1 b_0 + a_0 b_0 + a_n c_n x^{2n} +\cdots+ a_0 c_1 x + a_1 c_0 x + a_0 c_0$

$= f(x)g(x) + f(x)h(x))$

$(f(x)+g(x))h(x) = (a_n x^n +\cdots+ a_1 x + a_0 + b_n x^n +\cdots+ b_1 x + b_0)(c_n x^n +\cdots+ c_1 x + c_0)$

$= \{(a_n + b_n)x^n +\cdots+ (a_1 + b_1)x + (a_0 + b_0)\}(c_n x^n +\cdots+ c_1 x + c_0)$

$= (a_n + b_n)c_n x^{2n} +\cdots+ \{(a_1 + b_1)c_0 + (a_0 + b_0)c_1\}x + (a_0 + b_0)c_0$

$= (a_n c_n + b_n c_n)x^{2n} +\cdots+ \{(a_1 c_0 + b_1 c_0) + (a_0 c_1 + a_0 c_1)\}x + (a_0 c_0 + b_0 c_0)$

$= a_n c_n x^{2n} + b_n c_n x^{2n} +\cdots+ a_1 c_0 x + b_1 c_0 x + a_0 c_1 + a_0 c_1 x + a_0 c_0 + b_0 c_0$

$= a_n c_n x^{2n} +\cdots+ a_0 c_1 x + a_1 c_0 + a_0 c_0 + b_n c_n x^{2n} +\cdots+ b_0 c_1 x + b_1 c_0 x + b_0 c_0$

$= f(x)h(x) + g(x)h(x)$

(R_6) $\forall f(x), g(x), h(x) \in R[x],\ (f(x)g(x))h(x) = f(x)(g(x)h(x))$을 보이자.

$(f(x)g(x))h(x) = \{(a_n x^n +\cdots+ a_1 x + a_0)(b_n x^n +\cdots+ b_1 x + b_0)\}(c_n x^n +\cdots+ c_1 x + c_0)$

$$
\begin{aligned}
&= \left(a_n b_n x^{2n} + \cdots + a_1 b_0 x + a_0 b_1 x + a_0 b_0\right)(c_n x^n + \cdots + c_1 x + c_0) \\
&= a_n b_n c_n x^{3n} + \cdots + a_1 b_0 c_0 x + a_0 b_1 c_0 x + a_0 b_0 c_1 x + a_0 b_0 c_0 \\
&= (a_n x^n + \cdots + a_1 x + a_0)\left(b_n c_n x^{2n} + \cdots + b_1 c_0 x + b_0 c_1 x + b_0 c_0\right) \\
&= (a_n x^n + \cdots + a_1 x + a_0)\left\{(b_n x^n + \cdots + b_1 x + b_0)(c_n x^n + \cdots + c_1 x + c_0)\right\} \\
&= f(x)(g(x)h(x))
\end{aligned}
$$

따라서 $(P_F, +, \bullet)$은 F_F의 부분환이다.

(2) $F = \mathbb{Z}_2$이면 생성원 1에 대한 상은 0, 1뿐이므로 $|P_F| = 2$이지만 $|F[x]| = \infty$이므로 동형이 아니다.

== 연습문제 (5.5) ==

5.5.1.

(1) $f(x) = x^n + 1 \Rightarrow f(-1) = (-1)^n + 1 = -1 + 1 = 0$이므로 인수정리 5.5.4에 의하여 $f(x)$는 $x+1$의 배수이다.

(별해) $x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + \cdots - x + 1)$

(2) $f(x) = x^m + 2 \Rightarrow f(1) = 1 + 2 = 0$이므로 인수정리 5.5.4에 의하여 $f(x)$는 $x - 1 = x + 2$의 배수이다.

(별해) $x^m + 2 = x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \cdots + x + 1) = (x+2)(x^{m-1} + x^{m-2} + \cdots + x + 1)$

5.5.2. (1) $x = 0$일 때, $x^2 + 1 = 1$, $x = 1$일 때, $x^2 + 1 = 0$이므로 근은 1뿐이다.

(별해) $x^2 + 1 = x^2 - 1 = (x-1)(x+1)$에서 해는 $1 (= -1)$뿐이다.

(2) $x = 0$일 때, $x^5 + 3x^3 + x^2 + 2x = 0$, $x = 1$일 때, $x^5 + 3x^3 + x^2 + 2x = 2$

$x = 2$일 때, $x^5 + 3x^3 + x^2 + 2x = 4$, $x = 3 = -2$일 때, $x^5 + 3x^3 + x^2 + 2x = 4$

$x = 4 = -1$일 때, $x^5 + 3x^3 + x^2 + 2x = 0$

이므로 근은 0, 4이다.

(별해) $0 = x(x^4 + 3x^2 + x + 2) = x(x^4 - 2x^2 + x + 2) = x(x^4 + x - 2x^2 + 2) = x(x(x^3 + 1) - 2(x^2 - 1))$
$= x(x+1)(x^3 - x^2 + x - x + 1) = x(x+1)(x^3 - x^2 + 1)$

에서 해는 $0, -1 (= 4)$이다.

(3) $x = 0$일 때, $x^2 - x = 0$, $x = 1$일 때, $x^2 - x = 0$, $x = 2$일 때, $x^2 - x = 2$

$x = 3$일 때, $x^2 - x = 6$, $x = 4$일 때, $x^2 - x = 2$, $x = 5$일 때, $x^2 - x = 0$

$x = 6$일 때, $x^2 - x = 0$, $x = 7$일 때, $x^2 - x = 2$, $x = 8$일 때, $x^2 - x = 6$

$x = 9$일 때, $x^2 - x = 2$

이므로 근은 0, 1, 5, 6이다.

(별해) $0 = x^2 - x = x(x-1)$에서 근은 0, 1, 5, 6이다.

5.5.3. Fermat 정리에 의해 $x^4 = 1 (x \neq 0)$이므로 $f(x) = 2x^{219} + 3x^{74} + 2x^{57} + 3x^{44} = 2x^3 + 3x^2 + 2x + 3$이다.

$$
\begin{aligned}
&f(1) = 2 + 3 + 2 + 3 = 0, \\
&f(2) = 2 \cdot 3 + 3 \cdot 4 + 2 \cdot 2 + 3 = 0, \\
&f(3) = f(-2) = -2 \cdot 3 + 3 \cdot 4 - 2 \cdot 2 + 3 = 0, \\
&f(4) = f(-1) = -2 + 3 - 2 + 3 = 2 \neq 0
\end{aligned}
$$

이므로 $x = 1, 2, 3$이 해이다. $x = 0$일 때 분명히 원래 방정식의 해이다. 따라서 만족하는 해는 $x = 0, 1, 2, 3$이다.

(별해) Fermat 정리에 의해 $x^4 = 1 (x \neq 0)$이므로

$$2x^{219} + 3x^{74} + 2x^{57} + 3x^{44} = 2x^3 + 3x^2 + 2x + 3$$

$= (2x+3)(x^2+1) = (2x-2)(x^2-4) = 2(x-1)(x-2)(x+2)$

의 해는 $x = 1, 2, 3$이고 $x = 0$일 때 분명히 원래 방정식의 해이다. 따라서 만족하는 $x = 0, 1, 2, 3$ 이다.

5.5.4. $\mathbb{Z}_{11}$의 생성원은 2이므로 $2^1, 2^3 = 8, 2^7 = 7, 2^9 = 6$ (지수가 $\phi(11) = 10$과 서로소)이므로 2, 6, 7, 8이다.

5.5.5. $\mathbb{Z}_p$는 체이므로 $(\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}, \bullet)$는 곱셈에 대하여 순환군(정리 5.5.8)이다. 임의의 $a \in \mathbb{Z}_p^*$에 대하여 $|\mathbb{Z}_p^*| = p-1$ 이다. 따라서 $a^{p-1} = 1 (\because$ 라그랑주정리)이므로 $a^{p=a}$가 되어 a는 $x^p - x = 0$의 해이다. 그리고 0도 $x^p - x = 0$의 해이다. 즉

$$Z_p \subset \{a \in Z_p \mid a\text{는 } x^p - x \in \mathbb{Z}_p[x]\text{의 해}\}$$

이고 $x^p - x \in \mathbb{Z}_p[x]$의 해의 수는 p개 이하이므로

$$p = |\mathbb{Z}_p| \subset \{a \in Z_p \mid a\text{는 } x^p - x \in \mathbb{Z}_p[x]\text{의 해}\} \le p$$

이다. 그러므로 $Z_p = \{a \in Z_p \mid a\text{는 } x^p - x \in \mathbb{Z}_p[x]\text{의 해}\}$이다. 따라서 $x^p - x \in \mathbb{Z}_p[x]$는 p개의 근을 가진다.

5.5.6. (1) 몫 : $x^3 + x$, 나머지 : 1

(2) 몫 : $x^4 + x^3 + x^2 + x - 2$, 나머지 : $4x - 4$

(3) 몫 : $-2x^2 + 5x - 1$, 나머지 : 2

== 연습문제 (5.6) ==

5.6.1 (1) $x = 1$

5.6.2 (1) $x^4 + 4 = x^4 - 1 = (x^{-1})(x^2+1) = (x-1)(x+1)(x^2-4)$
$= (x-1)(x+1)(x-2)(x+2) = (x-1)(x-2)(x-3)(x-4)$

(2) $(x+1)(x-2)(x-4)$

(3) $(4x+2)(x+4)$

5.6.3 $\mathbb{Q}[x]$에서 인수분해하면 $(x^2+2)(x^2-2)$

$\mathbb{R}[x]$에서 인수분해하면 $(x^2+2)(x-\sqrt{2})(x+\sqrt{2})$

$\mathbb{C}[x]$에서 인수분해하면 $(x-\sqrt{2}\,i)(x+\sqrt{2}\,i)(x-\sqrt{2})(x+\sqrt{2})$

5.6.4 (1) $(x-1)(2x^2+3x+2)$

(2) $(x^2-x+1)(x^2+x+1)$

5.6.5 다항식이 3차이하인 경우 정리 5.6.4를 이용하자.

(1) 주어진 식을 $f(x)$라 하자. $f(0) \neq 0, f(1) \neq 0, f(2) \neq 0$이므로 $f(x)$는 0,1,2를 근으로 갖지 않는다. 따라서 $f(x)$의 기약다항식은 $2x^3 + x^2 + 2$이다.

(2) 주어진 식을 $f(x)$라 하자. $f(-1) = 0, f(0) \neq 0, f(1) \neq 0$이므로 $f(x) = (x+1)(x^3+2x-1)$이다.

(3) 주어진 식을 $f(x)$라 하자. $f(4) = f(-1) = 0$이고, $f(0) \neq 0, f(1) \neq 0, f(2) \neq 0, f(3) = f(-2) \neq 0$이므로
$f(x) = (x+1)(x^2+2x-1)$이다.

(4) 주어진 식을 $f(x)$라 하자. $f(3) = f(4) = 0$이고, $f(0), f(1), f(2), f(5), f(6) \neq 0$이므로 $f(x) = (x-3)(x-4)$이다.

(별해) $x^2 + 5 = x^2 + (4+3)x + 12 = (x+3)(x+4) = (x-4)(x-3)$

5.6.6

(1) $f(x)=x^3-2x-15$라 하자. 15의 약수 $\pm1,\ \pm3,\ \pm5,\ \pm15$에 대하여

$$f(\pm1)\neq0,\ f(\pm3)\neq0,\ f(\pm5)\neq0,\ f(\pm15)\neq0$$

이므로 따름정리 5.6.9와 정리 5.6.4(2)에 의하여 $f(x)$는 $\mathbb{Q}$위에서 기약이다.

(2) $f(x)=x^4+x^3+x^2+\frac{1}{2}$라 하자. $2f(x)=2x^4+2x^3+2x^2+1\in\mathbb{Z}[x]$가 $\mathbb{Q}$위에서 기약이면, $f(x)$는 $\mathbb{Q}$위에서 기약이다. $p=2$일 때 아이젠슈타인 판정법에 의하여 $2f(x)$는 $\mathbb{Q}$위에서 기약이므로 $f(x)$는 $\mathbb{Q}$위에서 기약이다.

(3) $f(x)=4x^3-2x^2+x+1$라 하자. 유리수 $\pm1,\ \pm\frac{1}{2},\ \pm\frac{1}{4}$에 대하여

$$f(\pm1)\neq0,\ f\left(\pm\frac{1}{2}\right)\neq0,\ f\left(\pm\frac{1}{4}\right)\neq0$$

이므로 정리 5.6.4(2)에 의하여 $f(x)$는 $\mathbb{Q}$위에서 기약이다.

(4) $f(x)=x^4+x^3+x^2+2x+1$라 하자. $f(-1)=0$이므로 인수정리에 의하여 $x+1$가 $f(x)$의 인수가 되어 $\mathbb{Q}$위에서 기약이 아니다.

5.6.7 (1) $3x-5=3(x-\frac{5}{3})$인데 $\frac{5}{3}\notin\mathbb{Z}$이므로 $\mathbb{Z}[x]$의 기약다항식이다.

(2) $3x-6=3(x-2)$인데 3은 $\mathbb{Z}$에서 단원이 아니므로 가약다항식이다.

(3) $3x-6=3(x-2)$인데 3은 $\mathbb{Q}$에서 단원이므로 $\mathbb{Q}[x]$의 기약다항식이다.

(4) $3x-6=3(x-2)$인데 3은 $3\times5=15=1$이므로 $\mathbb{Z}_7$에서 단원이다. 따라서 $\mathbb{Z}_7[x]$의 기약다항식이다.

5.6.8

(1) $f(x)=x^4+1$라 하자. $f(\pm1)\neq0$이므로 인수정리에 의하여 1차인수가 없다. 만약 2차인수의 곱으로 인수분해 된다면

$$x^4+1=(x^2+ax+b)(x^2+cx+d)=x^4+(a+c)x^3+(ac+b+d)x^2+(ad+bc)x+bd,\ a,\ b,\ c,\ d\in\mathbb{Z}$$

이다. $\begin{cases}a+c=0\\ac+b+d=0\\ad+bc=0\\bd=1\end{cases}$에서 $b=d=1$이거나 $b=d=-1$이다. $b=d=1$이면 $a+c=0,\ ac=-2\Rightarrow a^2=2$이므로 모순이다. $b=d=-1$이면 $a+c=0,\ ac=2\Rightarrow a^2=-2$이므로 모순이다. 따라서 2차인수가 없으므로 $\mathbb{Q}[x]$에서 기약이다(정리 5.6.7).

(2) $f(x)=x^3+3x^2-8$라 하자. $f(\pm1)\neq0,\ f(\pm2)\neq0,\ f(\pm4)\neq0,\ f(\pm8)\neq0$이므로 인수정리에 의하여 1차인수가 없 $\mathbb{Q}[x]$에서 기약이다(정리 5.6.4).

(3) $f(x)=x^{10}-\frac{25}{2}x^2+5x-15,\ 2f(x)=2x^{10}-25x^2+10x-30$에서 $p=5$인 경우 아이젠슈타인 판정법을 이용하면 $2f(x)$가 $\mathbb{Q}[x]$에서 기약이므로 $f(x)$도 $\mathbb{Q}[x]$에서 기약이다

(4) $f(x)=x^3+\frac{1}{2}x^2-\frac{3}{2}x+\frac{6}{5},\ 10f(x)=10x^3+5x^2-15x+12$에서 $p=5$인 경우 아이젠슈타인 판정법을 이용하면 $10f(x)$가 $\mathbb{Q}[x]$에서 기약이므로 $f(x)$도 $\mathbb{Q}[x]$에서 기약이다

5.6.9 $p=2$인 경우 Eisenstein 기약판정에 의해 $f(x)$는 $\mathbb{Q}$위에서 기약이다. $\mathbb{R}$위에서는 $f(1)=7>0$이고 $f(-1)=-11<0$이고 연속이므로 중간값정리에 의해 $f(a)=0$인 a가 존재한다. 따라서 $f(x)$는 기약이 아니다.

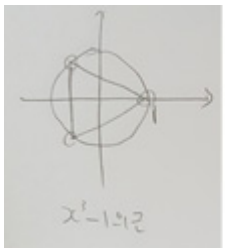
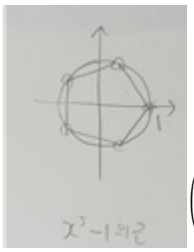
5.6.10 $n=2k$일 때, $f(x)=x^{2k}-1=(x^k+1)(x^k-1)$이고,

$n=2k-1$일 때, $f(x)=x^{2k-1}-1=(x-1)(x^{2k-2}+x^{2k-3}+\cdots+1)$이다.

$x^n=1$의 n개 근은 $x=e^{\frac{2\pi j}{n}i}=cox\frac{2\pi j}{n}+i\sin\frac{2\pi j}{n}(j=0,\ 1,\ \cdots,\ n-1)$이고

켤레 $cox\frac{2\pi j}{n}-i\sin\frac{2\pi j}{n}(j=0,\ 1,\ \cdots,\ n-1)$도 $x^n=1$의 근이 된다(참조 따름정리 9.1.5).

n이 홀수인 경우에는 1개의 실근 $1(j=0)$을 가지고 나머지는 $n-1(j=1,\ 2,\ \cdots,\ n-1)$개의 복소근이다.

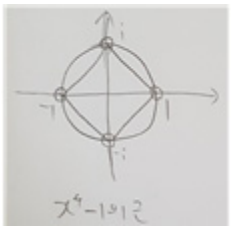
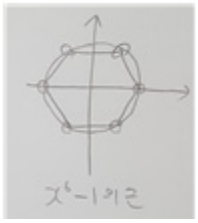
$\left(j=1,\ 2,\ \cdots,\ \frac{n-1}{2}\right)$과 $\left(j=n-1,\ \cdots,\ \frac{n-1}{2}+2,\ \frac{n-1}{2}+1\right)$은 켤레관계이므로

$$\left(x-cox\frac{2\pi j}{n}-i\sin\frac{2\pi j}{n}\right)\left(x-cox\frac{2\pi j}{n}+i\sin\frac{2\pi j}{n}\right)=x^2-2cox\frac{2\pi}{n}jx+1\in\mathbb{R}[x]\left(j=1,\ 2,\ \cdots,\ \frac{n-1}{2}\right)$$

은 $\mathbb{R}$ 위에서 기약다항식이다. 따라서 다음과 같이 기약다항식의 곱으로 인수분해된다.

$$\therefore x^n-1=(x-1)(x^2-2\cos\frac{2\pi}{n}x+1)(x^2-2\cos\frac{2\pi}{n}2x+1)\cdots(x^2-2\cos\frac{2\pi}{n}\frac{n-1}{2}x+1)$$

n이 짝수인 경우에는 2개의 실근 $\pm1\left(j=0,\ \frac{n}{2}\right)$을 가지고 나머지는 $n-2(j=1,\ 2,\ \cdots,\ \frac{n}{2}-1,\ \frac{n}{2}+1,\ \cdots,\ n-1)$개의 복소근이다.

$\left(j=1,\ 2,\ \cdots,\ \frac{n-2}{2}\right)$과 $\left(j=n-1,\ \cdots,\ \frac{n-2}{2}+2,\ \frac{n-2}{2}+1\right)$은 켤레관계이므로

$$\left(x-cox\frac{2\pi j}{n}-i\sin\frac{2\pi j}{n}\right)\left(x-cox\frac{2\pi j}{n}+i\sin\frac{2\pi j}{n}\right)=x^2-2cox\frac{2\pi}{n}jx+1\in\mathbb{R}[x]\left(j=1,\ 2,\ \cdots,\ \frac{n-2}{2}\right)$$

은 $\mathbb{R}$ 위에서 기약다항식이다. 따라서 다음과 같이 기약다항식의 곱으로 인수분해된다.

$$\therefore x^n-1=(x-1)(x+1)(x^2-2\cos\frac{2\pi}{n}x+1)(x^2-2\cos\frac{2\pi}{n}2x+1)\cdots(x^2-2\cos\frac{2\pi}{n}\frac{n-2}{2}x+1)$$

5.6.11 $x^n-pq,\ x^n+pq$는 $p=p$ or q에서 아이젠슈타인 판정법에 의해 $\mathbb{Q}$위에서 기약이다.

$\sqrt[n]{pq}$가 유리수라 하자. 그러면 $(\sqrt[n]{pq})^n-pq=0$이 되어 인수정리에 의하여 x^n-pq는 $\mathbb{Q}$위에서 $x-\sqrt[n]{pq}$인 일차인수를 가지게 되므로 x^n-pq가 $\mathbb{Q}$위에서 기약임에 모순이다. 따라서 $\sqrt[n]{pq}$는 무리수이다.

5.6.12 $\deg(f(x))=2$이므로 $\forall a\in\mathbb{Z}_p,\ f(a)\neq0\ \Leftrightarrow\ f(x)$는 $\mathbb{Z}_p$에서 기약이다.

따라서 $\forall c,d\in\mathbb{Z}_p,\ f(x)=(x-c)^2$ or $f(x)=(x-c)(x-d)$이면 가약이다.

$f(x)=(x-c)^2$인 경우 $c=\{1,2,\cdots,p\}\Rightarrow p$개

$f(x)=(x-c)(x-d)$인 경우 ${}_pC_2=\frac{p(p-1)}{2}$개

따라서 (기약다항식 전체의 개수)=(전체 다항식 수)-(기약다항식 수)

$$p^2-\left\{p+\frac{p(p-1)}{2}\right\}=\frac{p^2-p}{2}=\frac{p(p-1)}{2}$$

5.6.13

(1) $\mathbb{Z}_2[x]$의 2차 다항식은

x^2은 0이 근이므로 가약이다.

x^2+1은 1이 근이므로 가약이다.

x^2+x은 0이 근이므로 가약이다.

x^2+x+1은 0, 1이 근이 아니므로 기약이다.

그러므로 기약다항식은 x^2+x+1뿐이다.

(2) $x^2+1,\ x^2+x+2,\ x^2+2x+2,\ 2x^2+2,\ 2x^2+x+1,\ 2x^2+2x+1$

(3) $x^3+x+1,\ x^3+x^2+1$

5.6.14 페르마 정리에 의하여 $a\in\mathbb{Z}_p$에 의하여 $a^p=a$이다.

$$f(-a)=(-a)^p+a=-a+a=0$$

이다. 따라서 인수정리에 의하여 $f(x)$는 $x+a$를 인수로 가지므로 $f(x)$는 가약이다.

5.6.15 $f(x)=x^4+x^3+x^2-x+1$라 하면

$$f(-2)\equiv 16-8+4+2+1\equiv 15\equiv 0\,(\mathrm{mod}\,p)$$

이어야 하므로 $p=3,5$이다.

5.6.16 해가 a이므로 $a_n a^n+a_{n-1}a^{n-1}+\cdots+a_0=0$이다. 그러면 $a\neq 0$이므로 $\frac{1}{a}\in F$이다. 또한

$$a_n+\frac{1}{a}a_{n-1}+\cdots+a_0\frac{1}{a^n}=0$$

이므로 $\frac{1}{a}$은 $a_n+a_{n-1}x+\cdots+a_0x^n$의 해이다.

5.6.17

(1) 필요하면 계수를 0으로 하여 항의 개수를 $n+1$개로 맞춘 임의의 다항식

$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\,(a_i\in\mathbb{Z})$

$g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0\,(b_i\in\mathbb{Z})$에 대하여

$$\begin{aligned}
&\sigma_m(f(x)+g(x))\\
&=\sigma_m(a_nx^n+\cdots+a_1x+a_0+b_nx^n+\cdots+b_1x+b_0)\\
&=\sigma_m(a_n+b_n)x^n+\cdots+(a_1+b_1)x+(a_0+b_0))\\
&=[a_n+b_n]_mx^n+\cdots+[a_1+b_1]_mx+[a_0+b_0]_m\\
&=[a_n]_mx^n+[b_n]_mx^n+\cdots+[a_1]_mx+[b_1]_mx+[a_0]_m+[b_0]_m\\
&=([a_n]_mx^n+\cdots+[a_1]_mx+[a_0]_m)+([b_n]_mx^n+\cdots+[b_1]_mx+[b_0]_m)\\
&=\sigma_m(f(x))+\sigma_m(g(x))
\end{aligned}$$

$$\begin{aligned}
&\sigma_m(f(x)g(x))=\sigma_m(d_{n+n}x^{n+n}+\cdots+d_1x+d_0),\ d_i=\Sigma_{k=0}^{i}a_kb_{i-k}=a_0b_i+a_1b_{i-1}+\cdots+a_ib_0\\
&=\sigma_m(d_{n+n}x^{n+n}+\cdots+d_1x+d_0)\\
&=\Sigma_{i=0}^{2n}[\Sigma_{k=0}^{i}a_kb_{i-k}]_mx^i\\
&=\Sigma_{i=0}^{2n}\Sigma_{k=0}^{i}[a_kb_{i-k}]_mx^i\\
&=\Sigma_{i=0}^{2n}\Sigma_{k=0}^{i}[a_k]_m[b_{i-k}]_mx^i\\
&=\sigma_m(f(x))\sigma_m(g(x))
\end{aligned}$$

이므로 σ_m은 환 준동형사상이다.

(2) $f(x)$은 $\mathbb{Q}$ 위에서 기약이 아니라 하자. 그러면 적당한 1차 이상의 다항식 $g(x),h(x)\in\mathbb{Q}[x]$이 존재하여 $f(x)=g(x)h(x)$이다. 그러면 (1)에 의하여

$$\sigma_m(f(x))=\sigma_m(g(x)h(x))=\sigma_m(g(x))\sigma_m(h(x))$$

이고 $1\leqq\deg(g(x))=\sigma_m(g(x)),\ 1\leqq\deg(h(x))=\sigma_m(h(x))$이므로 $\sigma_m(g(x))\sigma_m(h(x))$은 $\mathbb{Z}_m[x]$에서 가약이다.

대우에 의하여 $f(x)$은 $\mathbb{Q}$위에서 기약이다.

(3) $m=5$인 경우

$$\sigma_5(x^3+17x+36)=x^3+2x+1$$

은 $\mathbb{Z}_5$ 위에서 기약이므로 (2)에 의하여 $x^3+17x+36$은 $\mathbb{Q}[x]$에서 기약이다.

== 연습문제 (5.7) ==

5.7.1.

(1) $\dfrac{x^2+1}{x+1}=\dfrac{(x+1)^2}{x+1}=x+1$

(2) $\dfrac{x^2+1}{x+1}+\dfrac{x^2+1}{x+1}=x+1+x+1=0$

(3) $\dfrac{x+1}{x}+\dfrac{x}{x+1}=\dfrac{(x+1)^2+x^2}{x(x+1)}=\dfrac{x^2+1+x^2}{x(x+1)}=\dfrac{1}{x(x+1)}$

5.7.2. (1) $p\mathbb{Z}=\{\cdots,-2p,-p,0,p,2p,\cdots\}$이므로 $0\in p\mathbb{Z}$이고 $1\notin p\mathbb{Z}$이다. 그러므로 $0\notin S, 1\in S$이다. S는 $\mathbb{Z}$에서 p의 배수 집합을 뺀 집합이므로, 임의의 $s,t\in S$는 법 p에서 0과 합동이 아니므로 st또한 법 p에서 0과 합동이 아니다. 따라서 S는 $\mathbb{Z}$의 곱셈집합이다.

(2) $0\in\mathbb{Z}$이므로 $0=\dfrac{0}{1}\in\mathbb{Q}_p$이다. 임의의 $\dfrac{a}{s},\dfrac{b}{t}\in\mathbb{Q}_p(a,b\in\mathbb{Z},s,t\in S)$에 대해 $st\in S$이므로

$$\frac{a}{s}-\frac{b}{t}=\frac{at-bs}{st}\in\mathbb{Q}_p,\ \frac{a}{s}\frac{b}{t}=\frac{ab}{st}\in\mathbb{Q}_p$$

이다. 따라서 $\dfrac{a}{s}-\dfrac{b}{t},\dfrac{a}{s}\dfrac{b}{t}\in\mathbb{Q}_p$이다. 따라서 $\mathbb{Q}_p<\mathbb{Q}$이다. 하지만 $\dfrac{1}{p}=p^{-1}\notin\mathbb{Q}_p$이므로 부분체가 아니다.

임의의 $a\in\mathbb{Z}$에 대하여 $a=\dfrac{a}{1}\in\mathbb{Q}_p$이므로 $\mathbb{Z}\subset\mathbb{Q}_p$이다. $\dfrac{1}{p+1}\in\mathbb{Q}_p$이지만 $\dfrac{1}{p+1}\notin\mathbb{Z}$이므로 $\mathbb{Z}\subsetneq\mathbb{Q}_p$이다.

임의의 $\dfrac{a}{s}\in\mathbb{Q}_p$에 대하여 $\dfrac{a}{s}\in\mathbb{Q}$이므로 $\mathbb{Q}_p\subset\mathbb{Q}$이다. $\dfrac{1}{p}\in\mathbb{Q}$인데 $\dfrac{1}{p}\in\mathbb{Q}_p$이면 적당한 $\dfrac{a}{s}\in\mathbb{Q}_p$에 대하여

$$\frac{1}{p}=\frac{a}{s}\ \Rightarrow\ ap=s\in S$$

가 되어 모순이다. 따라서 $\dfrac{1}{p}\notin\mathbb{Q}_p$이므로 $\mathbb{Q}_p\subsetneq\mathbb{Q}$이다.

그러므로 $\mathbb{Z}\subsetneq\mathbb{Q}_p\subsetneq\mathbb{Q}$이다.

(3) $Q(\mathbb{Q}_p)=\left\{\dfrac{a}{s}/\dfrac{c}{t}=\dfrac{at}{sc}\ \middle|\ \dfrac{a}{s},\dfrac{c}{t}(\neq 0)\in\mathbb{Q}_p,\ a,\ c(\neq 0)\in\mathbb{Z},s,t(\neq 0)\in S\right\}\subset\mathbb{Q}$

그리고 임의의 $\dfrac{a}{b}\in\mathbb{Q}$에 대하여 $\dfrac{a}{b}=\dfrac{a}{1}/\dfrac{b}{1}\in Q(\mathbb{Q}_p)$이므로 $\mathbb{Q}\subset Q(\mathbb{Q}_p)$이다. 따라서 $\mathbb{Q}=Q(\mathbb{Q}_p)$이다.

5.7.3. $D^*=D-\{0\}$, $S=D\times D^*=\{(a+bi,c+di)\,|\,a+bi\in D,c+di\in D^*\}$이고,
$(a+bi,c+di),(e+fi,g+hi)\in S$에 대하여

$$(a+bi,c+di)\sim(e+fi,g+hi)$$
$$\Leftrightarrow\ (ag-bh)+(ah+bg)i=(ce-df)+(cf+de)i$$

이므로,

$$Q(D)=S/\sim=\{p+qi\,|\,p,q\in\mathbb{Q}\}$$

단, $\dfrac{a+bi}{c+di}=\dfrac{(a+bi)(c-di)}{c^2+d^2}=\dfrac{(ac+bd)+(bc-bd)i}{c^2+d^2}$

5.7.4. (1) $Q(R,T)=\left\{\dfrac{b}{a}\,|\,b\in R,a\in T\right\}$, $a\in T$에 대하여 $\dfrac{a}{a}\in Q(R,T)$이다.

임의의 $\dfrac{c}{b}\in Q(R,T)$에 대하여

$$\frac{c}{b}\frac{a}{a}=\frac{ca}{ba}\sim\frac{c}{b}\ \Leftrightarrow\ cab=cba$$

이므로 $\frac{a}{a}$는 $Q(R, T)$의 곱셈항등원이다.

또한 함수 $f : R \to Q(R, T)$, $f(r) = \frac{ra}{a}$라 정의하자. f가 단사 준동형사상임을 보이면 $R \cong Imf < Q(R, T)$이므로 R을 $Q(R, T)$로 확장시킨다.

임의의 $r, s \in R$에 대하여

$$f(r+s) = \frac{(r+s)a}{a} = \frac{ra}{a} + \frac{sa}{a} = f(r) + f(s)$$
$$f(rs) = \frac{(rs)a}{a} = \frac{rsaa}{aa} = \frac{ra}{a}\frac{sa}{a} = f(r)f(s)$$

이므로 환 준동형사상이다. 그리고 $r \in \ker(f)$에 대하여 a는 영인자가 아니므로

$$\frac{0}{a} = f(r) = \frac{ra}{a} \Rightarrow raa = 0 \Rightarrow r = 0$$

이다. 그러므로 f는 단사함수가 되어 $Q(R, T)$는 R의 확장된 환이다.

(2) 임의의 $b \in T$는 $\frac{b}{bb} \in Q(R, T)$로 대응할 수 있다. 그러면

$$\frac{b}{bb}\frac{bb}{b} = \frac{bbb}{bbb} \sim \frac{a}{a}$$

이므로 $b^{-1} = \left(\frac{b}{bb}\right)^{-1} = \frac{bb}{b}$이다. 따라서 T의 모든 원소는 가역원이다.

5.7.5. 가환환 R의 영인자가 아닌 원소 a에 대하여 부분집합 $T = \{a^n \mid n \in \mathbb{N}\}$는 곱셈에 의하여 닫힌 집합이다. 4번에 의하여 $Q(R, T) = \left\{\frac{b}{a} \mid b \in R, a \in T\right\}$은 단위원을 가지며 R의 확장된 환이다.

5.7.6. $Q(\mathbb{Z}_6, \{1, 5\}) = \left\{\frac{a}{b} \mid a \in \mathbb{Z}_6, b \in \{1, 5\}\right\}$

$$= \left\{\frac{0}{1} = \frac{0}{5},\ \frac{1}{1} = \frac{5}{5},\ \frac{2}{1} = \frac{4}{5},\ \frac{3}{1} = \frac{3}{5},\ \frac{4}{1} = \frac{2}{5},\ \frac{5}{1} = \frac{1}{5}\right\}$$

따라서 6개이다.

== 연습문제 (6.1) ==

6.1.1. 주 아이디얼 환이다. 생성원은 약수에서 존재한다.

(1) $\mathbb{Z}_{12}$의 아이디얼 : $\{0\}$, $\mathbb{Z}_{12}$, $\langle 2\rangle$, $\langle 3\rangle$, $\langle 4\rangle$, $\langle 6\rangle$

(2) $\mathbb{Z}_{30}$의 아이디얼 : $\{0\}$, $\mathbb{Z}_{30}$, $\langle 2\rangle$, $\langle 3\rangle$, $\langle 5\rangle$, $\langle 6\rangle$, $\langle 10\rangle$, $\langle 15\rangle$

6.1.2. $H = \{(2a, 3b) \mid a, b \in \mathbb{Z}\}$라 하자.

$\forall (2a, 3b), (2a', 3b') \in H$, $\forall (r, s) \in Z \times Z$

$$(2a, 3b) - (2a', 3b') = (2(a-a'), 3(b-b')) \in H$$
$$(r, s)(2a, 3b) = (2ar, 3bs) \in H$$
$$(2a, 3b)(r, s) = (2ar, 3bs) \in H$$

따라서 H는 $\mathbb{Z} \times \mathbb{Z}$의 아이디얼이다.

$S = \{(2k, 3k) \mid k \in Z\}$라 하자.

$(1, 0) \in \mathbb{Z} \times \mathbb{Z}$, $(2k, 3k) \in S$에 대하여 $(1, 0)(2k, 3k) = (2k, 0) \notin S$이다.

따라서 H는 $\mathbb{Z} \times \mathbb{Z}$의 아이디얼이 아니다.

6.1.3. $H=\{(t,t)|t\in\mathbb{Z}_3\}$일 때, $\mathbb{Z}_3\times\mathbb{Z}_3$의 부분환은 되나 아이디얼이 되지 않는다.(위 6.1.2번 참조) 왜냐하면

$\forall\,(a,a),(b,b)\in H$

$$(a,a)-(b,b)=(a-b,a-b)\in H,$$
$$(a,a)(b,b)=(ab,ab)\in H$$

이므로 H는 $\mathbb{Z}_3\times\mathbb{Z}_3$의 부분환이다.

하지만 $(1,0)\in\mathbb{Z}_3\times\mathbb{Z}_3,(1,1)\in H$에 대하여 $(1,0)(1,1)=(1,0)\notin H$이다.

따라서 H는 $\mathbb{Z}_3\times\mathbb{Z}_3$의 아이디얼이 아니다.

6.1.4. S가 부분환이고 I가 아이디얼이므로 $\forall\,s+a,\,t+b\in S+I$에 대하여 $st\in S$이고 $sb,\,at,\,ab\in I$이다. 그러므로

$$(s+a)-(t+b)=(s-t)+(a-b)\in S+I,$$
$$(s+a)(t+b)=st+(sb+at+ab)\in S+I$$

이다. 따라서 H는 $\mathbb{Z}_3\times\mathbb{Z}_3$의 부분환이다.

6.1.5. a는 환 R의 원소이고 J는 환 R의 아이디얼이므로 ab는 J의 원소이다. 또한 b는 환 R의 원소이고 I는 환 R의 아이디얼이므로 ab는 I의 원소이다. 따라서 $ab\in I\cap J=\{0\}$이므로 $ab=0$이다. 같은 방법으로 $ba=0$임을 증명할 수 있다.

6.1.6. J를 $M_n(F)$의 아이디얼이라 하자. $\{0\}\neq J$이면 $\mathbb{O}\neq A\in J$인 행렬이 존재한다. 이때 A의 (r,s) 성분 $a(\neq 0)\in F$가 0이 아니라 하자. 또한 $E_{ij}\in M_n(F)$를 (i,j) 성분만 1이고 나머지 성분은 0인 행렬이라 하자. 그러면

$$A_{11}=E_{1r}AE_{s1}=aE_{11},\quad A_{22}=E_{2r}AE_{s2}=aE_{22},\quad\cdots\quad,\quad A_{nn}=E_{nr}AE_{sn}=aE_{nn}$$

은 J가 아이디얼이므로 모두 J의 원소이다.

(예를 들면 (1,2) 성분 $b\neq 0$인 행렬 $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$에 대하여 $A_{11}=E_{11}AE_{21}=\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}=\begin{pmatrix}b&0\\0&0\end{pmatrix}=b\begin{pmatrix}1&0\\0&0\end{pmatrix}=bE_{11}$)

그러면 J가 아이디얼이고 $a\neq 0$이 체 F의 원소이므로

$$I_n=E_{11}+E_{22}+\cdots+E_{nn}=a^{-1}A_{11}+a^{-1}A_{22}+\cdots+a^{-1}A_{nn}\in J$$

이 되어 $J=M_n(F)$이다(정리 6.1.6). 그러므로 $M_n(F)$는 단순환이다.

6.1.7. 먼저 I는 J의 아이디얼임을 보이자.

임의의 $\begin{pmatrix}0&a\\0&0\end{pmatrix},\begin{pmatrix}0&b\\0&0\end{pmatrix}\in I$와 $\begin{pmatrix}0&c\\0&0\end{pmatrix}\in J$에 대하여

$$\begin{pmatrix}0&a\\0&0\end{pmatrix}-\begin{pmatrix}0&b\\0&0\end{pmatrix}=\begin{pmatrix}0&a-b\\0&0\end{pmatrix}\in I,$$
$$\begin{pmatrix}0&c\\0&0\end{pmatrix}\begin{pmatrix}0&a\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\in I,$$
$$\begin{pmatrix}0&a\\0&0\end{pmatrix}\begin{pmatrix}0&c\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\in I$$

이므로 I는 J의 아이디얼이다. 다음에 J는 R의 아이디얼임을 보이자.

임의의 $\begin{pmatrix}0&a\\0&0\end{pmatrix},\begin{pmatrix}0&b\\0&0\end{pmatrix}\in J$와 $\begin{pmatrix}x&y\\0&z\end{pmatrix}\in R$에 대하여

$$\begin{pmatrix}0&a\\0&0\end{pmatrix}-\begin{pmatrix}0&b\\0&0\end{pmatrix}=\begin{pmatrix}0&a-b\\0&0\end{pmatrix}\in J,$$
$$\begin{pmatrix}x&y\\0&z\end{pmatrix}\begin{pmatrix}0&a\\0&0\end{pmatrix}=\begin{pmatrix}0&xa\\0&0\end{pmatrix}\in J,$$
$$\begin{pmatrix}0&a\\0&0\end{pmatrix}\begin{pmatrix}x&y\\0&z\end{pmatrix}=\begin{pmatrix}0&az\\0&0\end{pmatrix}\in J$$

이므로 J는 R의 아이디얼이다. 그리고

$$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}1&1\\0&\frac{1}{2}\end{pmatrix}=\begin{pmatrix}0&\frac{1}{2}\\0&0\end{pmatrix}\notin I$$

이므로 I는 R의 아이디얼 이 아니다.

6.1.8. 먼저 S는 $M_2(F)$의 우 아이디얼임을 보이자.

임의의 $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix} \in S$와 $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(F)$에 대하여

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-a' & b-b' \\ 0 & 0 \end{pmatrix} \in S,$$
$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} xa & ay \\ 0 & 0 \end{pmatrix} \in S$$

이므로 S는 $M_2(F)$의 우 아이디얼이다. 하지만

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} xa & xb \\ za & zb \end{pmatrix} \notin S$$

이므로 좌 아이디얼(left ideal)이 아니다.

6.1.9. 임의의 $r(x)f(x)+s(x)g(x), r'(x)f(x)+s'(x)g(x) \in N,\ h(x) \in F[x]$에 대하여

$$[r(x)f(x)+s(x)g(x)] - [r'(x)f(x)+s'(x)g(x)] = (r(x)-r'(x))f(x)+(s(x)-s'(x))g(x) \in N,$$
$$h(x)[r(x)f(x)+s(x)g(x)] = (h(x)r(x))f(x)+(h(x)s(x))g(x) \in N$$

이므로 N은 가환환 $F[x]$의 아이디얼이다.

$f(x), g(x)$ 둘 다 F 위에서 차수가 다르고 기약이면 $\gcd(f(x), g(x)) = 1$이므로

유클리드 호제법을 이용하면 적당한 $h(x), r(x) \in F[x]$에 대하여

$$1 = h(x)f(x)+r(x)g(x) \in N$$

이다. 그러면 $N = F[x]$이 되어 모순이다. 그러므로 $f(x), g(x)$ 둘 다 F 위에서 기약일 수 없다.

6.1.10. (1) 임의의 $\sum_{i=1}^{n} a_i b_i,\ \sum_{i=1}^{n} a_i' b_i' \in AB$와 $r \in R$에 대하여

$$\sum_{i=1}^{n} a_i b_i - \sum_{i=1}^{n} a_i' b_i' = \sum_{i=1}^{n} (a_i b_i - a_i' b_i') \in AB,$$
$$r\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (ra_i) b_i \in AB$$

이므로 AB는 R의 아이디얼이다.

(2) 아이디얼의 정의에 의하여

$$\sum_{i=1}^{n} a_i b_i \subset A \cap B$$

이므로 $AB \subset (A \cap B)$이다.

6.1.11. 모든 $a, b \in (A:B)$와 $r \in R$에 대하여

$$(a-b)B \subset aB - bB \subset A \ \Rightarrow\ a-b \in (A:B)$$
$$(ra)B = r(aB) \subset rA \subset A \ \Rightarrow\ ra \in (A:B),$$
$$(ar)B = a(rB) \subset aB \subset A \ \Rightarrow\ ar \in (A:B)$$

이므로 $(A:B)$는 R의 아이디얼이다.

6.1.12. (1) 모든 $a, b \in Ann(x)$와 $r \in R$에 대하여

$$(a-b)x = ax - bx = 0 \ \Rightarrow\ a-b \in Ann(x)$$
$$(ra)x = r(ax) = r0 = 0 \ \Rightarrow\ ra \in Ann(x),$$
$$(ar)x = (ra)x = r(ax) = r0 = 0 \ \Rightarrow\ ar \in Ann(x)$$

이므로 $Ann(x)$는 R의 아이디얼이다.

(2) 모든 $a, b \in Ann(X)$와 $r \in R$에 대하여

$$(a-b)X \subset aX - bX = \{0\} \ \Rightarrow\ a-b \in Ann(X)$$
$$(ra)X = r(aX) = r\{0\} = \{0\} \ \Rightarrow\ ra \in Ann(X),$$
$$(ar)X = (ra)X = r(aX) = r\{0\} = \{0\} \ \Rightarrow\ ar \in Ann(X)$$

이므로 $Ann(X)$는 R의 아이디얼이다.

(3) $Ann(2)=\{0, 6\}$
$Ann(\{2, 3\})=\{0\}$

6.1.13. (문제수정) 가환환 R의 닐래디칼 $N(R)=\{a\in R \mid a^n=0,\ \exists n\in\mathbb{N}\}$에 의한 잉여환 $R/N(R)$은 $\overline{0}(=0+N(R))$ 이외의 멱영원이 없음을 보여라.
(풀이) $r+N(R)\in R/N(R)$이 멱영원이라 하자. 그러면 적당한 $n\in\mathbb{N}$에 대하여

$$0+N(R)=(r+N(R))^n=r^n+N(R)\ \Rightarrow\ r^n\in N(R)\ \Rightarrow\ (r^n)^m=r^{nm}\in N(\exists m\in\mathbb{N})\ \Rightarrow\ r\in N(R)$$

이므로 $r+N(R)=0+N(R)$이다.

6.1.14. (문제수정) 가환환 R에 대하여 다음 물음에 답하라.
(1) R의 아이디얼 N에 대하여 $\sqrt{N}=\{a\in R \mid \exists n\in\mathbb{N},\ a^n\in N\}$은 R의 아이디얼임을 보여라. 이 아이디얼 $\sqrt{N}$을 N의 래디컬(radical)이라 한다.
(2) (정리 6.1.20) (1998학년도 임용시험 출제) $N(R)=\{a\in R \mid a^n=0,\ \exists n\in\mathbb{N}\}$은 R의 아이디얼임을 보여라. 아이디얼 $N(R)$을 닐래디칼(nilradical)이라 한다.
(풀이) (1) $i)$ 임의의 $a, b\in\sqrt{N}$에 대하여 $a^n, b^m\in N$이라 하자.

$$(a-b)^{n+m}=\sum_{k=0}^{m}\binom{n}{k}a^{n+m-k}b^k+\sum_{k=m+1}^{n+m}\binom{n}{k}a^{n+m-k}b^k\in N,\ \begin{cases}a^{n+m-k}b^k\in N, \text{ if } k\leqq m \text{ then } a^{n+m-k}\in N\\ a^{n+m-k}b^k\in N, \text{ if } k>m \text{ then } b^k\in N\end{cases}$$

이므로 $a-b\in\sqrt{N}$이다.
$ii)$ 모든 $r\in R$에 대하여

$$(ar)^n=a^nr^n\in N,\ (ra)^n=r^na^n\in N$$

이다. 따라서 $ar, ra\in\sqrt{N}$이다.
$i), ii)$에 의해 $\sqrt{N}$은 R의 아이디얼 이다.

(2) (1)에서 $N=\{0\}$인 경우를 생각하면 된다.

6.1.15.
$\mathbb{Z}/18\mathbb{Z}$는 제1동형정리에 의해 $\mathbb{Z}_{18}$와 동형이다. 그러므로 $\mathbb{Z}/18\mathbb{Z}$의 아이디얼을 구하기 위해서 $\mathbb{Z}_{18}$의 모든 아이디얼을 구해보자. $\mathbb{Z}_{18}$의 모든 아이디얼은 18의 약수를 생각해볼 수 있다.
{0}, $\mathbb{Z}_{18}$, <2>, <3>, <6>, <9> 가 $\mathbb{Z}_{18}$의 모든 아이디얼이 될 수 있다. 따라서 이에 대응되는 $\mathbb{Z}/18\mathbb{Z}$의 아이디얼을 모두 구해보면 $<18\mathbb{Z}>$, $<1+18\mathbb{Z}>$, $<2+18\mathbb{Z}>$, $<3+18\mathbb{Z}>$, $<6+18\mathbb{Z}>$, $<9+18\mathbb{Z}>$이다.

6.1.16. 체 F의 아이디얼은 {0}과 자기 자신 F뿐이다. 따라서 $F/\{0\}\cong F$, $F/F\cong\{0\}$이 성립함을 알 수 있다.

6.1.17. $\phi' : R/N\to R'/N'$, $\phi'(r+N)=\phi(r)+N'$이라 하자. ϕ'이 잘 정의됨을 보이자.
$r+N, s+N\in R/N$에 대하여

$$r+N=s+N\ \Rightarrow\ r-s\in N\ \Rightarrow\ \phi(r-s)\in\phi(N)\subset N'$$
$$\Rightarrow\ \phi(r)-\phi(s)\in N'\ \Rightarrow\ \phi(r)+N'=\phi(s)+N'\ \Rightarrow\ \phi'(r+N)=\phi(s+N)$$

이므로 잘 정의된다.

$$\phi'(r+N+s+N)=\phi'(r+s+N)=\phi(r+s)+N'$$
$$=\phi(r)+\phi(s)+N'=\phi(r)+N'+\phi(s)+N'=\phi'(r+N)+\phi'(s+N),$$
$$\phi'((r+N)(s+N))=\phi'(rs+N)=\phi(rs)+N'$$
$$=\phi(r)\phi(s)+N'=(\phi(r)+N')(\phi(s)+N')=\phi'(r+N)\phi'(s+N)$$

이므로 환 준동형사상이다.

== 연습문제 (6.2) ==

6.2.1. (1) 임의의 $a, b\in(H\cap K), k\in K$에 대하여

$$a-b,\ ak,\ ka\in H,\ a-b,\ ak,\ ka\in K(\because H\lhd R)$$
$$a-b,\ ak,\ ka\in H\cap K$$
$$\therefore (H\cap K)\lhd K$$

(2) $f : K\to(H+K)/H,\ f(k)=k+H$라 정의하자.

임의의 $k, k'\in K$에 대하여

$$f(k+k')=k+k'+H=(k+H)+(k'+H)=f(k)+f(k')$$
$$f(kk')=kk'+H=(k+H)(k'+H)=f(k)f(k')$$

이므로 환준동형사상이다. 다음에

$$\ker(f)=\{a\in K\,|\,H=f(a)=a+H\}=\{a\in K\,|\,a\in H\}=H\cap K$$

이고 분명히 $k+h+H=k+H$이므로 f는 전사함수이다. 따라서 제1동형정리에 의해 다음이 성립한다.

$$K/H\cap K=K/\ker(f)\cong Im(f)=(H+K)/H$$

(별해) $f : K/H\cap K\to(H+K)/H,\ f(k+H\cap K)=k+H$라 정의하자.

$$k+H\cap K=k'+H\cap K\Rightarrow k-k'\in H\cap K\subset H\Rightarrow k+H=k'+H\Rightarrow f(k+H)=f(k'+H)$$

이므로 f는 잘 정의된다. 임의의 $k+H, k'+H\in K/H\cap K$에 대하여

$$f((k+H\cap K)+(k'+H\cap K))=f(k+k'+H\cap K)=k+k'+H=(k+H)+(k'+H)=f(k+H\cap K)+f(k'+H\cap K)$$
$$f((k+H\cap K)(k'+H\cap K))=f(kk'+H\cap K)=kk'+H=(k+H)(k'+H)=f(k+H\cap K)f(k'+H\cap K)$$

이므로 환준동형사상이다. 다음에

$$\ker(f)=\{a+H\cap K\in K/H\,|\,H=f(a)=a+H\}=\{a+H\cap K\in K/H\,|\,a\in H\}=\{0+H\cap K\}$$

이므로 f단사함수이고 분명히 f는 전사함수이므로 동형사상이다. 따라서

$$K/H\cap K\cong(H+K)/H$$

6.2.2. (환 제 2동형정리) 환 R의 두 아이디얼 H, K 가 $H<K$ 일 때, 다음을 증명하라.

(1) $(K/H)\lhd(G/H)$

(2) $G/K\cong(G/H)/(K/H)$

(풀이) (1) $a+H, b+H\in K/H,\ r+H\in G/H$에 대하여

$$(a+H)-(b+H)=a-b+H\in K/H,$$
$$(a+H)(r+H)=ar+H\in K/H,$$
$$(r+H)(a+H)=ra+H\in K/H$$

이므로 $(K/H)\lhd(G/H)$이다.

(2) $f : G\to(G/H)/(K/H),\ f(r)=(r+H)+K/H$라 정의하자. 분명히 전사함수이다.

임의의 $r, r'\in G$에 대하여

$$f(r+r')=(r+r'+H)+K/H=((r+H)+K/H)+((r'+H)+K/H)=f(r)+f(r')$$
$$f(rr')=(rr'+H)+K/H=((r+H)+K/H)((r'+H)+K/H)=f(r)f(r')$$

이므로 환준동형사상이다. 다음에

$$\ker(f)=\{a\in G\,|\,(0+H)+K/H=f(a)=(a+H)+K/H\}=\{a\in G\,|\,a+H\in K/H\}=\{a\in G\,|\,a\in K\}=K$$

이고 분명히 f는 전사함수이므로 제1동형정리에 의해 다음이 성립한다.

$$G/K=K/\ker(f)\cong Im(f)=(G/H)/(K/H)$$

(별해) $f : G/K\to(G/H)/(K/H),\ f(r+K)=(r+H)+K/H$라 정의하자.

$$r+K=r'+K\Rightarrow r-r'\in K\Rightarrow(r-r'+H)+K/H=(0+H)+K/H$$
$$\Rightarrow(r+H)+K/H=(r'+H)+K/H\Rightarrow f(r+K)=f(r'+K)$$

이므로 f는 잘 정의된다. 임의의 $r+K, r'+K\in G/K$에 대하여

$$f((r+K)+(r'+K))=f(r+r'+K)=(r+r'+H)+K/H=((r+H)+K/H)+((r'+H)+K/H)=f(r+K)+f(r'+K)$$
$$f((r+K)(r'+K))=f(rr'+K)=(rr'+H)+K/H=((r+H)+K/H)((r'+H)+K/H)=f(r+K)f(r'+K)$$

이므로 환준동형사상이다. 다음에

$$\ker(f)=\{a+K\in G/K\,|\,(0+H)+K/H=f(a+K)=(a+H)+K/H\}$$
$$=\{a+K\in G/K\,|\,a+H\in K/H\}=\{a+K\in G/K\,|\,a\in K\}=\{0+K\}$$

이므로 f단사함수이고 분명히 f는 전사함수이므로 동형사상이다. 따라서

$$G/K\cong(G/H)/(K/H)$$

6.2.3. $\mathbb{Z}/Im(\phi)=\mathbb{Z}/5\mathbb{Z}\cong\mathbb{Z}_5$ 이므로 체가 된다(정리 5.2.9).

6.2.4. $\forall a+bi, c+di\in\mathbb{C}$에 대하여

$$f((a+bi)+(c+di))=f((a+c)+(b+d)i)=\begin{pmatrix}a+c & -b-d\\ b+d & a+c\end{pmatrix}=\begin{pmatrix}a-b\\ b\ \ a\end{pmatrix}+\begin{pmatrix}c-d\\ d\ \ c\end{pmatrix}=f(a+bi)+f(c+di),$$

$$f((a+bi)(c+di))=f((ac-bd+(ad+bc)i)=\begin{pmatrix}ac-bd & -(ad+bc)\\ ad+bc & ac-bd\end{pmatrix}=\begin{pmatrix}a-b\\ b\ \ a\end{pmatrix}\begin{pmatrix}c-d\\ d\ \ c\end{pmatrix}$$

$$=f(a+bi)f(c+di)$$

이므로 f는 환 준동형사상이다.

$\ker(f)=\{0\}$이므로 제1동형정리에 의하여 $\mathbb{C}\cong\mathbb{C}/\ker(f)\cong f(\mathbb{C})$은 체이다. 즉 $M_2(\mathbb{R})$은 체가 아니지만 부분환으로 부분체를 가질 수 있다.

6.2.5. 제1동형정리에 의하여 $Imf\cong R/\ker(f)$이다. 그러면 R이 유한환이므로

$$|Imf|=|R/\ker(f)|=\frac{|R|}{|\ker(f)|}$$

이다. 따라서 $|\ker(f)||Imf|=|R|$이다.

6.2.6. $\forall f(x), g(x)\in\mathbb{Z}[x]$

$$\phi(f(x)+g(x))=f(0)+g(0)=\phi(f(x))+\phi(g(x))$$

$$\phi(f(x)g(x))=f(0)g(0)=\phi(f(x))\phi(g(x))$$

이므로 ϕ는 환 준동형사상이다.

$$\ker(\phi)=\{f(x)\in\mathbb{Z}[x]\,|\,\phi(f(x))=0\}=\{2a+xg(x)\,|\,g(x)\in\mathbb{Z}[x]\}$$

$\forall f(x)\in\mathbb{Z}[x], f(x)$의 상수항을 n이라 하자.

n이 짝수일 때 $f(0)=0$, n이 홀수일 때 $f(0)=1$이므로 $Imf=\mathbb{Z}_2$이다. 제1동형정리에 의하여

$$\mathbb{Z}[x]/\ker(\phi)\cong\mathbb{Z}_2$$

가 되어 잉여환 $\mathbb{Z}[x]/\ker(\phi)$은 체가 된다.

== 연습문제 (6.3) ==

6.3.1. (1) $char\mathbb{Z}_4=4$ (2) $char\mathbb{Z}_4[x]=4$ (3) $char\mathbb{Q}=0$ (4) $charM_n(\mathbb{R})=0$

6.3.2. (1) $n(1,3)\neq(0,0)\,\forall n\in\mathbb{N}$이므로 $char(\mathbb{Z}_3\times 3\mathbb{Z})=0$이다.

(2) $char(\mathbb{Z}_3\times\mathbb{Z}_3)=3$

(3) $12(1,1)=(0,0)$ 이므로 $char(\mathbb{Z}_3\times 3\mathbb{Z}_4)=12$이다.

6.3.3. 환 $\mathbb{Z}_5\times\mathbb{Z}_6$의 표수를 구하고, 모든 단원과 영인자를 구하라.

(풀이) $char(\mathbb{Z}_5\times\mathbb{Z}_6)=30$ 이다.

단원은 $U(\mathbb{Z}_5\times\mathbb{Z}_6)=U(\mathbb{Z}_5)\times U(\mathbb{Z}_6)=\{(1,1),(2,1),(3,1),(4,1),(1,5),(2,5),(3,5),(4,5)\}$이다.

영인자는 $Zero(\mathbb{Z}_5\times\mathbb{Z}_6)=\mathbb{Z}_5\times\mathbb{Z}_6-U(\mathbb{Z}_5\times\mathbb{Z}_6)-\{(0,0)\}$ 이다.

6.3.4. $char(R[x])=q$라면 임의의 $f(x)\in R[x]$에 대하여 $pf(x)=0$이므로 분명히 $q\leqq p$이다.

$q<p$이라 하면 임의의 $a\in R$에 대하여 $f(x)=a\in R[x]$를 생각하자. 그러면

$$0=qf(x)=qa$$

가 되어 $q<p=char(R)\leqq q$가 되어 모순이다. 따라서 $char(R[x])=q=p$이다.

6.3.5. (1) $1_S1_S=1_S=1_S1_D$이다. 정역이므로 소거법칙에 의하여 $1_S=1_D$이다.

(2) 정리 6.3.3과 (1)에 의하여 $charS = charD$이다.

(별해) $charS = n$, $charD = m$이라 하자.

$\forall a \in S$에 대하여 $S \subset D$이므로 $a \in D$이다. 따라서

$$ma = 0 \Rightarrow n = char(S) \leqq m$$

이다. (1)에 의하여 $n1_D = n1_S = 0$이므로 임의의 $b \in D$에 대하여

$$na = n(1_D a) = (n1_D)a = 0a = 0 \Rightarrow m = char(S) \leqq n$$

이므로 $m = n$이다. 따라서 $charS = charD$이다.

6.3.6. (1) $(ax+b)^p = a^p x^p + b^p = ax^p + b$

(2) $(x^2 + x + 1)^p = x^{2p} + x^p + 1$

(3) $(x-1)^{p^2} = (x^p - 1)^p = x^{p^2} - 1$

6.3.7. (1) $\forall (r_1, a_1), (r_2, a_2), (r_3, a_3) \in S$

$(S,+)$는 덧셈 가환군임을 쉽게 증명할 수 있다.

$$((r_1, a_1) + (r_2, a_2))(r_3, a_3) = (r_1 + r_2, a_1 + a_2)(r_3, a_3) = ((r_1 + r_2)r_3 + (a_1 + a_2)r_3 + a_3(r_1 + r_2), (a_1 + a_2)a_3)$$
$$(r_1, a_1)(r_3, a_3) + (r_2, a_2)(r_3, a_3) = (r_1 r_3 + a_1 r_3 + a_3 r_1, a_1 a_3) + (r_2 r_3 + a_2 r_3 + a_3 r_2, a_2 a_3)$$
$$= (r_1 r_3 + a_1 r_3 + a_3 r_1 + r_2 r_3 + a_2 r_3 + a_3 r_2, a_1 a_3 + a_2 a_3)$$

이므로 $((r_1, a_1) + (r_2, a_2))(r_3, a_3) = (r_1, a_1)(r_3, a_3) + (r_2, a_2)(r_3, a_3)$이다. 같은 방법으로

$(r_3, a_3)((r_1, a_1) + (r_2, a_2)) = (r_3, a_3)(r_1, a_1) + (r_3, a_3)(r_2, a_2)$을 증명할 수 있다.

$$((r_1, a_1)(r_2, a_2))(r_3, a_3) = (r_1 r_2 + a_1 r_2 + a_2 r_1, a_1 a_2)(r_3, a_3) = ((r_1 r_2 + a_1 r_2 + a_2 r_1)r_3 + a_3(r_1 r_2 + a_1 r_2 + a_2 r_1) + (a_1 a_2)r_3, a_1 a_2 a_3)$$
$$(r_1, a_1)((r_2, a_2)(r_3, a_3)) = (r_1, a_1)(r_2 r_3 + a_2 r_3 + a_3 r_2, a_2 a_3) = (r_1(r_2 r_3 + a_2 r_3 + a_3 r_2) + a_1(r_2 r_3 + a_2 r_3 + a_3 r_2) + (a_2 a_3)r_1, a_1 a_2 a_3)$$

이므로 $((r_1, a_1)(r_2, a_2))(r_3, a_3) = (r_1, a_1)((r_2, a_2)(r_3, a_3))$이다.

그러므로 S는 환이다.

(2) $(0,1) \in S$, $\forall (r_1, a_1) \in S$

$(r_1, a_1)(0,1) = (r_1 0 + a_1 1 + 1r_1,\ a_1 1) = (r_1, a_1)$ 이므로
$(0,1)(r_1, a_1) = (0r_1 + 1r_1 + a_1 0,\ 1a_1) = (r_1, a_1)$

S는 곱셈항등원 (0,1)을 가진다.

(3) 단위원 (0,1)을 가지므로 정리 6.3.3을 이용하자.

$charR = 0$인 경우.

$\forall n \in \mathbb{N}, n(0,1) = (0,n) \neq (0,0)$ 이므로 $charS = 0$ 이다.

$charR = n$인 경우.

$n(0,1) = (0,n) = (0,0)$이고 $m(0,1) = (0,m) \neq (0,0)(1 \leqq \forall m < n)$

이므로 $charS = n$이다.

(4) $\forall a, b \in R$에 대하여

$$\phi(a+b) = (a+b, 0) = (a,0) + (b,0) = \phi(a) + \phi(b)$$
$$\phi(ab) = (ab, 0) = (a,0)(b,0) = \phi(a)\phi(b)$$

이므로 ϕ는 환 준동형사상이다.

$$\phi(a) = \phi(b) \Rightarrow (a,0) = (b,0) \Rightarrow a = b$$

$\therefore \phi$는 단사

그러므로 ϕ는 단사 준동형사상이다.

6.3.8 $\alpha \in F$가 $f(x)$의 근이므로 $f(\alpha) = \alpha^3 - \alpha + 1 = 0$이고, 정리 6.3.13에 의하여 $\alpha, \alpha^3, \alpha^9$은 $f(x)$의 근이다. 또한

$f(0)\neq 0,\ f(1)\neq 0,\ f(2)=f(-1)\neq 0$이므로 $\alpha\neq 0,\ 1,\ 2$이다. $\alpha^3=\alpha-1$에서

$$\alpha^3=\alpha-1,$$
$$\alpha^9=(\alpha-1)^3=\alpha^3-1=\alpha-1-1=\alpha-2=\alpha+1$$

이므로 $\alpha,\ \alpha^3,\ \alpha^9$ 은 $f(x)$의 서로 다른 세 근이다. 따라서 $f(x)$는 다음과 같이 인수분해 된다.

$$f(x)=(x-\alpha)(x-\alpha^3)(x-\alpha^9)=(x-\alpha)(x-\alpha+1)(x-\alpha-1)$$

== 연습문제 (6.4) ==

6.4.1. $U(\mathbb{Z}\times\mathbb{Q}\times\mathbb{Z})=U(\mathbb{Z})\times U(\mathbb{Q})\times U(\mathbb{Z})=\{(a,b,c)|a,c\in\{-1,1\},b\in\mathbb{Q}-\{0\}\}$

6.4.2. $\forall a(\neq 0)\in R,(a,0)\times(0,a)=(0,0)$이다. 따라서 영인자가 존재하므로 $R\times R$은 항상 정역이 아니다.

6.4.3. J 가 $R\times R'$의 아이디얼일 때

$$I=\{a\in R\mid (a,a')\in J\},\quad I'=\{b'\in R'\mid (b,b')\in J\}$$

라 하자.

이때 $a,\ b\in I,\ r\in R$에 대하여 $(a,a'),\ (b,b')\in J$인 $a',\ b'\in R'$이 존재하므로

$$(a-b,a'-b')=(a,a')-(b,b')\in J,$$
$$(ra,a')=(r,1)(a,a')\in J,$$
$$(ar,a')=(a,a')(r,1)\in J$$

이다. 따라서 $a-b,\ ra,\ ra\in I$가 되어 I는 R의 아이디얼이다.

같은 방법으로 I'은 R'의 아이디얼이다.

다음에 임의의 $(a,b')\in I\times I'$에 대하여 $(a,a'),\ (b,b')\in J$인 $a'\in R',\ b\in R$이 존재하므로

$$(a,b')=(a,0)+(0,b')=(1,0)(a,a')+(0,1)(b,b')\in J$$

이다. 그러므로 $I\times I'\subset J$이다. 역으로 $(x,y)\in J$에 대하여 분명히 $x\in I,\ y\in I'$이므로 $(x,y)\in I\times I'$이다. 따라서 $J\subset I\times I'$이다. 그러므로 $J=I\times I'$이다.

(별해) J 가 $R\times R'$의 아이디얼일 때 $(x,y)\in J$에 대하여

$$(x,0)=(1,0)(x,y)\in J,\quad (0,y)=(0,1)(x,y)\in J$$

이므로

$$I=\{a\in R\mid (a,0)\in J\},\quad I'=\{b'\in R'\mid (0,b')\in J\}$$

라 하자.

이때 $a,\ b\in I,\ r\in R$에 대하여 $(a,0),\ (b,0)\in J$이므로

$$(a-b,0)=(a,0)-(b,0)\in J,$$
$$(ra,0)=(r,0)(a,0)\in J,$$
$$(ar,0)=(a,0)(r,0)\in J$$

이다. 따라서 $a-b,\ ra,\ ra\in I$가 되어 I는 R의 아이디얼이다.

같은 방법으로 I'은 R'의 아이디얼이다.

다음에 임의의 $(a,a')\in I\times I'$에 대하여 $(a,0),\ (0,a')\in J$이므로

$$(a,a')=(a,0)+(0,a')\in J$$

이다. 그러므로 $I\times I'\subset J$이다. 역으로 $(x,y)\in J$에 대하여

$$(x,0)=(1,0)(x,y)\in J\Rightarrow x\in I,$$
$$(0,y)=(0,1)(x,y)\in J\Rightarrow y\in I'$$

이므로 $(x,y)\in I\times I'$이다. 따라서 $J\subset I\times I'$이다. 그러므로 $J=I\times I'$이다.

6.4.4. 위 연습문제 6.4.3.를 활용하자.

(1) $\mathbb{Z}_2$의 아이디얼은 $\{0\},\ \mathbb{Z}_2$뿐이므로 아이디얼은 $\{0\}\times\{0\},\{0\}\times\mathbb{Z}_2,\mathbb{Z}_2\times\{0\},\mathbb{Z}_2\times\mathbb{Z}_2$(4개)이다.

(2) $\mathbb{Z}_2$의 아이디얼은 $\{0\},\ \mathbb{Z}_2$이고 $\mathbb{Z}_6$의 아이디얼은 $\{0\},\ <1>'=\mathbb{Z}_6,\ <2>',\ <3>'$이므로 아이디얼은 다음과 같이

8개를 가진다.

$\{0\}\times\{0\},\{0\}\times\langle 2\rangle',\{0\}\times\langle 3\rangle',\{0\}\times\mathbb{Z}_6,\mathbb{Z}_2\times\{0\},\mathbb{Z}_2\times\langle 2\rangle',\mathbb{Z}_2\times\langle 3\rangle',\mathbb{Z}_2\times\mathbb{Z}_6$

(3) $\{0\}\times\{0\},\{0\}\times\mathbb{Z}_3,\mathbb{Z}_3\times\{0\},\mathbb{Z}_3\times\mathbb{Z}_3$

6.4.5.

(1) $e\in R$는 멱등원이므로 $e^2=e$이다.

$f^2=(1-e)^2=1-2e+e^2=1-2e+e=1-e=f$이므로 f는 멱등원이다.

$f=1-e$에서 $e+f=1$이다.

$ef=e(1-e)=e-e^2=e-e=0$이다. $\therefore ef=fe=0$

(2) $e+f=1$이므로 $\forall a\in R,\ a=ea+fa\in eR+fR$이다. 따라서 $eR+fR=R$이다.

$a\in eR\cap fR \Rightarrow a=ea'=fa'' \Rightarrow a=ea'=e^2a'=e(fa'')=(ef)a''=0a''=0$

이므로 $eR\cap fR=\{0\}$이다. 따라서 $R=eR\oplus fR$ 이다.

== 연습문제 (6.5) ==

6.5.1. 정리 6.5.8과 정리 6.5.12를 이용하자.

(1) 잉여환은 $\mathbb{Z}_2$와 $\mathbb{Z}_3$과 동형이어야 하므로 극대 아이디얼과 소 아이디얼은 $<2>'$, $<3>'$뿐이다.

(2) 잉여환은 $\mathbb{Z}_2$와 $\mathbb{Z}_3$과 동형이어야 하므로 극대 아이디얼과 소 아이디얼은 $<2>'$, $<3>'$뿐이다.

(3) 잉여환은 $\mathbb{Z}_2$와 동형이어야 하므로 $\mathbb{Z}_2$의 아이디얼은 $\{0\}$, $\mathbb{Z}_2$뿐이다. 따라서 극대 아이디얼과 소 아이디얼은 $\{0\}\times\mathbb{Z}_2$, $\mathbb{Z}_2\times\{0\}$이다.

(4) 잉여환은 $\mathbb{Z}_2$와 동형이어야 하므로 $\mathbb{Z}_4$의 소, 극대 아이디얼이 $<2>'$뿐이다. 따라서 극대 아이디얼과 소 아이디얼은 $\{0\}\times\mathbb{Z}_4$, $\mathbb{Z}_2\times 2\mathbb{Z}_4$이다.

(별해)

(1) $\mathbb{Z}_6$은 순환군이므로 라그랑주정리에 의해 $\mathbb{Z}_6$의 부분군의 위수는 1,2,3,6 이다.

즉, $\mathbb{Z}_6$의 부분군은 $\{0\},\mathbb{Z}_2,\mathbb{Z}_3,\mathbb{Z}_6$과 동형이다.

i $\mathbb{Z}_6/\{0\}\cong\mathbb{Z}_6$이고 $\mathbb{Z}_6$은 체가 아니므로 {0}은 극대 아이디얼이 아니다.

ii $\mathbb{Z}_6/3\mathbb{Z}_6\cong\mathbb{Z}_3$이고 $\mathbb{Z}_3$은 체이므로 $3\mathbb{Z}_6$이 극대 아이디얼 존재

iii $\mathbb{Z}_6/2\mathbb{Z}_6\cong\mathbb{Z}_2$이고 $\mathbb{Z}_2$는 체이므로 $2\mathbb{Z}_6$이 극대 아이디얼 존재

iv $\mathbb{Z}_6$은 극대 아이디얼이 아니다.

그러므로 $\{0,3\},\{0,2,4\}$은 $\mathbb{Z}_6$의 극대 아이디얼이다.

6.5.2.

(1) 정리 6.4.7에 의하여 $(\mathbb{Z}\times\mathbb{Z})/(\mathbb{Z}\times p\mathbb{Z})\cong(\mathbb{Z}/\mathbb{Z})\times(\mathbb{Z}/p\mathbb{Z})\cong\{0\}\times\mathbb{Z}_p\cong\mathbb{Z}_p$은 체이므로 정리 6.5.8에 의하여 $\mathbb{Z}\times p\mathbb{Z}$는 $\mathbb{Z}\times\mathbb{Z}$의 극대아이디얼이다.

(별해) $\mathbb{Z}\times p\mathbb{Z}$는 $\mathbb{Z}\times\mathbb{Z}$의 아이디얼이다.

$$\mathbb{Z}\times p\mathbb{Z}\subset\mathbb{Z}\times k\mathbb{Z}\subset\mathbb{Z}\times\mathbb{Z}$$

을 만족하는 $\mathbb{Z}\times k\mathbb{Z}$가 존재한다고 가정하자. 그러면 $p\in k\mathbb{Z}\Rightarrow k|p$가 되어 $k=1$ or p이다.

따라서 $\mathbb{Z}\times k\mathbb{Z}=\mathbb{Z}\times\mathbb{Z}$ or $\mathbb{Z}\times p\mathbb{Z}$가 되어 $\mathbb{Z}\times p\mathbb{Z}$는 $\mathbb{Z}\times\mathbb{Z}$의 극대아이디얼이다.

(2) 정리 6.4.7에 의하여 $(\mathbb{Z}\times\mathbb{Z})/(\mathbb{Z}\times\{0\})\cong(\mathbb{Z}/\mathbb{Z})\times(\mathbb{Z}/\{0\})\cong\{0\}\times\mathbb{Z}\cong\mathbb{Z}$은 체가 아닌 정역이므로 정리 6.5.8에 과 정리 6.5.12에 의하여 $\mathbb{Z}\times\{0\}$는 $\mathbb{Z}\times\mathbb{Z}$의 극대 아이디얼이 아닌 소 아이디얼이다.

(별해) 아이디얼 $\mathbb{Z}\times\{0\}$은 $\mathbb{Z}\times\{0\}\subset\mathbb{Z}\times 2\mathbb{Z}\subset\mathbb{Z}\times\mathbb{Z}$이다. 2가 소수이므로 (1)에 의하여 $\mathbb{Z}\times 2\mathbb{Z}$는 극대 아이디얼이

므로 $\mathbb{Z}\times\{0\}$은 $\mathbb{Z}\times\mathbb{Z}$의 극대 아이디얼이 아니다. 한편 (a,a'), $(b,b')\in\mathbb{Z}\times\mathbb{Z}$에 대하여

$$(a,a')(b,b')=(ab,a'b')\in\mathbb{Z}\times\{0\} \Rightarrow a'b'=0$$
$$\Rightarrow a'=0 \text{ or } b'=0 \Rightarrow (a,a')=(a,0)\in\mathbb{Z}\times\{0\} \text{ or } (b,b')=(b,0)\in\mathbb{Z}\times\{0\}$$

이 되어 $\mathbb{Z}\times\{0\}$은 $\mathbb{Z}\times\mathbb{Z}$의 소 아이디얼이다.

6.5.3. 정리 6.5.8, 정리 6.5.18에 의하여 기약다항식이 되는 c를 구하면 된다. 정리 5.6.4에 의하여 1차인수가 되지 않는 값을 구하자.

(1) $f(x)=x^2+c$라 하자. $f(0)=c\neq 0$, $f(1)=1+c\neq 0$, $f(2)=f(-1)=1+c\neq 0$이면 기약 다항식이 되므로 $c=1$일 때 $f(x)$는 기약다항식이 되고 $<f(x)'$은 극대 아이디얼이므로 잉여환은 체이다.

(2) 마찬가지로 구하면 $c=1,4$이다.

6.5.4. $\frac{x^4}{3}-x+1=\frac{1}{3}(x^4-3x+3)$이고 아이젠슈타인 기약판정법($p=3$)에 의하여 다항식 x^4-3x+3은 기약이므로 $\frac{x^4}{3}-x+1$도 기약다항식이 되어 주어진 잉여환은 체이다(정리 6.5.18, 정리 6.5.8).

6.5.5. (1) $F[x]/<x>'\cong F$가 체이므로 $<x>'$은 극대 아이디얼이다.

(2) $a(\neq 0)\in F$에 대하여 $x+a\in F[x]$는 F 위에서 기약 다항식이므로 정리 6.5.18에 의하여 $<x+a>'$은 극대 아이디얼이다. 한편 양변의 차수를 비교하면

$$<x>'=<x+a>' \Rightarrow x=(x+a)f(x) \Rightarrow f(x)=1 \Rightarrow a=0$$

이 되어 모순이므로 $<x>'\neq<x+a>'$이다.

(3) 정리 6.5.17에 의하여 $F[x]$는 PID이므로 비자명 소 아이디얼은 0이 아닌 생성원 $f(x)(\neq 0)\in F[x]$가 존재하여 $<f(x)>'$이다. 이때 $f(x)$가 기약임을 보이면 충분하다(정리 6.5.18).. 적당한 $g(x)$, $h(x)\in F[x]$에 대하여 $f(x)=g(x)h(x)$라 하자. 그러면 $<f(x)>'$가 소 아이디얼이므로

$$g(x)h(x)=f(x)\in<f(x)>' \Rightarrow g(x)\in<f(x)>' \text{ or } h(x)\in<f(x)>'$$

이다. 먼저 $g(x)\in<f(x)>'$인 경우에는

$$g(x)=f(x)g'(x)(\exists\, g'(x)\in F[x]) \Rightarrow f(x)=g(x)h(x)=f(x)g'(x)h(x) \Rightarrow 1=g'(x)h(x)$$

가 되어 $h(x)$가 단원이다. 다음에 $h(x)\in<f(x)>'$인 경우에도 같은 방법으로 $g(x)$가 단원이 되어 $f(x)$는 기약다항식이 되어 $<f(x)>'$는 극대 아이디얼이다.

6.5.6. $2a+xf(x)$, $2b+xg(x)\in I$와 $h(x)\in\mathbb{Z}[x]$에 대하여

$$(2a+xf(x))-(2b+xg(x))=2(a-b)+x(f(x)-g(x))\in I,$$
$$(2a+xf(x))h(x)=2a\cdot h(x)+xf(x)h(x)\in I,$$
$$h(x)(2a+xf(x))=2a\cdot h(x)+xf(x)h(x)\in I$$

이므로 I는 $\mathbb{Z}[x]$의 아이디얼이다. 그리고 임의의 $f(x)+I\in\mathbb{Z}[x]/I$에 대하여

$$f(x)+I=a_0+a_1x+\cdots a_nx^n+I=a_0+x(a_1+a_2x+\cdots+a_nx^{n-1})+I=a_0+I$$

이다. 또한

$$a_0=2t \Rightarrow a_0+I=0+I,$$
$$a_0=2t+1 \Rightarrow a_0+I=1+I$$

이므로 $\mathbb{Z}[x]/I=\{1+I, 0+I\}\cong\mathbb{Z}_2$이 체가 되어 I는 극대 아이디얼이다.

한편 $\mathbb{Z}[x]/<x>'\cong\mathbb{Z}$는 체가 아니므로 $<x>'$는 극대 아이디얼이 아니다(정리 6.5.8).

6.5.7. $\mathbb{Z}$는 PID이므로 소 아이디얼은 $p\mathbb{Z}$($p=$소수)의 형태이므로 $I=p\mathbb{Z}$, $J=q\mathbb{Z}$ ($p,q=$소수)라 하자.

$p\mathbb{Z}\cap q\mathbb{Z}=\mathrm{lcm}(p,q)\mathbb{Z}=pq\mathbb{Z}$이다.

이때, $pq\in pg\mathbb{Z}$이지만, $p\notin pq\mathbb{Z}$이고 $q\notin pq\mathbb{Z}$이므로 $I\cap J$는 $\mathbb{Z}$의 소 아이디얼이 아니다.

6.5.8. ($\Rightarrow$) P가 소 아이디얼이라 하자. $P\neq R$이므로 $1\in S=R-P$이다. 그리고 $0\notin S$이다. $a, b\in S$에 대하여 $a, b\notin P$이고 P가 소 아이디얼이므로 $ab\notin P$이다. 따라서 $ab\in S$가 되어 S는 곱셈집합이다.

(별해) $a, b \in S$에 대하여 $a, b \notin P$이고 P가 소 아이디얼이므로 $ab \notin P$이다. 0이 아닌 원소 $a+P, b+P \in R/P$에 대하여 R/P가 정역이므로

$$a \in S,\ b \in S \Rightarrow a \notin P,\ b \notin P \Rightarrow a+P \neq 0+P,\ b+P \neq 0+P$$
$$\Rightarrow (ab+P) = (a+P)(b+P) \neq 0+P \Rightarrow ab \in S$$

($\Leftarrow$) $S = R - P$가 R의 곱셈집합이라 하자. $a, b \in R$ 에 대하여 $ab \in P$에 대하여

$$ab \notin S \Rightarrow a \notin S \text{ or } b \notin S \Rightarrow a \in P \text{ or } b \in P$$

그러므로 P는 소 아이디얼이다.

(별해) $a+P, b+P \in R/P$에 대하여

$$0+P = (a+P)(b+P) = ab+P \Rightarrow ab \in P \Rightarrow ab \notin S$$
$$\Rightarrow a \notin S \text{ or } b \notin S \Rightarrow a \in P \text{ or } b \in P \Rightarrow a+P = 0+P \text{ or } b+P = 0+P$$

이므로 R/P는 영인자를 갖지 않으므로 정역이다. 따라서 P는 소 아이디얼이다.

6.5.9. 연습문제 5.7.2에 의하여 $\mathbb{Q}_p$는 $\mathbb{Q}$의 부분환이다.

(1) 임의의 $\frac{pa}{s}, \frac{pa'}{s'} \in M,\ \frac{b}{t} \in \mathbb{Q}_P$에 대하여

$$\frac{pa}{s} - \frac{pa'}{s'} = \frac{p(as'-sa')}{ss'} \in M,$$
$$\frac{pa}{s} \cdot \frac{b}{t} = \frac{pab}{st} \in M,\ \frac{b}{t} \cdot \frac{pa}{s} = \frac{pab}{st} \in M$$

이므로 M는 $\mathbb{Q}_p$의 아이디얼이다.

다음에 $M \subsetneqq H < \mathbb{Q}_p$인 아이디얼 H가 존재한다고 하자. 그러면 $\frac{a}{1} \in H - M, a \notin p\mathbb{Z}$가 존재한다. 그러면 $a \in S$이고 $\frac{1}{a} \in \mathbb{Q}_p$이다. 따라서 $1 = \frac{a}{1} \cdot \frac{1}{a} \in H$가 되어 $H = \mathbb{Q}_p$가 된다(정리 6.1.6). 따라서 M은 $\mathbb{Q}_p$의 극대 아이디얼이다.

(2) I가 $\mathbb{Q}_p$의 극대 아이디얼이라 하자. $I \neq M$이라 하면 $\frac{a}{s} \in I - M$이 존재한다. 그러면 $a \notin p\mathbb{Z}$이므로 $a \in S$이고 $\frac{s}{a} \in \mathbb{Q}_p$이다. 그러므로 $1 = \frac{a}{s} \cdot \frac{s}{a} \in I$이 되어 $I = \mathbb{Q}_p$가 되어 극대 아이디얼에 모순이다. 따라서 $\mathbb{Q}_p$의 극대 아이디얼은 M뿐이다.

6.5.10.

sol) 모든 0이 아닌 R의 소 아이디얼 P에 대하여 $P < M < R$인 아이디얼 M이 존재한다고 하자.

R이 PID이므로 $P = \langle a \rangle', M = \langle b \rangle'$인 $a, b \in R$이 존재한다. 그러면

$$a \in \langle a \rangle' < \langle b \rangle' \Rightarrow a = bb' (\exists\, b' \in R) \Rightarrow bb' \in \langle a \rangle' = P$$

이다. P가 소 아이디얼이므로 $b \in P$ or $b' \in P$이다.

먼저 $b \in P$이면 $b = aa'$이고 $a = bb' = aa'b' \Rightarrow 1 = a'b'$이 되어 b'이 단원이다. 따라서

$$b = ab'^{-1} \in P \Rightarrow M = P$$

이다. 다음에 $b' \in P$이면 같은 방법으로 b가 단원이다. 따라서

$$b \in M \Rightarrow M = R$$

이다(정리 6.1.6). 그러므로 P는 R의 극대 아이디얼이다.

6.5.11.

($\Rightarrow$) N이 환 R의 극대 아이디얼이면 R/N은 체가 되어 단순환이다(따름정리 6.5.10).

($\Leftarrow$) 잉여환 R/N이 단순환이라 하자. R의 아이디얼 N, M에 대하여 $N < M < R$이라하자. 그러면 자연 준동형사상 $f : R \to R/N$에 대하여 정리 6.2.1에 의하여 $f(M) = M/N$은 R/N의 아이디얼이고

$$N/N < M/N < R/N$$

이다. 다. R/N이 단순환이므로

$M/N = N/N$ or $M/N = R/N$이다. 따라서 $M = N$이거나 $M = R$이 되어 M은 R의 극대 아이디얼이다.

6.5.12 ϕ가 전사이고 환 준동형사상이므로 제1동형정리에 의해 $R/\ker(\phi) \cong Im(\phi) = F$가 체이다.
따라서 $\ker\phi$는 R의 극대 아이디얼이다.

6.5.13. **P가 소 아이디얼이므로 R/P는 정역이다(정리 6.5.12).**
R/P이 유한정역이므로 R/P는 체이다(정리 5.2.9). 따라서 P는 R의 극대 아이디얼이다(정리 6.5.8).

== 연습문제 (7.1) ==

7.1.1 a가 소원이라 하면 $a = bc$이므로 $a \neq 0, b \neq 0, c \neq 0$이고 a는 단원이 아니다.
$a|bc\ (\because a = bc)$
$\Rightarrow a|b$ or $a|c$
$\Rightarrow bc|b$ or $bc|c$
$\Rightarrow c|1$ or $b|1$
$\Rightarrow b$가 단원 or c가 단원 (b, c가 둘 다 기약원임에 모순)
따라서 a는 소원이 아니다. 그러므로 (정리 7.1.9)에 의하여 $\langle a\rangle'$는 소 아이디얼이 아니다.
그러므로 극대 아이디얼이 아니다(정리 6.5.13).

7.1.2 (i) p가 D의 소원이면 p는 D의 기약원이다.($\because$ 정리7.1.7)
(ii) p가 D의 기약원이면 0과 가역원이 아닌 원소이다.
또한 $p|ab$라고 가정하자. 그러면 $ab = pc(\exists\, c \in D)$이다. D가 UFD이고 p가 기약원이므로 인수분해의 유일성에 의하여 p는 a의 인수이거나 b의 인수이다. 따라서 p는 소원이다.
따라서 (i), (ii) 에 의하여 D에서 기약원과 소원은 동일한 개념이다.

7.1.3 (1) $x^3 - 2$는 아이젠슈타인 정리($p = 2$)에 의해 $\mathbb{Q}$ 위에서 기약이므로 $\mathbb{Z}[x]$에서도 기약이다.
$\mathbb{Z}[x]$는 UFD이므로 $x^3 - 2$는 소원이다.

(2) $\mathbb{Z}[x]/\langle x\rangle' = \{a + \langle x\rangle' | a \in \mathbb{Z}\} \cong \mathbb{Z}$이고 $\mathbb{Z}$는 정역이다.
따라서 $\mathbb{Z}[x]/\langle x\rangle'$는 정역이므로 $\langle x\rangle'$는 소 아이디얼이다.

(3) (연습문제 6.5.6 참조) $\mathbb{Z}[x]/\langle x, 2\rangle' = \{0 + \langle x, 2\rangle', 1 + \langle x, 2\rangle'\} \cong \mathbb{Z}_2$이고 $\mathbb{Z}_2$는 체이다.
따라서 $\mathbb{Z}[x]/\langle x, 2\rangle'$는 체이므로 $\langle x, 2\rangle'$는 극대 아이디얼이다.

== 연습문제 (7.2) ==

7.2.1. $F[x, y]$는 PID라 하자. 그러면 아이디얼 $< x, y >' = < f(x, y) >'$ 인 $f(x, y) \in F[x, y]$가 존재한다.
$x \in < x, y >' = < f(x, y) >' \Rightarrow \exists\, g(x, y)\ s.t.\ x = f(x, y)g(x, y)$
x가 기약원이므로 $f(x, y)$가 단원이거나 $g(x, y)$가 단원이다.
먼저 $f(x, y)$가 단원인 경우에는 정리 6.1.6에 의하여

$$< x, y >' = < f(x,y) >' = F[x] \ni 1 \Rightarrow EXIST g', h' \in F[x, y],\ x g'(x, y) + y h'(x, y) = 1$$

이다. 이것은 좌변은 상수항이 없으므로 모순이다.

다음에 $g(x, y)$가 단원 u이면 $f(x,y) = u^{-1}x$이다. 그러면

$$y \in < x, y >' = < u^{-1}x >' = < x >' \Rightarrow \exists\, g'' \in F[x, y],\ y = x g''(x, y)$$

이다. 이것은 우변에 계수가 1인 y항이 없으므로 모순이다. 따라서 $F[x, y]$는 PID가 아니다.

7.2.2. ($\Rightarrow$) a, b가 서로소라 하자. a, b의 최대공약수는 단원 u이다. D가 PID이므로 정리 7.2.2에 의하여 적당한 $x, y \in D$가 존재하여

$$u = ax + by \Rightarrow 1 = a(xu^{-1}) + b(yu^{-1})$$

이다.

($\Leftarrow$) $ax + by = 1$인 $x, y \in D$가 존재한다고 하자. 그리고 d가 a, b의 최대공약수라 하자. 그러면

$$d|(ax + by) \Rightarrow d|1$$

이므로 적당한 $d' \in D$가 존재하여 $1 = dd'$이므로 d는 단원이 되어 a, b는 서로소이다.

7.2.3. 정리 7.2.3을 이용하자.

(1) ($\Rightarrow$) $aa' + cc' = 1, bx + cy = 1$인 $a', c', x, y \in D$가 존재한다.

$$(aa' + cc')(bx + cy) = (ab)a'b' + c(aa'y + bc'x + cc'y) = 1 \Rightarrow 1 \in GCD(ab, c)$$

($\Leftarrow$) $abx + cy = 1$인 $x, y \in D$가 존재한다.

$$(a)bx + cy = (b)ax + cy = 1 \Rightarrow 1 \in GCD(a,c),\ 1 \in GCD(b,c)$$

(2) a, b가 서로소이므로 $ax + by = 1$인 $x, y \in D$가 존재한다. 한편 $a|bc \Rightarrow bc = ad\,(\exists\, d)$이므로

$$axc + byc = c \Rightarrow acx + ady = c \Rightarrow a(cx + dy) = c \quad \therefore a|c$$

(3) a, b가 서로소이므로 $ax + by = 1$인 $x, y \in D$가 존재한다. 가정에서 $\exists\, a', b' \in D,\ c = aa',\ c = bb'$이므로

$$acx + bcy = c \Rightarrow abb'x + baa'y = c \quad \therefore ab|c$$

7.2.4.

(1) 정리 7.2.2에 의하여 $d \neq 0$이므로

$$d = ax + by = da'x + db'y \Rightarrow 1 = a'x + b'y$$

인 $x, y \in D$가 존재한다. 정리 7.2.3에 의하여 a', b'은 서로소이므로 $1 \in GCD(a', b')$이다.

(2) $m = da'b' = ab' = ba'$이므로 $a|m,\ b|m$이다. 한편 $a|l,\ b|l$이라 하자. 그러면 적당한 $a'',\ b'' \in D$에 대하여

$$l = aa'' = bb'' \Rightarrow lb' = ab'a'' = (da'b')a'' = ma'' \Rightarrow l = \frac{ma''}{b'}$$

이다. 한편 (1)에 의하여 $1 \in GCD(a', b')$이므로 정리 7.2.4(2)를 이용하면

$$aa'' = bb'' \Rightarrow da'a'' = db'b'' \Rightarrow a'a'' = b'b'' \Rightarrow b'|a'a'' \Rightarrow b'|a''$$

이다. 그러므로

$$l = \frac{ma''}{b'} = m\frac{a''}{b'} \Rightarrow m|l$$

이 되어 $m \in LCM(a,b)$이다. 분명히 $ab = da'db' = dm$이다.

(별해) 정리 7.2.2에 의하여 최소공배수 $m' \in LCM(a,b)$가 존재한다. 그리고 $d' = ab/m'$이라 하자. 그러면

$$a = \frac{ab}{m'} \cdot \frac{m'}{b} = d' \cdot \frac{m'}{b}, \qquad b = \frac{ab}{m'} \cdot \frac{m'}{a} = d' \cdot \frac{m'}{a}$$

이므로 $d'|a,\ d'|b$이다. 다음에 $e|a,\ e|b$라 하면

$$a \left| \frac{ab}{e}, \quad b \right| \frac{ab}{e}$$

이므로 $m' \left| \frac{ab}{e} \right.$이다. 그러므로 $e \left| \frac{ab}{m'} \right. = d'$이고 따라서 $d' \in GCD(a,b)$이다.

그러면 분명히 $ab = dm$이다. 또한 정리 7.1.14에 의하여 $d' = ab/m'$와 $d = ab/m$은 동반원이다. 따라서 m과 m'은 동반원이다. 그러면 정리 7.1.14(1)과 같은 방법으로 $m \in LCM(a,b)$을 증명할 수 있다.

7.2.5. 예 6.1.26에 의하여 $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$이고 p가 소수이므로 $\mathbb{Z}_p$는 체이다. 따라서 정리 6.5.8에 의하여 $p\mathbb{Z}$는 $\mathbb{Z}$의 극대 아이디얼이다.

7.2.6. (풀이1) $\mathbb{Z}_{p^aq^b}$가 주아이디얼 환이므로 아이디얼의 생성원은 p^aq^b의 약수에서 나온다. 즉, 모든 아이디얼은 $\langle p^{a'}q^{b'}\rangle'(0 \leqq a' \leqq a,\ 0 \leqq b' \leqq b)$인 형태이다. 따라서

$$\mathbb{Z}_{p^aq^b}/\langle p^{a'}q^{b'}\rangle \cong \mathbb{Z}_{p^{a'}q^{b'}}$$

이 체가 되려면 $a' = 1,\ b' = 0$이거나 $a' = 0,\ b' = 1$이어야 하므로 극대아이디얼은 $\langle p\rangle, \langle q\rangle$이다.

(풀이2) $\mathbb{Z}_{p^aq^b}$가 주아이디얼 환이므로 아이디얼의 생성원은 p^aq^b의 약수에서 나온다. 즉, 모든 아이디얼은 $\langle p^{a'}q^{b'}\rangle'(0 \leqq a' \leqq a,\ 0 \leqq b' \leqq b)$인 형태인데, $a' \neq 0,\ b' \neq 0$인 아이디얼 중에서 극대 아이디얼이 나온다. 이 때,

$a' \neq 0$이면, $\langle p^{a'}q^{b'}\rangle' < \langle p\rangle' \neq \langle 1\rangle' = \mathbb{Z}_{p^aq^b}$이고, $b' \neq 0$이면, $\langle p^{a'}q^{b'}\rangle' < \langle q\rangle' \neq \langle 1\rangle' = \mathbb{Z}_{p^aq^b}$이다.

한편, p, q가 서로 다른 소수이므로 $\langle p\rangle, \langle q\rangle$는 서로 포함관계가 없다. 따라서 극대 아이디얼은 $\langle p\rangle, \langle q\rangle$이다.

== 연습문제 (7.3) ==

7.3.1 (풀이1) $f(x) = x^4 - 4x^2 + 3 = (x^2-1)(x^2-3)$

$g(x) = x^3 + 3x^2 - x - 3 = (x^2-1)(x+3)$이므로 $GCD(f(x), g(x)) = \{u(x^2-1) \mid u \in \mathbb{Q} - \{0\}\}$이다.

(풀이2) 유클리드 호제법을 이용하자.

x	$x^4 - 4x^2 + 3$ $x^4 + 3x^3 - x^2 - 3x$	$x^3 + 3x^2 - x - 3$ $x^3 + x^2 - x - 1$	$-\frac{1}{3}$
$-\frac{3}{2}x$	$-3x^3 - 3x^2 + 3x + 3$ $-3x^3 + 3x$	$2x^2 - 2$ $2x^2 - 2$	$-\frac{2}{3}$
	$-3x^2 + 3$	0	

$GCD(f(x), g(x)) = \{u(x^2-1) \mid u \in \mathbb{Q} - \{0\}\}$이다.

7.3.2 (풀이) (1) $f(x) = x^3 + 4x^2 + 3x - 8,\ g(x) = x^2 + x - 2$라 하자.

x	$x^3 + 4x^2 + 3x - 8$ $x^3 + x^2 - 2x$	$x^2 + x - 2$ $x^2 + \frac{5}{3}x - \frac{8}{3}$	$\frac{1}{3}$
$-\frac{9}{2}x$	$3x^2 + 5x - 8$ $3x^2 - 3x$	$-\frac{2}{3}x + \frac{2}{3}$ $-\frac{2}{3x} + \frac{2}{3}$	$-\frac{2}{24}$
	$8x - 8$	0	

$f(x) = x^3 + 4x^2 + 3x - 8$과 $g(x) = x^2 + x - 2$의 최대공약수는 $d(x) = 8x - 8$이다.

최소공배수는 $l(x) = (x^3 + 4x^2 + 3x - 8)\left(\frac{x}{8} + \frac{1}{4}\right) = \left(\frac{1}{8}x^2 + \frac{5}{8}x + 1\right)(x^2 + x - 2)$이다.

유크리드 호제법의 역순으로 계산하면

$$
\begin{aligned}
&8x-8\\
&=(3x^2+5x-8)-(3x^2-3x)\\
&=(3x^2+5x-8)-\left(-\frac{9}{2}x\right)\left(-\frac{2}{3}x+\frac{2}{3}\right)\\
&=(3x^2+5x-8)-\left(-\frac{9}{2}x\right)\left((x^2+x-2)-\frac{1}{3}(3x^2+5x-8)\right)\\
&=(3x^2+5x-8)\left(1-\frac{3}{2}x\right)-\left(-\frac{9}{2}x\right)(x^2+x-2)\\
&=(f(x)-xg(x))\left(1-\frac{3}{2}x\right)-\left(-\frac{9}{2}x\right)g(x)\\
&=f(x)\left(1-\frac{3}{2}x\right)+g(x)\left(\frac{7}{2}x+\frac{3}{2}x^2\right)
\end{aligned}
$$

이다.

(별해)

몫			x	$\frac{1}{3}$	$-\frac{9}{2}x$
$f(x)$	1	0	1	$-\frac{1}{3}$	$1-\frac{3}{2}x$
$g(x)$	0	1	$-x$	$1+\frac{1}{3}x$	$\frac{7}{2}x+\frac{3}{2}x^2$
나머지	$f(x)$	$g(x)$	$3x^2+5x-8$	$-\frac{2}{3}x+\frac{2}{3}$	$8x-8$

(위 표에서 $3x^2+5x-8=f(x)\cdot 1+g(x)(-x)$가 성립한다.)

에서 $8x-8=f(x)\left(1-\frac{3}{2}x\right)+g(x)\left(\frac{7}{2}x+\frac{3}{2}x^2\right)$이다. $\therefore\ s(x)=1-\frac{3}{2}x\ ,\ t(x)=\frac{7}{2}x+\frac{3}{2}x^2$

(2) $f(x)=x^4-x^3-x^2+1,\quad g(x)=x^3-1$라 하자.

$x-1$	$x^4-x^3-x^2+1$ x^4-x^3-x+1	x^3-1 x^3-x^2	$-x$
-1	$-x^2+x$ $-x^2+1$	x^2-1 x^2-1	$x+1$
	$x-1$	0	

따라서 $d(x)=x-1$이고 $l(x)=(x^2+x+1)(x^4-x^3-x^2+1)$이다.

몫			$x-1$	$-x$	-1
$f(x)$	1	0	1	x	$1+x$
$g(x)$	0	1	$-x+1$	$-x^2+x+1$	$-x^2+2$
나머지	$f(x)$	$g(x)$	$-x^2+x$	x^2-1	$x-1$

$x-1=f(x)(x+1)+g(x)(-x^2+2)$이므로 $s(x)=x+1,\ t(x)=-x^2+2$이다.

7.3.3 (풀이) (1) ($\Rightarrow$) $d\in GCD(p(x),f(x))$라 하자.

그러면 $p(x)=d\cdot p'(x),\ f(x)=d\cdot p'(x)$인 $p'(x),f'(x)\in F[x]$가 존재한다.

그런데 $p(x)$는 기약이므로 d 또는 $p'(x)$가 단원이다.

$p'(x)$가 단원이면 $p(x)|d$이고 $d|f(x)$이므로 $p(x)|f(x)$이다. 이것은 모순이다.

그러므로 d가 단원이고, $1\in GCD(p(x),f(x))$이다.

($\Leftarrow$) $p(x)|f(x)$라 하자. 그러면 $p(x)\in GCD(p(x),f(x))$이다.

그런데 $1\in GCD(p(x),f(x))$이므로 $p(x)$는 단원(정리 7.1.14)이 되어 모순이다. 따라서 $p(x)|f(x)$이다.

(2) ($\Rightarrow$) $p(x)$가 기약이므로 $d(x)\in GCD(p(x),f(x))$는 단원이거나 $p(x)$와 동반원이다.
하지만 (1)에 의하여 단원이 될 수 없으므로 정리 7.1.14에 의하여 $p(x)\in GCD(p(x),f(x))$이다.
($\Leftarrow$) $p(x)\in GCD(p(x),f(x))$이면 $f(x)=p(x)g(x)$인 $g(x)\in F[x]$가 존재한다. 그러므로 $p(x)|f(x)$ 이다.

7.3.4. $U(\mathbb{Z}[i])=\{\pm 1,\ \pm i\}$이므로 최대공약수는 4개가 존재한다.

(1) $\dfrac{53+9i}{1+7i}=\dfrac{116}{50}-\dfrac{362i}{50}\fallingdotseq 2-7i$(몫)이고 나머지는 $2+2i$, $\dfrac{1+7i}{2+2i}=2+\dfrac{3i}{2}\fallingdotseq 2+i$

$2-7i$	$53+9i$ $51+7i$	$1+7i$ $2+6i$	$2+i$
$-2i$	$2+2i$ $2+2i$	$-1+i$	
	0		

$GCD(53+9i,1+7i)=\{\pm(-1+i),\ \pm i(-1+i)\}=\{1\pm i,-1\pm i\}$

(2) $GCD(3+4i,\ 11-2i)=\{\pm(3+4i),\ \pm i(3+4i)\}$

(3) $GCD(6-7i,-1-8i)=\{\pm(-1+2i),\ \pm i(-1+2i)\}$

(4) $GCD(4+6i,3-5i)\equiv\{\pm(1+i),\ \pm i(1+i)\}$

7.3.5 (1) i) 정수의 나눗셈 알고리즘에 의하여 $a,b(\neq 0)\in\mathbb{Z}$, $\exists\, q,r\in\mathbb{Z}$, $a=bq+r,\ 0\leqq r<|b|$이므로

$r=0,\quad a^2<b^2\Rightarrow \delta(a)<\delta(b)$이다.

ii) $\forall\, a,b\neq 0\in\mathbb{Z},\quad \delta(a)=a^2\leqq a^2b^2=\delta(ab)\quad\Rightarrow\ \delta(a)\leqq\delta(ab)$

그러므로 δ는 유클리드 노름이다.

(2) 유클리드 노름이 아니다.

(반례) $a=1/2,\ b=1/3$일 때 $\delta(a)=(1/2)^2=1/4>1/36=\delta(1/6)=\delta(ab)$가 되어 조건 2가 성립하지 않는다.

7.3.6 (1) $a,b\in D$가 동반원이므로 단원 u가 존재하여 $a=bu$이다.

$\delta(a)=\delta(bu)\geqq\delta(b)$

이다. 한편 $b=au^{-1}$이므로

$\delta(b)=\delta(au^{-1})\geqq\delta(a)$

이다. 따라서 $\delta(a)=\delta(b)$이다.

(2) ($\Rightarrow$) 임의의 $ar\in\langle a\rangle'$에 대하여 적당한 $q,\ r'\in D$가 존재하여

$ar=abq+r',\ r'=0$ 또는 $\delta(r')<\delta(ab)=\delta(a)$

이므로 $r'=ar-abq=a(r-bq)$이다. 만약 $r'\neq 0$이라 하면

$\delta(r')=\delta(a(r-bq))\geqq\delta(a)=\delta(ab)>\delta(r')$

이 되어 모순이다. 따라서 $r=0$이다. 그러므로

$ar=abq\in\langle ab\rangle'\Rightarrow\langle a\rangle'\subset\langle ab\rangle'$

분명히 $\langle ab\rangle'\subset\langle a\rangle'$이므로 $\langle a\rangle'=\langle ab\rangle'$이다.

($\Leftarrow$) $\langle a\rangle'=\langle ab\rangle'$이라 하자. 분명히 $\delta(a)\leqq\delta(ab)$이다.

$a\in\langle a\rangle'=\langle ab\rangle'$이므로 $a=abr(\exists\, r\in D^*)$이다. 따라서

$\delta(a)=\delta(abr)\geqq\delta(ab)$

이므로 $\delta(a)=\delta(ab)$이다.

(3) ($\Rightarrow$) b가 단원이면 $\langle a\rangle'=\langle ab\rangle'$이므로 (2)에 의하여 $\delta(a)=\delta(ab)$이다.

(별해) $\delta(a)\leqq\delta(ab)\leqq\delta(abb^{-1})=\delta(a\cdot 1)=\delta(a)\Rightarrow\delta(a)=\delta(ab)$

($\Leftarrow$) $\delta(a)=\delta(ab)$라 하자. (2)에 의하여 $\langle a\rangle'=\langle ab\rangle'$이다. 그러면 $a\neq 0$이므로

$a = abr (EXISTr \in D^*) \Rightarrow 1 = br$

이므로 b가 단원이다.

(4) D가 정역이므로 0이 아닌 원소 $a \in D$가 가역임을 보이면 된다. δ가 상수함수이므로 모든 원소 $b(\neq 0) \in D$에 대하여

$$\delta(b) = \delta(ba)$$

이다. (3)에 의하여 a는 단원이다. 따라서 D는 체이다.

(별해) δ가 상수함수이므로 모든 원소 $a(\neq 0) \in D$에 대하여

$$\delta(1) = \delta(a)$$

이다. 그러면 정리 7.3.13에 의하여 a는 단원이다. 따라서 D는 체이다.

7.3.7 임의의 $a, b \in I$와 $r \in D$에 대하여

1) $abr \neq 0$인 경우를 살펴보자.

$\delta(-b) = \delta((-1)b) \geqq \delta(b) > \delta(1)$이다. 그러므로 $-b \in I$이다. 그리고 $a - b \neq 0$이면

$$\delta(a-b) = \delta(a) + \delta(-b) \geqq \delta(a) > \delta(1) \Rightarrow a - b \in I$$
$$\delta(ra) \geqq \delta(a) > \delta(1) \Rightarrow ra \in I$$

$a - b = 0$이면 $a - b = 0 \in I$이다.

2) $abr = 0$인 경우는 $a = 0$이면 위 1)에서 $a - b = -b \in I$이다.

$b = 0$이면 분명히 $a - b = a \in I$이다.

또한 $r = 0$이면 임의의 $a \in I$에 대하여 분명히 $ra = 0 \in I$이다. 그러므로 I는 D의 아이디얼이다.

다음에 D의 아이디얼 $M < D$에 대하여 $I < M < D$라 하자. $I \neq M$이면 $\exists m \in M - I$이므로 정리 7.3.13에 의하여 $\delta(m) = \delta(1)$이 되어 m은 단원이 되어야 한다. 따라서 $M = D$이다(정리 6.1.6).

7.3.8 f가 환 준동형사상이라 하자. 임의의 $a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$에 대하여

$$f(a + b\sqrt{m}) = f(a) + f(b\sqrt{m}) = af(1) + bf(\sqrt{m})$$

이므로 f는 1과 $\sqrt{m}$에 의하여 결정된다. 1은 멱등원이므로 $f(1) = f(1)^2$에서 $f(1) = 0$이거나 1이다.

$f(\sqrt{m}) = c + d\sqrt{m} \in \mathbb{Q}(\sqrt{m})$이라 하자.

i) $f(1) = 0$인 경우.

$$f(a + b\sqrt{m}) = bf(\sqrt{m}) = b(c + d\sqrt{m}) = bc + bd\sqrt{m}$$

이다. 임의의 $a + b\sqrt{m}$, $a' + b'\sqrt{m} \in \mathbb{Q}(\sqrt{m})$에 대하여

$$f((a + b\sqrt{m})(a' + b'\sqrt{m})) = f(aa' + bb'm + (a'b + ab')\sqrt{m}) = (a'bc + ab'c) + (a'bd + ab'd)\sqrt{m}$$
$$f(a + b\sqrt{m})f(a' + b'\sqrt{m}) = (bc + bd\sqrt{m})(b'c + b'd\sqrt{m}) = (bcb'c + bdb'dm) + 2bcb'd\sqrt{m}$$

에서

$$\begin{cases} a'bc + ab'c = bcb'c + bdb'dm \\ a'bd + ab'd = 2bcb'd \end{cases} \Rightarrow \begin{cases} (a'b + ab')c = bb'c^2 + bb'd^2m \\ a'bd + ab'd = 2bcb'd \end{cases}$$

이다. $d \neq 0$이면 $a'b + ab' = 2bcb'$이므로

$$2bb'cc = bb'c^2 + bb'd^2m \Rightarrow c^2 = d^2m$$

이 되어 소인수분해의 유일성에 모순이다. 따라서 $d = 0$이고 $c = 0$이다. 그러므로 $f(\sqrt{m}) = c + d\sqrt{m} = 0$이 되어

$$f(a + b\sqrt{m}) = af(1) + bf(\sqrt{m}) = 0$$

이다.

ii) $f(1) = 1$인 경우.

$$f(a + b\sqrt{m}) = a + b(c + d\sqrt{m}) = (a + bc) + bd\sqrt{m}$$

이다. 임의의 $a + b\sqrt{m}$, $a' + b'\sqrt{m} \in \mathbb{Q}(\sqrt{m})$에 대하여

$$f((a + b\sqrt{m})(a' + b'\sqrt{m})) = f(aa' + bb'm + (a'b + ab')\sqrt{m})$$
$$= (aa' + bb'm + (ab' + a'b)c) + (ab'd + a'bd)\sqrt{m},$$

$$f(a+b\sqrt{m})f(a'+b'\sqrt{m}) = ((a+bc)+bd\sqrt{m})((a'+b'c)+b'd\sqrt{m})$$
$$= (aa'+ab'c+a'bc+bb'c^2+bb'd^2m)+(a'bd+bb'cd+ab'd+bb'cd)\sqrt{m}$$

에서

$$\begin{cases} aa'+bb'm+(ab'+a'b)c = aa'+ab'c+a'bc+bb'c^2+bb'd^2m, \\ ab'd+a'bd = a'bd+bb'cd+ab'd+bb'cd \end{cases} \Rightarrow \begin{cases} c^2+d^2m = m, \\ 2cd = 0 \end{cases}$$

이다. $c \neq 0$이면 $d=0$이므로 $c^2=m$이 되어 소인수분해의 유일성에 모순이다. 따라서 $c=0$이어야 한다. 그러면 $d^2=1$이다. 그러므로 $f(\sqrt{m}) = c+d\sqrt{m} = \pm\sqrt{m}$이 되어

$$f(a+b\sqrt{m}) = a \pm b\sqrt{m}$$

이다.

그러므로 환 준동형사상을 3가지 존재한다.

7.3.9 동형사상 $f:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(\sqrt{3})$가 존재한다고 하자. 그러면 적당한 $a+b\sqrt{3}\in\mathbb{Q}(\sqrt{3})$에 대하여

$$f(\sqrt{2}) = a+b\sqrt{3}$$

이다. 그러면 $f(1)=1$이므로

$$2 = f(2) = f((\sqrt{2})^2) = f(\sqrt{2})^2 = (a+b\sqrt{3})^2 = a^2+3b^2+2ab\sqrt{3}$$

이므로 $a^2+3b^2=2,\ 2ab=0$에서 $a=0$ 또는 $b=0$이다. 어느 경우든 소인수분해의 유일성에 모순이다. 따라서 동형사상이 존재하지 않는다.

(별해) 동형사상 $f:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(\sqrt{3})$가 존재한다고 하자. 그러면 전사이므로 적당한 $a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$에 대하여

$$f(a+b\sqrt{2}) = \sqrt{3}$$

이다. 그러면

$$f(3) = 3 = (\sqrt{3})^2 = f(a+b\sqrt{3})^2 = f(a^2+2b^2+2ab\sqrt{2})$$

이고 f가 단사이므로 $a^2+2b^2=3,\ 2ab=0$에서 $a=0$ 또는 $b=0$이다. 어느 경우든 소인수분해의 유일성에 모순이다. 따라서 동형사상이 존재하지 않는다.

== 연습문제 (7.4) ==

7.4.1 (1) $N(\sqrt{2})=2$ 소수이므로 $\mathbb{Z}[\sqrt{2}]$에서 기약원(따름정리 7.4.4)이지만 $2=\sqrt{2}\sqrt{2}$이므로 2는 기약원이 아니다.

(2) 정리 7.4.7에 의하여 $\mathbb{Z}[\sqrt{2}]$는 ED이다.

(풀이1) $\mathbb{Z}[\sqrt{2}]$의 유클리드 노름 $\delta(a+b\sqrt{2}) = |a^2-2b^2|$이다(정리 7.3.7). 그러면

$\delta(\sqrt{2})=2$이므로 $\mathbb{Z}[\sqrt{2}]/\langle\sqrt{2}\rangle'$의 원소 $a+b\sqrt{2}+\langle\sqrt{2}\rangle' = a+\langle\sqrt{2}\rangle'$는 유클리드 정역의 성질①에 의하여

$$\delta(a+b\sqrt{2}) = |a^2-2b^2| = |a| < \delta(\sqrt{2}) = 2 \Rightarrow a = 0,\ 1,\ -1$$

로 택할 수 있다. 그러면

$$1-(-1) = (\sqrt{2})^2 \in \langle\sqrt{2}\rangle'$$

이므로

$$\mathbb{Z}[\sqrt{2}]/\langle\sqrt{2}\rangle' = \{a+b\sqrt{2}+\langle\sqrt{2}\rangle' \mid a,b\in\mathbb{Z}\} = \{0+\langle\sqrt{2}\rangle',\ 1+\langle\sqrt{2}\rangle'\} \cong \mathbb{Z}_2$$

이다. 이것은 유한 정역이므로 체이다.

(별해) 함수

$$\phi:\mathbb{Z}[\sqrt{2}]/\langle\sqrt{2}\rangle' \to \mathbb{Z}_2,\ \phi(a+b\sqrt{2}) = [a]_2 \text{ (단, } [a]_2\text{는 2로 나눈 나머지)}$$

라 정의하면

$$\phi((a+b\sqrt{2})+(c+d\sqrt{2})) = \phi((a+c)+(b+d\sqrt{2})) = [a+c]_2 = [a]_2+[c]_2 = \phi(a+b\sqrt{2})+\phi(c+d\sqrt{2})$$
$$\phi((a+b\sqrt{2})(c+d\sqrt{2})) = \phi((ac+2bd)+(ad+bc)\sqrt{2}) = [ac+2bd]_2 = [ac]_2 = [a]_2[c]_2 = \phi(a+b\sqrt{2})\phi(c+d\sqrt{2})$$

이므로 환 준동형사상이다. 분명히 전사함수이고

$$\ker\phi = \{2a+b\sqrt{2} \mid a,\ b\in\mathbb{Z}\} = \{\sqrt{2}(b+a\sqrt{2} \mid a,\ b\in\mathbb{Z}\} = \langle\sqrt{2}\rangle'$$

이므로 제1동형정리에 의하여

$$\mathbb{Z}[\sqrt{2}]/\langle\sqrt{2}\rangle' \cong \mathbb{Z}_2$$

이다.

다음에 $\mathbb{Z}[\sqrt{2}]/\langle 2\rangle'$의 원소 $\sqrt{2}+\langle 2\rangle' \neq 0+\langle 2\rangle'$에 대하여

$$(\sqrt{2}+\langle 2\rangle')^2 = 2+\langle 2\rangle' = 0+\langle 2\rangle'$$

이므로 $\mathbb{Z}[\sqrt{2}]/\langle 2\rangle'$는 정역이 아니다.

7.4.2. 곱셈노름 N(정리 7.3.6)을 이용하여 증명하자. 원소 $a+b\sqrt{5}i,\ c+d\sqrt{5}i \in \mathbb{Z}[i\sqrt{5}]$에 대하여

$$11 = (a+b\sqrt{5}i)(c+d\sqrt{5}i)$$

이라 하자. 양변에 곱셈노름을 취하면

$$121 = N(11) = N((a+b\sqrt{5}i)(c+d\sqrt{5}i)) = N(a+b\sqrt{5}i)N(c+d\sqrt{5}i) = (a^2+5b^2)(c^2+5d^2)$$

이므로 a^2+5b^2은 121의 약수 1, 11, 121 중의 하나이다. 이 때 $a^2+5b^2=11$인 $a, b\in\mathbb{Z}$는 없으므로 $a^2+5b^2=1$이거나 $c^2+5d^2=1$이다. 정리 7.3.7에 의하여 $a+b\sqrt{5}i$가 단원이거나 $c+d\sqrt{5}i$가 단원이 되어 11은 기약원이다.

11과 같은 방법으로 $-2+i\sqrt{5}$도 기약임을 증명할 수 있다.

7.4.3. 정리 7.3.7에 의하여 $a+b\sqrt{7}i \in \mathbb{Z}[\sqrt{7}i],\ N(a+b\sqrt{7}i) = a^2+7b^2 = 1$인 $a+b\sqrt{7}i \in \mathbb{Z}[\sqrt{7}i]$가 가역원이다. 그러면 $a=\pm 1, b=0$이므로 $\mathbb{Z}[\sqrt{7}i]$의 가역원은 ± 1이다.

7.4.4. $21 = 3 \cdot 7 = (1+2\sqrt{5}i)(1-2\sqrt{5}i) = (4-\sqrt{5}i)(4+\sqrt{5}i)$이다.

여기서 3, 7, $1+2\sqrt{5}i$, $1-2\sqrt{5}i$, $4-\sqrt{5}i$, $4+\sqrt{5}i$가 기약원임을 보이면 된다.

1) 먼저 3인 경우. 원소 $a+b\sqrt{5}i,\ c+d\sqrt{5}i \in \mathbb{Z}(i\sqrt{5})$에 대하여

$$3 = (a+b\sqrt{5}i)(c+d\sqrt{5}i)$$

이라 하자. 양변에 곱셈노름을 취하면

$$9 = N(3) = N((a+b\sqrt{5}i)(c+d\sqrt{5}i)) = N(a+b\sqrt{5}i)N(c+d\sqrt{5}i) = (a^2+5b^2)(c^2+5d^2)$$

이므로 a^2+5b^2은 9의 약수 1, 3, 9 중의 하나이다. 이 때 $a^2+5b^2=3$인 $a, b\in\mathbb{Z}$는 없으므로 $a^2+5b^2=1$이거나 $c^2+5d^2=1$이다. 정리 7.3.7에 의하여 $a+b\sqrt{5}i$가 단원이거나 $c+d\sqrt{5}i$가 단원이 되어 3은 기약원이다.

2) 7인 경우. 3인 경우와 같은 방법으로 기약을 증명할 수 있다.

3) $1+2\sqrt{5}i$인 경우. 원소 $a+b\sqrt{5}i,\ c+d\sqrt{5}i \in \mathbb{Z}(i\sqrt{5})$에 대하여

$$1+2\sqrt{5}i = (a+b\sqrt{5}i)(c+d\sqrt{5}i)$$

이라 하자. 양변에 곱셈노름을 취하면

$$21 = N(1+2\sqrt{5}i) = N((a+b\sqrt{5}i)(c+d\sqrt{5}i)) = N(a+b\sqrt{5}i)N(c+d\sqrt{5}i) = (a^2+5b^2)(c^2+5d^2)$$

이므로 a^2+5b^2은 21의 약수 1, 3, 7, 21 중의 하나이다. 이 때 $a^2+5b^2=3$ 또는 7인 $a, b\in\mathbb{Z}$는 없으므로 $a^2+5b^2=1$이거나 $c^2+5d^2=1$이다. 정리 7.3.7에 의하여 $a+b\sqrt{5}i$가 단원이거나 $c+d\sqrt{5}i$가 단원이 되어 $1+2\sqrt{5}i$은 기약원이다.

4) $1-2\sqrt{5}i$인 경우. $1+2\sqrt{5}i$와 같은 방법으로 기약임을 보일 수 있다.

5) $4-\sqrt{5}i$인 경우. 원소 $a+b\sqrt{5}i,\ c+d\sqrt{5}i \in \mathbb{Z}[i\sqrt{5}]$에 대하여

$$4-\sqrt{5}i = (a+b\sqrt{5}i)(c+d\sqrt{5}i)$$

이라 하자. 양변에 곱셈노름을 취하면

$$21 = N(4-\sqrt{5}i) = N((a+b\sqrt{5}i)(c+d\sqrt{5}i)) = N(a+b\sqrt{5}i)N(c+d\sqrt{5}i) = (a^2+5b^2)(c^2+5d^2)$$

이므로 a^2+5b^2은 21의 약수 1, 3, 7, 21 중의 하나이다. 이 때 $a^2+5b^2=3$ 또는 7인 $a, b\in\mathbb{Z}$는 없으므로

$a^2+5b^2=1$이거나 $c^2+5d^2=1$이다. 정리 7.3.7에 의하여 $a+b\sqrt{5}i$가 단원이거나 $c+d\sqrt{5}i$가 단원이 되어 $4-\sqrt{5}i$은 기약원이다.

6) $4+\sqrt{5}i$인 경우. $4-\sqrt{5}i$와 같은 방법으로 기약임을 보일 수 있다.

7.4.5. (1) 정리 7.3.7에 의하여 $\pm 1=N(a+b\sqrt{10})=a^2-10b^2$인 정수 a, b의 4쌍만 구하면 된다. 예를 들어

$$(a,b)=(1,0),\ (-1,0),\ (3,1),\ (3,-1)\ \cdots$$

에서 $1,\ -1,\ 3+\sqrt{10},\ 3-\sqrt{10},\ \cdots$가 단원이다.

(2) 2-1) 2가 기약임을 보이자. 원소 $a+b\sqrt{10},\ c+d\sqrt{10}\in\mathbb{Z}[\sqrt{10}]$에 대하여

$$2=(a+b\sqrt{10})(c+d\sqrt{10})$$

이라 하자. 양변에 곱셈노름을 취하면

$$4=N(2)=N((a+b\sqrt{10})(c+d\sqrt{10}))=N(a+b\sqrt{10})N(c+d10)=(a^2-10b^2)(c^2-10d^2)$$

이므로 a^2-10b^2은 4의 약수 $\pm 1,\ \pm 2,\ \pm 4$ 중의 하나이다. 이 때

$$a^2-10b^2=2\text{이거나 } a^2-10b^2=-2$$

이면 $a^2\equiv 2(\mathrm{mod}\,5)$이거나 $a^2\equiv -2\equiv 3(\mathrm{mod}\,5)$이다. 르장드르 기호를 이용하면

$$\left(\frac{2}{5}\right)=(-1)^{\frac{4\cdot 6}{8}}=-1\text{이고 } \left(\frac{-2}{5}\right)=\left(\frac{-1}{5}\right)\left(\frac{2}{5}\right)=(-1)^{\frac{4}{2}}(-1)=-1$$

이므로 해가 존재하지 않는다. 그러므로 a^2-10b^2은 ± 1이거나 c^2-10d^2은 ± 1이다. 정리 7.3.7에 의하여 $a+b\sqrt{10}$가 단원이거나 $c+d\sqrt{10}$가 단원이 되어 2는 기약원이다.

2-2) $4-\sqrt{10}$이 기약임을 보이자. 원소 $a+b\sqrt{10},\ c+d\sqrt{10}\in\mathbb{Z}[\sqrt{10}]$에 대하여

$$4-\sqrt{10}=(a+b\sqrt{10})(c+d\sqrt{10})$$

이라 하자. 양변에 곱셈노름을 취하면

$$6=N(4-\sqrt{10})=N((a+b\sqrt{10})(c+d\sqrt{10}))=N(a+b\sqrt{10})N(c+d10)=(a^2-10b^2)(c^2-10d^2)$$

이므로 a^2-10b^2은 6의 약수 $\pm 1,\ \pm 2,\ \pm 3,\ \pm 6$ 중의 하나이다. 이 때

$$a^2-10b^2=\pm 2\text{이거나 } a^2-10b^2=\pm 3$$

이면 2-1)과 같은 방법으로 해가 존재하지 않음을 보일 수 있다. 그러면 a^2-10b^2은 ± 1이거나 c^2-10d^2은 ± 1이다. 정리 7.3.7에 의하여 $a+b\sqrt{10}$가 단원이거나 $c+d\sqrt{10}$가 단원이 되어 $4-\sqrt{10}$은 기약원이다.

(3) 3-1) 2가 소원이 아님을 보이자. $(4+\sqrt{10})(4-\sqrt{10})=6$이므로

$$2|6\ \Rightarrow\ 2|(4+\sqrt{10})(4-\sqrt{10})$$

이다. 하지만 $2|(4+\sqrt{10})$이면

$$(4+\sqrt{10})=2t,\ t\in\mathbb{Z}[\sqrt{10}]$$

이다. 그러면

$$6=N(4+\sqrt{10})=N(2t)=N(2)N(t)=4N(t)\ \Rightarrow\ 4|6$$

이 되어 모순이다. 따라서 $2\nmid(4+\sqrt{10})$이다. 같은 방법으로 $2\nmid(4-\sqrt{10})$을 보일 수 있으므로 2는 소원이 아니다.

3-2) $4-\sqrt{10}$가 소원이 아님을 보이자.

$$4-\sqrt{10}\,|\,6\ \Rightarrow\ 4-\sqrt{10}\,|\,2\cdot 3$$

이다. 하지만 $(4+\sqrt{10})\,|\,2$이면

$$2=(4+\sqrt{10})t,\ t\in\mathbb{Z}[\sqrt{10}]$$

이다. 그러면

$$4=N(2)=N((4+\sqrt{10})t)=N(4+\sqrt{10})N(t)=6N(t)\ \Rightarrow\ 6|4$$

이 되어 모순이다. 따라서 $(4+\sqrt{10})\nmid 2$이다. 같은 방법으로 $(4+\sqrt{10})\nmid 3$을 보일 수 있으므로 $4-\sqrt{10}$는 소원이 아니

다.

7.4.6. $a, b\in D$가 존재하여 $\alpha=\gamma a,\ \beta=\gamma b$이다. 따라서

$$GCD(N(\alpha),N(\beta))=GCD(N(\gamma a),N(\gamma b))=GCD(N(\gamma)N(a),N(\gamma)N(b))$$

이므로 $N(\gamma)$는 $GCD(N(\alpha),N(\beta))$의 약수이다.

7.4.7 잉여환 $\mathbb{Z}[i]/<2>'$는 유한환이다(정리 7.4.10). 또한

$$<2>'<\{2a+bi\,|\,a,b\in\mathbb{Z}\}<\mathbb{Z}[i]$$

이므로 $<2>'$는 극대 아이디얼이 아니다. 따라서 $\mathbb{Z}[i]/<2>'$는 체가 아니다. 만약 $\mathbb{Z}[i]/<2>'$가 정역이면 유한 정역이 되어 체(정리 5.2.9)가 되므로 모순이다. 따라서 $\mathbb{Z}[i]/<2>'$는 정역이 아니다.

(별해) $U(\mathbb{Z}[i])=\{\pm1,\ \pm i\}$이다. 원소 $\alpha+<2>'\in\mathbb{Z}[i]/<2>'$를 $\overline{\alpha}=\alpha+<2>'$라 정의하자. 그러면

$$\overline{(1+i)}\cdot\overline{(1-i)}=\overline{(1+i)(1-i)}=\overline{2}=\overline{0}$$

이다. 만약 $\overline{(1+i)}=\overline{0}$이면 적당한 원소 $t\in\mathbb{Z}[i]$가 존재하여 정리 3.1.7(4)과 곱셈노름 N을 이용하면

$$1+i=2t\ \Rightarrow\ 2=N(1+i)=N(2t)=N(2)N(t)=4N(t)$$

이다. 이때 $4|2$가 되어 모순이다. 따라서 $\overline{(1+i)}\neq\overline{0}$이다. 같은 방법으로 $\overline{(1-i)}\neq\overline{0}$이다. 그러면 영인자가 존재하므로 $\mathbb{Z}[i]/<2>'$는 정역이 아니다.

7.4.8. $\mathbb{Z}[i]/\langle 2+2i\rangle'=\{a+bi+\langle 2+2i\rangle'\,|\,a+bi\in\mathbb{Z}[i],\ N(a+bi)<N(2+2i)=8\}$이다.

이때 원소 $\alpha+\langle 2+2i\rangle'\in\mathbb{Z}[i]/\langle 2+2i\rangle'$를 $\overline{\alpha}=\alpha+\langle 2+2i\rangle'$라 정의하자. 그러면

$$\mathbb{Z}[i]/\langle 2+2i\rangle'=\{\overline{0},\ \overline{\pm1},\ \overline{\pm i},\ \overline{\pm1\pm i},\ \overline{\pm1\mp i},\ \overline{\pm2},\ \overline{\pm2i},\ \overline{\pm2\pm i},\ \overline{\pm2\mp i},\ \overline{\pm1\pm2i},\ \overline{\pm1\mp2i}\}$$

이다(복호동순). 한편

$$\overline{0}=\overline{(2+2i)}\ \Rightarrow\ \overline{2}=\overline{-2i},\ \overline{-2}=\overline{2i},$$
$$\overline{0}=\overline{(2+2i)(1-i)}=\overline{4}\ \Rightarrow\ \overline{2}=\overline{-2}$$

이므로 $\overline{2}=\overline{-2}=\overline{2i}=\overline{-2i}$이다. 따라서

$$\overline{2+i}=\overline{2}+\overline{i}=\overline{-2i}+\overline{i}=\overline{-i}$$
$$\overline{2-i}=\overline{2}-\overline{i}=\overline{2i}-\overline{i}=\overline{i}$$
$$\overline{1+2i}=\overline{1}+\overline{2i}=\overline{1}+\overline{-2}=\overline{-1}$$
$$\overline{1-2i}=\overline{1}-\overline{2i}=\overline{1}-\overline{2}=\overline{-1}$$

이다. 나머지 2가 있는 원소는 같은 방법으로 $\overline{\pm1},\ \overline{\pm i},\ \overline{2}$ 중의 하나와 같음을 증명할 수 있으므로

$$\mathbb{Z}[i]/\langle 2+2i\rangle'=\{\overline{0},\ \overline{\pm1},\ \overline{\pm i},\ \overline{\pm1\pm i},\ \overline{\pm1\mp i},\ \overline{2}\}$$

이다. 한편

$$\overline{1+i}-\overline{-1-i}=\overline{2+2i}=\overline{0}\ \Rightarrow\ \overline{1+i}=\overline{-1-i}$$
$$\overline{1-i}-\overline{-1+i}=\overline{2-2i}=\overline{(2+2i)(-i)}=\overline{0}\ \Rightarrow\ \overline{1-i}=\overline{-1+i}$$

이다. 따라서

$$\mathbb{Z}[i]/\langle 2+2i\rangle'=\{\overline{0},\ \overline{1},\ \overline{-1},\ \overline{i},\ \overline{-i},\ \overline{1+i},\ \overline{1-i},\ \overline{2}\}$$

이다. 이때 각 원소의 차의 곱셈노름을 구해 보면 $8(=N(2+2i))$의 배수가 아니므로 서로 다른 원소가 된다. 예를 들어 $\overline{i}=\overline{-i}$이라 하자. 그러면

$$i-(-i)=2i\in\langle 2+2i\rangle'$$

이고, 적당한 $t\in\mathbb{Z}[i]$에 대하여

$$2i=(2+2i)t\ \Rightarrow\ 4=N(2i)=N((2+2i)t)=N(2+2i)N(t)=8N(t)$$

에서 $8|4$가 되어 모순이다. 따라서 $\overline{i}\neq\overline{-i}$이다.

따라서 $\mathbb{Z}[i]/\langle 2+2i\rangle'$은 8개의 원소를 가진다.

7.4.9. (1) $\mathbb{Z}[i]/\langle 1-2i\rangle'=\{a+bi+\langle 1-i\rangle'\,|\,a+bi\in\mathbb{Z}[i],\ N(a+bi)<N(1-2i)=5\}$이다.

이때 원소 $\alpha+\langle 1-2i\rangle'\in\mathbb{Z}[i]/\langle 1-2i\rangle'$를 $\overline{\alpha}=\alpha+\langle 1-2i\rangle'$라 정의하자. 그러면

$$\mathbb{Z}[i]/\langle 1-2i\rangle'=\{\overline{0},\ \overline{\pm 1},\ \overline{\pm i},\ \overline{\pm 1\pm i},\ \overline{\pm 1\mp i},\ \overline{\pm 2},\ \overline{\pm 2i}\}$$

이다(복호동순). 한편

$$\begin{aligned}&\overline{0}=\overline{(1-2i)}\Rightarrow\ \overline{1}=\overline{2i},\\&\overline{0}=\overline{(1-2i)(i)}=\overline{(i+2)}\Rightarrow\ \overline{i}=\overline{-2},\\&\overline{0}=\overline{(1-2i)(1+2i)}=\overline{5}\end{aligned}$$

이다. 따라서 $\overline{-2}=\overline{3}$이므로

$$\mathbb{Z}[i]/\langle 1-2i\rangle'=\{\overline{0},\ \overline{\pm 1},\ \overline{\pm 2},\ \overline{\pm 3},\ \overline{\pm 4}\}$$

이다. 한편

$$\overline{1}=\overline{-4},\ \overline{2}=\overline{-3},\ \overline{3}=\overline{-2},\ \overline{4}=\overline{-1}$$

이다. 따라서

$$\mathbb{Z}[i]/\langle 1-2i\rangle'=\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4}\}$$

이다. 이때 각 원소의 차의 곱셈노름을 구해 보면 $5(=N(1-2i))$의 배수가 아니므로 서로 다른 원소가 된다. 예를 들어 $\overline{1}=\overline{4}$이라 하자. 그러면

$$4-1=3\in\langle 1-2i\rangle'$$

이고, 적당한 $t\in\mathbb{Z}[i]$에 대하여

$$3=(1-2i)t\ \Rightarrow\ 9=N(3)=N((1-2i)t)=N(1-2i)N(t)=5N(t)$$

에서 $5|3$가 되어 모순이다. 따라서 $\overline{1}\neq\overline{4}$이다.

따라서 $\mathbb{Z}[i]/\langle 1-2i\rangle'$은 5개의 원소를 가진다. 그러면 체 $\mathbb{Z}_5$와 동형이므로 체가 된다.

(2) 위 풀이 (1)에서 $\overline{i}=\overline{-2}$이므로 $\overline{(1+i)}=\overline{(1-2)}=\overline{-1}$이다. 따라서

$$\overline{(1+i)}^2=\overline{(-1)}^2=\overline{1}$$

이므로 $\overline{(1+i)}^{-1}=\overline{(1+i)}$이다.

7.4.10. 7이 PID $\mathbb{Z}[i]$에서 기약원임을 보이면 충분하다(정리 7.4.10(2)).

원소 $a+bi,\ c+di\in\mathbb{Z}[i]$에 대하여

$$7=(a+bi)(c+di)$$

이라 하자. 양변에 곱셈노름을 취하면

$$49=N(7)=N((a+bi)(c+di))=N(a+bi)N(c+di)=(a^2+b^2)(c^2+d^2)$$

이므로 a^2+b^2은 49의 약수 1, 7, 49 중의 하나이다. 이 때 $a^2+b^2=7$인 $a,b\in\mathbb{Z}$는 없으므로 $a^2+b^2=1$이거나 $c^2+d^2=1$이다. 정리 7.3.7에 의하여 $a+bi$가 단원이거나 $c+di$가 단원이 되어 7은 기약원이다. (정리 7.2.6에 의하여 $\langle 7\rangle'$은 극대 아이디얼이고, 정리 6.5.8에 의하여) $\mathbb{Z}[i]/\langle 7\rangle'$은 체이다(또는 정리 7.4.10(2)).

다음에 원소수를 구하자.

$\mathbb{Z}[i]/\langle 7\rangle'=\{a+bi+\langle 7\rangle'\mid a+bi\in\mathbb{Z}[i],\ N(a+bi)<N(7)=49\}$이다.

이때 원소 $\alpha+\langle 7\rangle'\in\mathbb{Z}[i]/\langle 7\rangle'$를 $\overline{\alpha}=\alpha+\langle 7\rangle'$라 정의하자. 그러면 $\overline{0}=\overline{7}$이므로

$$\begin{aligned}&\overline{6}=\overline{-1},\ \overline{-6}=\overline{1},\\&\overline{5}=\overline{-2},\ \overline{-5}=\overline{2},\\&\overline{4}=\overline{-3},\ \overline{-4}=\overline{3}\end{aligned}$$

이다. 그러므로

$$\mathbb{Z}[i]/\langle 7\rangle'=\{\overline{0},\ \overline{\pm 1},\ \overline{\pm 2},\ \overline{\pm 3},\ \overline{\pm i},\ \overline{\pm 2i},\ \overline{\pm 3i},\ \overline{\pm a\pm bi},\ \overline{\pm a\mp bi},\ a=1,2,3,\ b=1,2,3\}$$

이다(복호동순).

이다. 이때 두 원소의 차 $c+di\ (c,d=0,\pm 1,\cdots\pm 6)$의 곱셈노름을 구해 보면

$$1^2=1,\ 2^2=4,\ 3^2=9,\ 4^2=16,\ 5^2=25,\ 6^2=36,$$

$$
\begin{aligned}
&(|c|,|d|) \text{ or } (|d|,|c|)=(1,1) \Rightarrow N(c+di)=1^2+1^2=2,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(1,2) \Rightarrow N(c+di)=1^2+2^2=5,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(1,3) \Rightarrow N(c+di)=1^2+3^2=10,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(1,4) \Rightarrow N(c+di)=1^2+4^2=17,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(1,5) \Rightarrow N(c+di)=1^2+5^2=26,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(1,6) \Rightarrow N(c+di)=1^2+6^2=37,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(2,2) \Rightarrow N(c+di)=2^2+2^2=8,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(2,3) \Rightarrow N(c+di)=2^2+3^2=13,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(2,4) \Rightarrow N(c+di)=2^2+4^2=20,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(2,5) \Rightarrow N(c+di)=2^2+5^2=29,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(2,6) \Rightarrow N(c+di)=2^2+6^2=40,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(3,3) \Rightarrow N(c+di)=3^2+3^2=18,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(3,4) \Rightarrow N(c+di)=3^2+4^2=25,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(3,5) \Rightarrow N(c+di)=3^2+5^2=34,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(3,6) \Rightarrow N(c+di)=3^2+6^2=45,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(4,4) \Rightarrow N(c+di)=4^2+4^2=32,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(4,5) \Rightarrow N(c+di)=4^2+5^2=41,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(4,6) \Rightarrow N(c+di)=4^2+6^2=52,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(5,5) \Rightarrow N(c+di)=5^2+5^2=50,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(5,6) \Rightarrow N(c+di)=5^2+6^2=61,\\
&(|c|,|d|) \text{ or } (|d|,|c|)=(6,6) \Rightarrow N(c+di)=6^2+6^2=72
\end{aligned}
$$

중에서 나온다. 하지만 어느 것도 $49(=N(7))$의 배수가 아니므로 서로 다른 원소이다(정리 3.1.7(1) 참조).

예를 들어 $\overline{3+3i}=\overline{-3-3i}$이라 하자. 그러면

$$(3+3i)-(-3-3i)=6+6i\in\langle 7\rangle'$$

이고, 적당한 $t\in\mathbb{Z}[i]$에 대하여

$$6+6i=7t \Rightarrow 72=N(6+6i)=N(7t)=N(7)N(t)=49N(t)$$

에서 $49|72$가 되어 모순이다. 따라서 $\overline{3+3i}\neq\overline{-3-3i}$이다.

여기서 $\overline{\pm a\pm bi}$, $\overline{\pm a\mp bi}$의 쌍이 $4\cdot 9=36$개이므로 원소수는 49개이다.

따라서 $\mathbb{Z}[i]/\langle 7\rangle'$은 49개의 원소를 가진다.

7.4.11. (1)(문제 수정) 잉여환 $\mathbb{Z}[i]/\langle 3\rangle'$은 체임을 보이고 위수를 구하라.

(풀이) 3이 PID $\mathbb{Z}[i]$에서 기약원임을 보이면 충분하다(정리 7.4.10(2)). .

원소 $a+bi,\ c+di\in\mathbb{Z}[i]$에 대하여

$$3=(a+bi)(c+di)$$

이라 하자. 양변에 곱셈노름을 취하면

$$9=N(3)=N((a+bi)(c+di))=N(a+bi)N(c+di)=(a^2+b^2)(c^2+d^2)$$

이므로 a^2+b^2은 9의 약수 1, 3, 9 중의 하나이다. 이 때 $a^2+b^2=3$인 $a,b\in\mathbb{Z}$는 없으므로 $a^2+b^2=1$이거나 $c^2+d^2=1$이다. 정리 7.3.7에 의하여 $a+bi$가 단원이거나 $c+di$가 단원이 되어 3은 기약원이다. (정리 7.2.6에 의하여 $\langle 3\rangle'$은 극대 아이디얼이고, 정리 6.5.8에 의하여) $\mathbb{Z}[i]/\langle 3\rangle'$은 체이다(또는 정리 7.4.10(2)).

다음에 위수를 구하자.

$\mathbb{Z}[i]/\langle 3\rangle'=\{a+bi+\langle 3\rangle' \mid a+bi\in\mathbb{Z}[i],\ N(a+bi)<N(3)=9\}$이다.

이때 원소 $\alpha+\langle 3\rangle'\in\mathbb{Z}[i]/\langle 3\rangle'$를 $\overline{\alpha}=\alpha+\langle 3\rangle'$라 정의하자. 그러면

$$\mathbb{Z}[i]/\langle 3\rangle'=\{\overline{0},\ \overline{\pm 1},\ \overline{\pm i},\ \overline{\pm 1\pm i},\ \overline{\pm 1\mp i},\ \overline{\pm 2},\ \overline{\pm 2i},\ \overline{\pm 2\pm i},\ \overline{\pm 2\mp i},\ \overline{\pm 1\pm 2i},\ \overline{\pm 1\mp 2i}\}$$

이다(복호동순). 한편 $\overline{0}=\overline{3}$이므로 $\overline{2}=\overline{-1}$이고 $\overline{-2}=\overline{1}$이다. 그러므로

$$\mathbb{Z}[i]/\langle 3\rangle'=\{\overline{0},\ \overline{\pm 1},\ \overline{\pm i},\ \overline{\pm 1\pm i},\ \overline{\pm 1\mp i}\}$$

이다. 이때 두 원소의 차의 곱셈노름을 구해 보면 $9(=N(3))$의 배수가 아니므로 서로 다른 원소가 된다. 예를 들어 $\overline{i}=\overline{-i}$이라 하자. 그러면

$$i-(-i)=2i\in\langle 3\rangle'$$

이고(정리 3.1.7(1) 참조), 적당한 $t\in\mathbb{Z}[i]$에 대하여

$$2i=3t \Rightarrow 4=N(2i)=N(3t)=N(3)N(t)=9N(t)$$

에서 $9|4$가 되어 모순이다. 따라서 $\overline{i}\neq\overline{-i}$이다.

따라서 $\mathbb{Z}[i]/\langle 3\rangle'$은 9개의 원소를 가진다.

(2) 노름이 4인 원소를 $a+bi\in\mathbb{Z}[i]$라 하자. 그러면

$$4=N(a+bi)=a^2+b^2$$

이므로 $a=0,\ b=\pm 2$이거나 $a=\pm 2,\ b=0$이어야 한다. 한편 $2+\langle 3\rangle'=-1+\langle 3\rangle',\ 2i+\langle 3\rangle'=-i+\langle 3\rangle'$이다. 그러므로

$$\begin{aligned}
&a+bi+\langle 3\rangle'=2+\langle 3\rangle'=-1+\langle 3\rangle',\\
&a+bi+\langle 3\rangle'=-2+\langle 3\rangle'=1+\langle 3\rangle',\\
&a+bi+\langle 3\rangle'=2i+\langle 3\rangle'=-i+\langle 3\rangle',\\
&a+bi+\langle 3\rangle'=-2i+\langle 3\rangle'=i+\langle 3\rangle'
\end{aligned}$$

이다.

== 연습문제 (8.1) ==

8.1.1. $T: V\to W$ 는 동형사상이다. B와 V의 기저이면 $T(B)$는 W의 기저가 됨을 보여라.

(풀이) T가 동형 사상이므로 $\dim V=din\,W=n$이라 하고, $B=\{b_1, b_2, \cdots, b_n\}$가 V의 기저라 하자.

$T(B)=\{T(b_1), T(b_2), \cdots, T(b_n)\}$가 W의 기저임을 보이자. 정리 8.1.7에 의하여 $T(B)$가 1차독립임을 보이면 충분하다.

스칼라 $x_i\in F\ (i=1,2,\cdots,n)$에 대하여 $x_1T(b_1)+x_2T(b_2)+\cdots+x_nT(b_n)=0$이라 하자. 그러면

$$T(x_1b_1+x_2b_2+\cdots+x_nb_n)=0$$

이고 T가 단사함수이므로

$$x_1b_1+x_2b_2+\cdots+x_nb_n=0$$

이다. 이때 B가 기저이므로 $x_1=x_2=\cdots=x_n=0$이다. 따라서 $T(B)$는 W에서 최대 1차독립이므로 W의 기저이다(정리 8.1.7).

8.1.2 (1) $f(0)=0$이므로 $0\in f(V)$이다.

임의의 $f(a),\ f(b)\in F(V),\ r\in F$에 대하여

$$\begin{aligned}
&f(a)+f(b)=f(a+b)\in F(V),\\
&rf(a)=f(ra)\in F(V)
\end{aligned}$$

이므로 $F(V)$는 V'의 부분공간이다.

(2) $\dim V=n,\ \dim\ker(f)=m(m\le n)$이라 하자.

$\ker(f)$의 기저를 $\{v_1,\cdots,v_m\}$라 하자. 그러면 기저확장정리에 의해 V의 기저 $\{v_1,\cdots,v_m,v_{m+1},\cdots,v_n\}$이 존재한다.

그러면 임의의 $f(v)\in f(V)$에 대하여 $v=a_1v_1+\cdots+a_mv_m+a_{m+1}v_{m+1}+\cdots+a_nv_n\in V$인 스칼라 $a_i\in F$가 존재하므로

$$\begin{aligned}
f(v)&=f(a_1v_1+\cdots+a_mv_m+a_{m+1}v_{m+1}+\cdots+a_nv_n)=a_1f(v_1)+\cdots+a_mf(v_m)+a_{m+1}f(v_{m+1})+\cdots+a_nf(v_n)\\
&=a_{m+1}f(v_{m+1})+\cdots+a_nf(v_n)
\end{aligned}$$

이다. 따라서 $f(v_{m+1}),\cdots,f(v_n)$은 $f(V)$의 생성원이 된다.

다음에 $\alpha_{m+1},\cdots,\alpha_n\in F$가 존재하여

$$\alpha_{m+1}f(v_{m+1})+\cdots+\alpha_nf(v_n)=0$$

$\Rightarrow\ f(\alpha_{m+1}v_{m+1})+\cdots+f(\alpha_n v_n)=0$

$\Rightarrow\ f(\alpha_{m+1}v_{m+1}+\cdots+\alpha_n v_n)=0$

$\Rightarrow\ \alpha_{m+1}v_{m+1}+\cdots+\alpha_n v_n\in\ker(f)$

$\Rightarrow\ b_1v_1+\cdots+b_mv_m=\alpha_{m+1}v_{m+1}+\cdots+\alpha_n v_n$이 되는 $b_1,\cdots,b_m\in F$가 존재한다.

$\Rightarrow\ b_1v_1+\cdots+b_mv_m+(-\alpha_{m+1})v_{m+1}+\cdots+(-\alpha_n)v_n=0$

$\Rightarrow\ b_1=\cdots=b_m=-\alpha_{m+1}=\cdots=-\alpha_n=0$ ($\because\{v_1,\cdots,v_n\}$이 기저이므로 1차독립)

$\Rightarrow\ \alpha_{m+1}=\ \cdots\ =\alpha_n=0$

그러므로 $f(v_{m+1}),\cdots,f(v_n)$은 일차독립이다. 따라서 $f(v_{m+1}),\cdots,f(v_n)$은 $f(V)$의 기저이다.

$\dim f(V)=n-m$, $\dim\ker(f)=m$, $\dim V=n$이므로 $\dim V=\dim\ker(f)+\dim f(V)$이다.

8.1.3

(1) $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$이므로 $\mathbb{Q}(\sqrt{2})$의 기저는 $\{1,\sqrt{2}\}$이다.

(2) $\mathbb{Q}(\sqrt[3]{2})=\{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2\mid a,b\in\mathbb{Q}\}$이므로 $\mathbb{Q}(\sqrt[3]{2})$의 기저는 $\{1,\sqrt[3]{2},(\sqrt[3]{2})^2\}$이다.

8.1.4

4. $x=\sqrt{2+\sqrt{2}}$라 하자.

$x^2=(\sqrt{2+\sqrt{2}})^2=2+\sqrt{2}$

$\Rightarrow\ x^2-2=\sqrt{2}$

$\Rightarrow\ (x^2-2)^2=(\sqrt{2})^2$

$\Rightarrow\ x^4-4x^2+4=2$

$\Rightarrow\ x^4-4x^2+2=0$이다.

$f(x)=x^4-4x^2+2\in\mathbb{Q}[x]$라 하자.

x^4-4x^2+2가 기약임을 보이자. 일차인수가 있다면, 즉, $f(x)$의 근이 존재한다면 ±1 또는 ±2 중에 있다. 하지만 $f(\pm1)=-1$, $f(\pm2)=2$이므로 일차인수는 없다.

다음에 $f(x)$의 이차인수가 존재한다고 하자.

$f(x)=x^4-4x^2+2=(x^2+ax+b)(x^2+cx+d)\ \ (a,b,c,d\in\mathbb{Z})$

$=x^4+(a+c)x^3+(ac+b+d)x^2+(ad+bc)x+bd$

$\Rightarrow\ a+c=0$, $ac+b+d=-4$, $ad+bc=0$, $bd=2$

$\Rightarrow\ a=-c$, $b+d=-4-ac$, $a(d-b)=0$, $bd=2$

이다(정리 5.6.7). 이때 $a=0$이면 $b+d=-4$, $bd=2$이고 $a\neq0$이면 $b-d=0$, $b^2=2$이다. 이 식을 만족하는 $b,d\in\mathbb{Z}$는 존재하지 않으므로 모순이다. 따라서 $f(x)$의 이차인수는 존재하지 않는다. 따라서 $f(x)$는 $\mathbb{Q}$ 위에서 기약이다.

$\therefore irr(\sqrt{2+\sqrt{2}},\mathbb{Q})=x^4-4x^2+2$

8.1.5. $x=i+\sqrt{2}$라 하자. $x-\sqrt{2}=i$, $(x-\sqrt{2})^2=-1$, $x^2-2\sqrt{2}x+3=0$이다.

$p(x)=x^2-2\sqrt{2}x+3\in\mathbb{Q}(\sqrt{2})[x]$, $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$

가 $\mathbb{Q}(\sqrt{2})[x]$에서 일차인수가 없음을 보이자. $p(x)$의 두 근 $\sqrt{2}\pm i$는 $\mathbb{Q}(\sqrt{2})$의 원소가 아니므로 인수정리에 의하여 $\mathbb{Q}(\sqrt{2})[x]$에서 일차인수를 갖지 않는다. 따라서 $p(x)=x^2-2\sqrt{2}x+3$는 $\mathbb{Q}(\sqrt{2})$ 위에서 기약이다.

(별해) $a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$가 근이라 하자.

$(a+b\sqrt{2})^2-2\sqrt{2}(a+b\sqrt{2})+3=0$이고 $a^2+2b^2+2\sqrt{2}ab-2\sqrt{2}a-4b+3=0$이다.

즉, $a^2+2b^2-4b+(2ab-2a)\sqrt{2}=-3$이다. $a^2+2b^2-4b=-3$이고 $2a(b-1)=0$이다.

먼저 $a=0$인 경우 $2b^2-4b=-3$이므로 $b=2\pm\sqrt{2}i$는 $\mathbb{Q}$의 원소가 아니다.

다음에 $b=1$인 경우 $a^2-2=-3$, $a=-i$는 $\mathbb{Q}$의 원소가 아니므로 인수 정리에 의하여 $\mathbb{Q}(\sqrt{2})[x]$에서 일차 인수가 없으므로 $x^2-2\sqrt{2}x+3$는 $\mathbb{Q}(\sqrt{2})$ 위에서 기약이다.

8.1.6

6. $\sqrt{3}+i$의 다음 체위에서의 기약다항식을 구하라.

(1) $irr(\sqrt{3}+i, \mathbb{R})$을 구하자.

$x=\sqrt{3}+i$라 하자

$$x-\sqrt{3}=i$$
$$x^2-2\sqrt{3}x+3=-1$$
$$x^2-2\sqrt{3}x+4=0$$

$p(x)=x^2-2\sqrt{3}x+4\in\mathbb{R}[x]$라 하자. $p(x)$의 근은 $\sqrt{3}\pm i$은 실수가 아니므로 인수정리에 의하여 $p(x)$에 1차인수가 없다. 따라서 $p(x)$는 $\mathbb{R}$ 위에서 기약이다

$$\therefore irr(\sqrt{3}+i, \mathbb{R})=x^2-2\sqrt{3}x+4$$

(2) $irr(\sqrt{3}+i, \mathbb{Q})$를 구하자.

$x=\sqrt{3}+i$라 하자

$$x^2=3+2i\sqrt{3}-1=2+2i\sqrt{3}$$
$$x^2-2=2i\sqrt{3}$$
$$x^4-4x^2+16=0$$

$p(x)=x^4-4x^2+16\in\mathbb{Q}[x]$라 하자. 만약 $p(x)$가 $\mathbb{Q}[x]$에서 1차인수가 있으면 따름정리 5.6.9에 의하여 $p(x)$의 근은 16의 약수에서 존재한다.

$$p(\pm 1)=1-4+16\neq 0$$
$$p(\pm 4)=4^4-4^3+16\neq 0$$
$$p(\pm 16)=16^4-4\times 16^2+16\neq 0$$

이므로 인수정리에 의하여 $p(x)$는 $\mathbb{Q}[x]$에서 1차인수가 없다

$p(x)$가 $\mathbb{Q}[x]$에서 2차인수가 없음을 보자.

$$p(x)=(x^2+ax+b)(x^2+cx+d)\ \ a,b,c,d\in\mathbb{Z}$$

라 하자(정리 5.6.7).

$$p(x)=x^4+(a+c)x^3+(b+d+ax)x^2+(ad+bc)x+bd$$
$$\begin{cases} a+c=0 \\ b+d+ac=-4 \\ ad+bc=0 \\ bd=16 \end{cases}$$

에서 $a=-c$, $a(b-d)=0$이므로 $a=0$이거나 $b=d$이다.

$a=0$인 경우에는 $b+d=-4$, $bd=16$이므로

$$16=bd=b(-b-4)=-b^2-4b \Rightarrow (b+2)^4+12=0$$

를 만족하는 정수는 없다.

다음에 $b=d$인 경우에는

$$a^2=2b+4,\ b^2=16 \Rightarrow a^2=12 \text{ or } -4$$

를 만족하는 정수는 없다. 따라서 $p(x)$에 $\mathbb{Q}[x]$에서 2차인수가 없으므로 $\mathbb{Q}$ 위에서 기약이다.

$$\therefore irr(\sqrt{3}+i, \mathbb{Q})=x^4-4x^2+16$$

(3) $irr(\sqrt{3}+i, \mathbb{Q}(i))$를 구하자. $\mathbb{Q}(i)=\{a+bi\,|\,a,b\in\mathbb{Q}\}$

$x=\sqrt{3}+i$라 하자. $x-i=\sqrt{3}$이므로 $x^2-2ix-4=0$이다.

$p(x)=x^2-2ix-4\in\mathbb{Q}(i)[x]$의 두 근 $i\pm\sqrt{3}$은 $\mathbb{Q}(i)$에 속하지 않으므로 인수정리에 의하여 $\mathbb{Q}(i)[x]$에서 일차인수가 없다.

따라서 $irr(\sqrt{3}+i, \mathbb{Q}(i))=x^2-2ix-4$이다.

(4) $irr(\sqrt{3}+i, \mathbb{Q}(\sqrt{3}))$을 구하자. $\mathbb{Q}(\sqrt{3})=\{a+b\sqrt{3}\,|\,a,b\in\mathbb{Q}\}$

$x=\sqrt{3}+i$라 하자. $x-\sqrt{3}=i$. $x^2-2\sqrt{3}x+4=0$

$p(x)=x^2-2\sqrt{3}x+4\in\mathbb{Q}(\sqrt{3})[x]$라 할 때 $\mathbb{Q}(\sqrt{3})[x]$에서 일차인수가 없음을 보이자. $p(x)$의 두 근 $\sqrt{3}\pm i$는 $\mathbb{Q}(\sqrt{3})$의 원소가 아니므로 인수정리에 의하여 $\mathbb{Q}(\sqrt{3})[x]$에서 일차인수를 갖지 않는다. 따라서 $p(x)=x^2-2\sqrt{3}x+4$는 $\mathbb{Q}(\sqrt{3})$ 위에서 기약이다.

따라서 $irr(\sqrt{3}+i,\mathbb{Q}(\sqrt{3}))=x^2-2\sqrt{3}x+4$이다.

8.1.7. $p(x)=x^4+1$는 $\mathbb{Q}$ 위의 기약다항식고 $p(u)=0$이므로 크로네커 정리에 의하여

$$\mathbb{Q}[x]/\langle p(x)\rangle'=\{a+bu+cu^2+du^3\mid a,b,c,d\in\mathbb{Q},\ u^4=-1\}$$

이다.

(1) $u^5+u^6+u^7=u^4\cdot u+u^4\cdot u^2+u^4\cdot u^3=(-u)+(-u^2)+(-u^3)$

$\therefore u^5+u^6+u^7=-u-u^2-u^3$

(2) $u+2u^4+3u^5=u+2\cdot u^4+3\cdot u^4\cdot u=u+2\cdot(-1)+3\cdot(-1)\cdot u=u-2-3u=-2u-2$

$\therefore u+2u^4+3u^5=-2u-2$

(3) $x^4+1=(x+1)(x^3-x^2+x-1)+2$

$\Rightarrow 0=u^4+1=(u+1)(u^3-u^2+u-1)+2$

$\Rightarrow (u+1)^{-1}=-\frac{1}{2}(u^3-u^2+u-1)$

(별해1) $f(x)=x^4+1$, $g(x)=x+1$라 하자.

x^3	x^4+1 x^4+x^3	$x+1$	
$-x^2$	$-x^3+1$ $-x^3-x^2$		
x	x^2+1 x^2+x		
-1	$-x+1$ $-x-1$		
	2		

따라서

몫			x^3-x^2+x-1
$f(x)$	1	0	1
$g(x)$	0	1	$-x^3+x^2-x+1$
나머지	$f(x)$	$g(x)$	2

$2=f(x)\cdot 1+g(x)(-x^3+x^2-x+1)=(x^4+1)\cdot 1+(x+1)(-x^3+x^2-x+1)$이다.

그러므로 다음을 얻는다.

$$2=(u^4+1)\cdot 1+(u+1)(-u^3+u^2-u+1)=(u+1)(-u^3+u^2-u+1)$$

$$\Rightarrow (u+1)^{-1}=\frac{1}{2}(-u^3+u^2-u+1)$$

(별해2) $(1+u)(au^3+bu^2+cu+d)=1$이라 하자.

$$au^4+(a+b)u^3+(b+c)u^2+(c+d)u+(d-1)=(d-a-1)+(a+b)u^3+(b+c)u^2+(c+d)u=0$$

에서 $-a+d-1=0$, $a+b=0$, $b+c=0$, $c+d=0$이므로 a,b,c,d 의 값을 구하면

$$a=-\frac{1}{2},\ b=\frac{1}{2},\ c=\frac{1}{2},\ d=\frac{1}{2}$$

이다. $\quad \therefore (1+u)^{-1} = -\frac{1}{2}u^3 + \frac{1}{2}u^2 - \frac{1}{2}u + \frac{1}{2}$

(4) $\quad x^4+1 = (x^3+1)x - x + 1$

$\Rightarrow\ 0 = u^4+1 = (u^3+1)u - u + 1$

$\Rightarrow\ u-1 = (u^3+1)u$

$\Rightarrow\ 1 = (u^3+1)u(u-1)^{-1}$

이다. 한편

$x^4+1 = (x-1)(x^3+x^2+x+1)+2$

$\Rightarrow\ 0 = u^4+1 = (u-1)(u^3+u^2+u+1)+2$

$\Rightarrow\ (u-1)^{-1} = -\frac{1}{2}(u^3+u^2+u+1)$

이므로 $\quad 1 = (u^3+1)u(u-1)^{-1}$

$\Rightarrow\ 1 = (u^3+1)u\left(-\frac{1}{2}(u^3+u^2+u+1)\right)$

$\Rightarrow\ (u^3+1)^{-1} = -\frac{1}{2}(u^4+u^3+u^2+u) = -\frac{1}{2}(u^3+u^2+u-1)$

(별해1) $f(x) = x^4+1,\ g(x) = x^3+1$라 하자.

x	x^4+1 x^4+x	x^3+1 x^3-x^2	$-x^2$
	$-x+1$	x^2+1 x^2-x	$-x$
		$x+1$ $x-1$	-1
		2	

따라서

몫			x	$-x^2-x-1$
$f(x)$	1	0	1	$-x^2-x-1$
$g(x)$	0	1	$-x$	$1-x^3-x^2-x$
나머지	$f(x)$	$g(x)$	$-x+1$	2

$2 = f(x)(-x^2-x-1) + g(x)(1-x^3-x^2-x) = (x^4+1)(-x^2-x-1) + (x^3+1)(1-x^3-x^2-x)$이다.

그러므로 다음을 얻는다.

$2 = (u^4+1)(-u^2-u-1) + (u^3+1)(1-u^3-u^2-u) = (u^3+1)(1-u^3-u^2-u)$

$\Rightarrow\ (u^3+1)^{-1} = \frac{1}{2}(1-u^3-u^2-u)$

(별해2) $(1+u^3)(au^3+bu^2+cu+d) = 1$이라 하자.

$(a+d)u^3 + (b-a)u^2 + (c-b)u + (d-c-1) = 0$

에서 $a+d=0,\ b-a=0,\ c-b=0,\ d-c=1$이므로 a,b,c,d 의 값을 구하면

$a = -\frac{1}{2},\ b = -\frac{1}{2},\ c = -\frac{1}{2},\ d = \frac{1}{2}$

이다. $\quad \therefore (1+u^3)^{-1} = -\frac{1}{2}u^3 - \frac{1}{2}u^2 - \frac{1}{2}u + \frac{1}{2}$

8.1.8 (1) $f(x) = x^3+x+1 \in \mathbb{Z}_5[x]$에 대하여

$f(0) = 1 \neq 0, f(1) = 3 \neq 0, f(2) = 1 \neq 0, f(-1) = f(4) = 4 \neq 0$

$f(-2) = f(3) = 1 \neq 0, f(x) = 0$인 $x \in \mathbb{Z}_5$가 존재 하지 않는다.

따라서 $f(x)$는 $\mathbb{Z}_5$ 위에서 기약이다(정리 5.6.4(2)).

(2) $f(x)$가 기약이므로 크로네커 정리에 의해 $E=\{a\theta^2+b\theta+c \mid \theta^3+\theta+1=0, a,b,c\in\mathbb{Z}_5\}$이다.

E의 원소의 개수는 5^3=125개이다.

(3) $x^3+x+1=(x+2)(x^2-2x)+1$

$\Rightarrow 0=\theta^3+\theta+1=(\theta+2)(\theta^2-2\theta)+1$

$\Rightarrow (\theta+2)^{-1}=-(\theta^2-2\theta)=-\theta^2+2\theta=4\theta^2+2\theta$

(별해) $(a\theta^2+b\theta+c)(\theta+2)=1$ 인 a,b,c를 구하자.

$a=4, b=2, c=0$이다.

$\therefore (\theta+2)^{-1}=4\theta^2+2\theta$

8.1.9 (1) $f(0)=1\neq 0$, $f(1)=1\neq 0$이므로 인수정리에 의해 $f(x)$는 일차인수를 갖지 않으므로 $\mathbb{Z}_2$에서 기약이다.

(2) $\theta=x+\langle f(x)\rangle'$

$\mathbb{Z}_2(\theta)=\mathbb{Z}_2[x]/\langle f(x)\rangle'$

$=\{g(x)+\langle f(x)\rangle' \mid g(x)\in\mathbb{Z}_2[x]\}$

$=\{f(x)\cdot g(x)+ax^2+bx+c+\langle f(x)\rangle' \mid g(x)\in\mathbb{Z}_2[x], a,b,c\in\mathbb{Z}_2\}$

$=\{a\theta^2+b\theta+c \mid a,b,c\in\mathbb{Z}_2, \theta^3+\theta+1=0\}$

$=\{0,1,\theta,\theta+1,\theta^2,\theta^2+\theta,\theta^2+1,\theta^2+\theta+1 \mid \theta^3+\theta+1=0\}$

(3) θ가 $f(x)$의 근이고 표수가 2이므로 θ,θ^2,θ^4이 $f(x)$의 근이 된다.

$\theta^4=\theta^3+\theta=\theta^2+\theta+1$이므로 $f(x)=(x-\theta)(x-\theta^2)(x-\theta^2-\theta-1)$

8.1.10 $\left\langle \frac{1}{3}x^4-x+2\right\rangle'=\langle x^4-3x+6\rangle'$이므로 $f(x)=x^4-3x+6$가 $\mathbb{Q}$ 위에서 기약임을 보이면 된다. $p=3$일 때 Eisenstein 판정에 의하여 $f(x)$는 $\mathbb{Q}$ 위에서 기약이다.

따라서 $\mathbb{Q}[x]\Big/\left\langle \frac{1}{3}x^4-x+2\right\rangle'=\mathbb{Q}[x]\Big/\langle x^4-3x+6\rangle'$은 체이다(정리 7.2.6).

$0+\langle f(x)\rangle'=(x^4-3x+6)+\langle f(x)\rangle'=(x+1)(x^3-x^2+x-4)+10+\langle f(x)\rangle'$

$\Rightarrow ((x+1)+\langle f(x)\rangle')^{-1}=-\frac{1}{10}(x^3-x^2+x-4)+\langle f(x)\rangle'$

8.1.11 i) 유리수체 $\mathbb{Q}$ 위의 다항식 $f(x)=x^3-x+1$이 $\mathbb{Q}$ 에서 기약임을 보이자

$f(1)=1-1+1=1\neq 0$, $f(-1)=-1+1+1=1\neq 0$

$\therefore$ $f(x)$는 $\mathbb{Q}$에서 기약(따름정리 5.6.9와 정리 5.6.4)

ii) $f(x)=x^3-x+1$, $g(x)=x^2-2$라 하자.

x	x^3-x+1 x^3-2x	x^2-2 x^2+x	x
	$x+1$	$-x-2$ $-x-1$	-1
		-1	

따라서

몫			x	$x-1$
$f(x)$	1	0	1	$-x+1$
$g(x)$	0	1	$-x$	$1+x^2-x$
나머지	$f(x)$	$g(x)$	$-x+1$	2

$-1=f(x)(-x+1)+g(x)(1+x^2-x)=(x^3-x+1)(-x+1)+(x^2-2)(1+x^2-x)$이다.

그러면 $\theta^3-\theta+1=0$이므로 다음을 얻는다.

$$-1=(\theta^3-\theta+1)(-\theta+1)+(\theta^2-2)(1+\theta^2-\theta)=(\theta^2-2)(1+\theta^2-\theta)$$
$$\Rightarrow\ (\theta^2-2)^{-1}=-(1+\theta^2-\theta)=-\theta^2+\theta-1$$

(별해) $\theta^3-\theta+1=0$이다. 그러면

$$(\theta^2-2)(a\theta^2+b\theta+c)=1\quad(a,b,c\in\mathbb{Q})$$
$$\Rightarrow\ a\theta^4+b\theta^3+(-2a+c)\theta^2-2b\theta-2c=1$$
$$\Rightarrow\ a(\theta^2-\theta)+b(\theta-1)+(-2a+c)\theta^2-2b\theta-2c=1$$
$$\Rightarrow\ (-a+c)\theta^2+(-a-b)\theta-b-2c=1$$
$$\Rightarrow\ a=-b=c=-1$$
$$\therefore(\theta^2-2)^{-1}=-\theta^2+\theta-1$$

8.1.12.

(1) $F=\mathbb{Q}(\pi^3)$라 하자.

π가 초월수이므로 $\pi\notin\mathbb{Q}(\pi^3)$이다(정리 8.1.14). 따라서 $irr(\pi,\mathbb{Q}(\pi^3))=x^3-\pi^3$이다.

그러면 $\deg(x^3-\pi^3)=3$
$\mathbb{Q}(\pi^3)<\mathbb{R}$

(2) $F=\mathbb{Q}(e^{10})$라 하자

e가 초월수이므로 $e^2\notin\mathbb{Q}(e^{10})$이다(정리 8.1.14). 따라서 $irr(e^2,\mathbb{Q}(e^{10}))=x^5-e^{10}$이다.

그러면 $\deg(x^5-e^{10})=5$
$\mathbb{Q}(e^{10})<\mathbb{R}$

8.1.13 β가 F 위에서 대수적이면 β는 $F(\alpha)$ 위에서 대수적이다. 그러므로 β가 F 위에서 초월적일 때, β는 $F(\alpha)$ 위에서 대수적임을 증명하면 충분하다. β가 F 위에서 초월적이라 하자. 그러면

$$F(\beta)=\left\{\frac{g(\beta)}{f(\beta)}\,|\,f(x)\neq0,g(x)\in F[x]\right\}$$

이다. 이때 $\alpha\in E$가 $F(\beta)$ 위에서 대수적이므로 $\exists\,g(x)(\neq0)\in F(\beta)[x],\ g(\alpha)=0$이다. 즉,

$$g(x)=b_0+b_1x+b_2x^2+\cdots+b_nx^n\ \left(\forall\,b_i\in F(\beta),\ \exists\,h_i(x),\ f_i(x)\in F[x],\ b_i=\frac{f_i(\beta)}{h_i(\beta)}\right),\ \frac{f_n(\beta)}{h_n(\beta)}=b_n\neq0$$

$$0=g(\alpha)=b_0+b_1\alpha+b_2\alpha^2+\cdots+b_n\alpha^n$$
$$0=g(\alpha)=\frac{f_0(\beta)}{h_0(\beta)}+\frac{f_1(\beta)}{h_1(\beta)}\alpha+\cdots+\frac{f_n(\beta)}{h_n(\beta)}\alpha^n$$

양변에 $h_0(\beta)h_1(\beta)\cdots h_n(\beta)$를 곱하고 β에 관하여 정리하면 (참조: $(F[x])[y]\cong(F[y])[x]$)

$$0=[f_0(\beta)h_1(\beta)\cdots h_n(\beta)]+[f_1(\beta)h_0(\beta)h_2(\beta)\cdots h_n(\beta)]\alpha+\cdots+[f_n(\beta)h_0(\beta)h_1(\beta)h_2(\beta)\cdots h_{n-1}(\beta)]\alpha^n$$
$$=[a_0(\alpha)]+[a_1(\alpha)]\beta+\cdots+[a_m(\alpha)]\beta^m\ (\exists\,a_i(\alpha)\in F(\alpha))$$

이고 $[f_n(\beta)h_0(\beta)h_1(\beta)h_2(\beta)\cdots h_{n-1}(\beta)]\neq0$이고 α가 F 위에서 초월적이므로 α^n항을 가진 $a_i(\alpha)\neq0(0\leqq i\leqq m)$가 존재한다. 따라서

$$0\neq[a_0(\alpha)]+[a_1(\alpha)]x+\cdots+[a_m(\alpha)]x^m\in F(\alpha)[x]$$

이다.

$\therefore \beta$는 $F(\alpha)$위에서 대수적

8.1.14 귀류법을 이용하자. $\beta \in F(\alpha)-F$가 F 위에서 대수적이라 하자. 그러면

$$\exists\, (0 \neq) f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x],\ f(\beta) = a_n \beta^n + \cdots + a_1 \beta + a_0 = 0$$

이다. 또한 α가 F 위에서 초월적이고 $\beta \in F(\alpha)-F$이므로 $\exists\, g(x), h(x) \in F[x]$,

$$\beta = \frac{h(\alpha)}{g(\alpha)}$$

이다. $f(\beta)=0$의 양변에 $g(\alpha)^n$을 곱하면

$$(g(\alpha))^n f(\beta) = a_n (h(\alpha))^n + a_{n-1}(h(\alpha)^{n-1} g(\alpha)) + \cdots + a_0 (g(\alpha))^n = 0$$

이다. 이때 $g(x), f(x) \neq 0$이므로 $(g(x))^n f(x) \neq 0$이다. 따라서 α가 F 위에서 대수적이 되어 모순이다.
$\therefore \beta$는 F위에서 초월적이다.

8.1.15. $f(x)$를 $\alpha \in E$를 해를 가지고 $\deg(f(x))=3$이고, $\mathbb{Z}_2$ 위에서 기약다항식이라 하자.
크로네커 정리에 의해 $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2[x]/\langle f(x)\rangle$'는

$$\mathbb{Z}_2(\alpha) = \{a\alpha^2 + b\alpha + c \mid a,b,c \in \mathbb{Z}_2, f(\alpha)=0\}$$
$$= \{0,1,\alpha,\alpha+1,\alpha^2+1,\alpha^2,\alpha^2+\alpha,\alpha^2+\alpha+1 \mid f(\alpha)=0\}$$

이다. 그러므로 $\mathbb{Z}_2(\alpha)$는 원소가 8개인 표수 2인 체가 된다. 따라서 덧셈에 대하여 0이 아닌 모든 원소의 위수가 2이므로

$$(\mathbb{Z}_2(\alpha),\ +) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ +)$$

이다. 또한 유한체이므로 정리 5.5.8에 의하여 $(\mathbb{Z}_2^*(\alpha),\ \bullet\ )$는 곱셈 순환군이므로

$$(\mathbb{Z}_2^*(\alpha),\ \bullet\ ) \cong (\mathbb{Z}_7,\ +)$$

이다.

== 연습문제 (8.2) ==

8.2.1. 정리 8.1.17와 정리 8.2.3(차원정리)을 이용하자.
(1) (예 8.2.6 참조) $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})]\,[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^2-3)\deg(x^3-2) = 6$,
기저 = $\{1,\ \sqrt{3},\ \sqrt[3]{2},\ \sqrt[3]{2^2},\ \ \sqrt{3}\sqrt[3]{2},\ \ \sqrt{3}\sqrt[3]{2^2}\}$
(2) (예 8.2.7 참조) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 8$,
기저 = $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$
(3) (예 8.2.6 참조) $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})]\,[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^2-2)\deg(x^3-2) = 6$,
기저 = $\{1,\ \sqrt{2},\ \sqrt[3]{2},\ \sqrt[3]{2^2},\ \sqrt{2}\sqrt[3]{2},\ \sqrt{2}\sqrt[3]{2^2}\}$
(4) $[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2$, 기저 = $\{1, \sqrt{6}\}$
(5) $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$이므로 다음이 성립한다. (연습문제 12번과 예 8.2.8, 정리 8.1.17 참조)
$[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\sqrt{3})]\,[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \deg(x^2-2)\deg(x^2-3) = 4$
기저 = $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$,
(6) $\alpha = \sqrt{2} + \sqrt[3]{4}$라 하자. 그러면

$$4 = (\sqrt[3]{4})^3 = (\alpha - \sqrt{2})^3 = \alpha^3 - 3\alpha^2\sqrt{2} + 6\alpha - 2\sqrt{2}$$

따라서

$$\sqrt{2}(3\alpha^2+2) = \alpha^3 + 6\alpha - 4$$

에서

$$2(3\alpha^2+2)^2=(\alpha^3+6\alpha-4)^2$$

이고 이식을 전개하면 α는 유리수 계수 6차 기약다항식(판정은 까다로움) $2(3x^2+2)^2=(x^3+6x-4)^2$의 근이다. 그러므로 정리 8.1.17에 의하여

$$[\mathbb{Q}(\sqrt{2}+\sqrt[3]{4}):\mathbb{Q}]=\deg(\sqrt{2}+\sqrt[3]{4},\mathbb{Q})=6$$

$\alpha=\sqrt{2}+\sqrt[3]{4}$라 하자. 기저 = $\{1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^5\}$

(별해) $\mathbb{Q}(\sqrt{2}+\sqrt[3]{4})=\mathbb{Q}(\sqrt{2},\sqrt[3]{4})$이므로 다음이 성립한다. (예 8.2.6 참조)

$$[\mathbb{Q}(\sqrt{2}+\sqrt[3]{4}):\mathbb{Q}]=6$$

기저 = $\{1,\ \sqrt{2},\ \sqrt[3]{4},\ \sqrt[3]{4^2},\ \sqrt{2}\sqrt[3]{4},\ \sqrt{2}\sqrt[3]{4^2}\}$ 또는 $\{1,\ \sqrt{2},\ \sqrt[3]{2},\ \sqrt[3]{2^2},\ \sqrt{2}\sqrt[3]{2},\ \sqrt{2}\sqrt[3]{2^2}\}$

(7) $[\mathbb{Q}(\sqrt{2},\sqrt{6})=\mathbb{Q}(\sqrt{2},\sqrt{2}\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$이므로 다음이 성립한다. (예 8.2.8 참조)

$$[\mathbb{Q}(\sqrt{2},\sqrt{6}):\mathbb{Q}(\sqrt{3})]=2,$$

기저 = $\{1,\sqrt{2}\}$

(8) $\mathbb{Q}(\sqrt{2},\sqrt{6}+\sqrt{10})=\mathbb{Q}(\sqrt{2},\sqrt{2}(\sqrt{3}+\sqrt{5}))=\mathbb{Q}(\sqrt{2},\sqrt{3}+\sqrt{5})$이므로 다음이 성립한다.

$$[\mathbb{Q}(\sqrt{2},\sqrt{6}+\sqrt{10}):\mathbb{Q}(\sqrt{3}+\sqrt{5})]=2,$$

기저 = $\{1,\sqrt{2}\}$

8.2.2. (1) $\mathbb{Q}(\sqrt[3]{2})$-기저 $\{1,\sqrt{5}\}$, $\mathbb{Q}(\sqrt{5})$-기저 $\{1,\sqrt[3]{2},\sqrt[3]{2^2}\}$

(2) $\mathbb{Q}$-기저 = $\{1,\sqrt{5},\sqrt[3]{2},\sqrt[3]{2^2},\sqrt{5}\sqrt[3]{2},\sqrt{5}\sqrt[3]{2^2}\}$,

$$[\mathbb{Q}(\sqrt{5},\sqrt[3]{2}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{5},\sqrt[3]{2}):\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=\deg(x^2-5)\deg(x^3-2)=6$$

8.2.3.

(1) $i\sqrt{3}\notin\mathbb{Q}(\sqrt[3]{2})$이므로 x^2+3은 $\mathbb{Q}(\sqrt[3]{2})$ 위에서 기약이다. $\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$의 $\mathbb{Q}(\sqrt[3]{2})$ 위에서 기저는 $\{1,i\sqrt{3}\}$이다.

x^3-2가 Eisenstein 판정에 의하여 $\mathbb{Q}$ 위에서 기약이므로 $\mathbb{Q}(\sqrt[3]{2})$의 $\mathbb{Q}$위에서 기저는 $\{1,\sqrt[3]{2},(\sqrt[3]{2})^2\}$이다.

$$[\mathbb{Q}(\sqrt[3]{2},i\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2},i\sqrt{3}):\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=\deg(x^2+3)\deg(x^3-2)=6$$

$$\therefore[\mathbb{Q}(\sqrt[3]{2},i\sqrt{3}):\mathbb{Q}]=6$$

(2) $[\mathbb{Q}(\sqrt[3]{2},i\sqrt{3}):\mathbb{Q}(\sqrt[3]{2})]=2$ $(\because(1))$

(3) $[\mathbb{Q}(\sqrt[3]{2},i,\sqrt{3}):\mathbb{Q}]$

$$=[\mathbb{Q}(\sqrt[3]{2},i,\sqrt{3}):\mathbb{Q}(\sqrt[3]{2},\sqrt{3})][\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$$
$$=\deg(x^2+1)\deg(x^2-3)\deg(x^3-2)=2\cdot2\cdot3=12$$

(4) $[\mathbb{Q}(\sqrt[3]{2},\sqrt{2},i):\mathbb{Q}]$

$$=[\mathbb{Q}(\sqrt[3]{2},\sqrt{2},i):\mathbb{Q}(\sqrt[3]{2},\sqrt{2})][\mathbb{Q}(\sqrt[3]{2},\sqrt{2}):\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$$
$$\equiv\deg(x^2+1)\deg(x^2-2)\deg(x^3-2)=2\cdot2\cdot3=12$$

8.2.4.

풀이)

(1) $\mathbb{Z}[\sqrt{12}]=\{a+b\sqrt{12}\,|\,a,b\in\mathbb{Z}\}=\{a+2b\sqrt{3}\,|\,a,b\in\mathbb{Z}\}\subset\mathbb{Z}[\sqrt{3}]=\{a+b\sqrt{3}\,|\,a,b\in\mathbb{Z}\}$이다.

그리고 $\sqrt{3}\notin\mathbb{Z}[\sqrt{12}]=\mathbb{Z}[2\sqrt{3}]$이므로 $\mathbb{Z}[\sqrt{12}]\subsetneq\mathbb{Z}[\sqrt{3}]$이다.

(2) $\mathbb{Q}(\sqrt{12})$와 $\mathbb{Q}(\sqrt{3})$의 각각의 기저는 $1,\sqrt{12}$와 $1,\sqrt{3}$인데 $\sqrt{12}$와 $\sqrt{3}$이 각각에 들어감을 보이면 된다.

먼저 $\sqrt{12}=\sqrt{4\times3}=2\sqrt{3}$이므로 $\sqrt{12}$는 $\sqrt{3}$의 1차결합이다. 따라서 $\sqrt{12}\in\mathbb{Q}(\sqrt{3})$이 성립한다.

다음으로 $\sqrt{3}=\frac{1}{2}\times2\sqrt{3}=\frac{1}{2}\sqrt{12}$이므로 $\sqrt{3}$역시 $\sqrt{12}$의 1차결합이므로 $\sqrt{3}\in\mathbb{Q}(\sqrt{12})$가 성립한다.

따라서 $\mathbb{Q}(\sqrt{12})=\mathbb{Q}(\sqrt{3})$이다.

(3) $\sqrt{6} = \sqrt{2}\sqrt{3} \in \mathbb{Q}(\sqrt{2})$라 하자. 그럼 $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$이다. 이것은 예 8.2.7에서 $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$임을 보였으므로 모순이다. 그러므로 $\sqrt{6} \notin \mathbb{Q}(\sqrt{2})$이다.

(별해) $\sqrt{6} \in \mathbb{Q}(\sqrt{2})$라 하자. 그러면 $\sqrt{2}+\sqrt{6} \in \sqrt{\mathbb{Q}}(\sqrt{2})$이다.

$$irr(\sqrt{2}+\sqrt{6}, \mathbb{Q}) = x^4 - 16x^2 + 16$$

이다. 그러면

$$2 = \deg(x^2-2) = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}(\sqrt{2}+\sqrt{6})][\mathbb{Q}(\sqrt{2}+\sqrt{6}) : \mathbb{Q}] \geqq \deg(x^4-16x^2+16) = 4$$

이 되어 모순이다. 따라서 $\sqrt{6} \notin \mathbb{Q}(\sqrt{2})$이다.

(4) $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$, $\mathbb{Q}(\sqrt{6}) = \{a'+b'\sqrt{6} \mid a',b' \in \mathbb{Q}\}$.

임의의 원소 $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{6})$에 대하여 유리수 $a', b' \in \mathbb{Q}$가 존재해서

$$a+b\sqrt{2} = a'+b'\sqrt{6}$$

이다. 그러면

$$a-a' = -b\sqrt{2}+b'\sqrt{6}$$
$$(a-a')^2 = 2b^2 - 4bb'\sqrt{3} + 6b'^2$$

에서 $\sqrt{3}$이 무리수이므로 $bb'=0$이어야 한다. $b=0$이거나 $b'=0$이다. 이때 $b'=0$이면 분명히 $b=0$이다. 따라서 $a+b\sqrt{2}=a \in \mathbb{Q}$이므로 $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}$이다. 그러므로 $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{6}) = \mathbb{Q}$이다.

(5) $\mathbb{Q}(\sqrt[4]{8})$의 기저는

$$1,\ \sqrt[4]{8} = \sqrt[4]{2^3},\ \sqrt[4]{2^6} = 2\sqrt[4]{2^2},\ \sqrt[4]{2^9} = 4\sqrt[4]{2}$$

이고, $\mathbb{Q}(\sqrt[4]{2})$의 기저는

$$1,\ \sqrt[4]{2},\ \sqrt[4]{2^2},\ \sqrt[4]{2^3}$$

이다. 각각의 기저들이 다른 기저들의 일차결합으로 표현 가능하므로, 두 집합은 서로 같다.

(6) $\mathbb{Q}(\sqrt[4]{8})$의 기저는

$$1,\ i\sqrt[4]{8} = i\sqrt[4]{2^3},\ \sqrt[4]{2^6} = 2\sqrt[4]{2^2},\ i\sqrt[4]{2^9} = 4i\sqrt[4]{2}$$

이고, $\mathbb{Q}(\sqrt[4]{2})$의 기저는

$$1,\ i\sqrt[4]{2},\ \sqrt[4]{2^2},\ i\sqrt[4]{2^3}$$

이다. 각각의 기저들이 다른 기저들의 일차결합으로 표현 가능하므로, 두 집합은 서로 같다.

따라서 주어진 집합 $\mathbb{Q}(i\sqrt[4]{8}) = \mathbb{Q}(i\sqrt[4]{2})$이다.

8.2.5. $irr(a+bi, \mathbb{R}) = x^2 - 2ax + a^2 + b^2$이므로 $1, a+bi$가 $\mathbb{R}$-기저이다. 그러면 $\mathbb{R}(a+bi) = \{x+y(a+bi) \mid x, y \in \mathbb{R}\}$이다. 먼저$\mathbb{C} \subset \mathbb{R}(a+bi)$임을 보이자. 임의의 $c+di \in \mathbb{C}$에 대하여

$$c+di = c - \frac{ad}{b} + \frac{d}{b}(a+bi) \in \mathbb{R}(a+bi)$$

이다. 따라서 $\mathbb{C} \subset \mathbb{R}(a+bi)$이다. $\mathbb{R}(a+bi) \subset \mathbb{C}$은 분명히 성립하므로 $\mathbb{R}(a+bi) = \mathbb{C}$이다.

8.2.6. (1) $x^2 - 5 = (x-\sqrt{5})(x+\sqrt{5})$이므로 $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$임을 보이면 된다.

$\sqrt{5} \in \mathbb{Q}(\sqrt{3})$이라면 $\sqrt{3}+\sqrt{5} \in \mathbb{Q}(\sqrt{3})$이므로 $\mathbb{Q} < \mathbb{Q}(\sqrt{3}+\sqrt{5}) < \mathbb{Q}(\sqrt{3})$이다.

그런데 $irr(\sqrt{3}+\sqrt{5}, \mathbb{Q}) = x^4 - 16x + 4$이고, $irr(\sqrt{3}, \mathbb{Q}) = x^2 - 3$이므로

$$2 = \deg(\sqrt{3}, \mathbb{Q}) = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}(\sqrt{3}+\sqrt{5})][\mathbb{Q}(\sqrt{3}+\sqrt{5}) : \mathbb{Q}] \geqq \deg(\sqrt{3}+\sqrt{5}, \mathbb{Q}) = 4$$

이므로 모순이다. 따라서 $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$이다. 인수정리에 의하여 x^2-5는 $\mathbb{Q}(\sqrt{3})$ 위에서 기약이다.

(2) $x^2 - 3 = (x-\sqrt{3})(x+\sqrt{3})$이므로 $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2})$임을 보이면 된다.

$\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2})$이라면 $irr(\sqrt{3}, \mathbb{Q}) = x^2 - 3$이므로

$3 = \deg(\sqrt[3]{2}, \mathbb{Q}) = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})]$

이므로 2|3이 되어 모순이다. 따라서 $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2})$이다. $x^2 - 3$는 $\mathbb{Q}(\sqrt[3]{2})$ 위에서 기약이다.

8.2.7. (1) $p = 2$에 대하여 Eisentein 기약판정에 의해 $f(x)$는 $\mathbb{Q}[x]$에서 기약이다.

(2) $f(-1) = -1 - 4 - 2 + 2 = -5 < 0$
$f(0) = 2 > 0$
$f(2) = 32 - 64 + 4 + 2 = -26 < 0$
$f(4) = 4^5 - 4^5 + 8 + 2 = 10 > 0$

이므로 중간값의 정리에 의하여 적어도 3개의 실근을 갖는다. 또한

$f'(x) = 5x^4 - 16x^3 + 2$
$f''(x) = 20x^3 - 48x^2 = x^2(20x - 48)$

이므로 $x = 0$(중근), $x = \frac{12}{5}$에서 변곡점 2개를 갖는다. 따라서 실근이 4개 이상이려면 변곡점이 3개 이상이어야 하므로 3개의 실근과 2개의 허근을 갖는다.

(3) $\mathbb{Q}$ 위의 기약다항식 $f(x)$의 차수는 5이므로 $[\mathbb{Q}(r_1) : \mathbb{Q}] = \deg(r_1, \mathbb{Q}) = \deg(f(x)) = 5$이다.

8.2.8. (1) $\alpha = \frac{-1 + \sqrt{3}i}{2}$, $\alpha^2 = \frac{-1 - \sqrt{3}i}{2}$, $\alpha^3 = 1$이다. 또한 이들은 $x^3 - 1 = (x-1)(x^2 + x + 1) = 0$의 근이다. 이때 α, α^2은 $x^2 + x + 1$의 근이고 α, $\alpha^2 \notin \mathbb{Q}$이므로 $irr(\alpha, \mathbb{Q}) = irr(\alpha^2, \mathbb{Q}) = x^2 + x + 1$이다.

(별해) $x = \frac{-1 + i\sqrt{3}}{2}$라 하면 $2x + 1 = +i\sqrt{3}$
$(2x+1)^2 = (i\sqrt{3})^2$
$4x^2 + 4x + 1 = -3$
$x^2 + x + 1 = 0$

이다. 또한 α, $\alpha^2 \notin \mathbb{Q}$이므로 $irr(\alpha, \mathbb{Q}) = x^2 + x + 1$이다. 또한 $\alpha^2 = \frac{-1 - \sqrt{3}i}{2}$ 이므로 $x = \frac{-1 - \sqrt{3}i}{2}$라 하면

$2x + 1 = -\sqrt{3}i$
$(2x+1)^2 = (-\sqrt{3}i)^2$
$4x^2 + 4x + 1 = -3$
$x^2 + x + 1 = 0$

이다. 또한 α, $\alpha^2 \notin \mathbb{Q}$이므로 $irr(\alpha^2, \mathbb{Q}) = x^2 + x + 1$이다. 따라서 $irr(\alpha, \mathbb{Q}) = irr(\alpha^2, \mathbb{Q}) = x^2 + x + 1$이다.

이제 $\mathbb{Q}(\alpha) = \mathbb{Q}(i\sqrt{3})$임을 보이자.

$$\mathbb{Q}\left(\frac{-1 + i\sqrt{3}}{2}\right) = \left\{a + \frac{-1 + i\sqrt{3}}{2}b \mid a, b \in \mathbb{Q}\right\} = \{c + di\sqrt{3} \mid c, d \in \mathbb{Q}\} = \mathbb{Q}(i\sqrt{3})$$

$\mathbb{Q}(\alpha) = \mathbb{Q}(i\sqrt{3})$와 같은 방법으로 $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha)$임을 보일 수 있다.

(별해) $\mathbb{Q}(i\sqrt{3}) \supset \mathbb{Q}\left(\frac{-1 + i\sqrt{3}}{2}\right)$은 분명히 성립한다. 다음에

$$i\sqrt{3} = \left(\frac{-1 + i\sqrt{3}}{2}\right) \cdot 2 + 1 \in \mathbb{Q}\left(\frac{-1 + i\sqrt{3}}{2}\right)$$

이므로 $\mathbb{Q}(i\sqrt{3}) \subset \mathbb{Q}\left(\frac{-1 + i\sqrt{3}}{2}\right)$이다. 따라서 $\mathbb{Q}(i\sqrt{3}) = \mathbb{Q}\left(\frac{-1 + i\sqrt{3}}{2}\right)$이다.

(2) α, α^2은 $x^2 + x + 1$의 근이고 α, $\alpha^2 \notin \mathbb{R}$이므로 $irr(\alpha, \mathbb{R}) = x^2 + x + 1$이다.

(별해) $x=\dfrac{-1+i\sqrt{3}}{2}$

$2x+1=+i\sqrt{3}$

$(2x+1)^2=(i\sqrt{3})^2$

$4x^2+4x+1=-3$

$x^2+x+1=0$

$\therefore irr(\alpha,\mathbb{R})=x^2+x+1$

$$\mathbb{R}(\alpha)=\mathbb{R}\left(\frac{-1+i\sqrt{3}}{2}\right)=\mathbb{R}(i)=\mathbb{C}$$

8.2.9(1) $\alpha^p=1$(즉, α는 $x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+x+1)$의 근)이고
$\alpha\neq 1$이므로 α는 기약다항식 $x^{p-1}+x^{p-2}+\cdots+x+1$(따름정리 5.6.17)의 근이다.

$irr(\alpha,\mathbb{Q})=x^{p-1}+x^{p-2}+\cdots+x+1$

$[\mathbb{Q}(\alpha):\mathbb{Q}]=p-1$

(2) $\alpha^n(1\leqq n\leqq p-1)$은 $(\alpha^n)^p=(\alpha^p)^n=1$이고 $\alpha^n\neq 1$이므로 기약다항식 $x^{p-1}+x^{p-2}+\cdots+x+1$의 근이다. 그러므로

$$irr(\alpha^n,\mathbb{Q})=x^{p-1}+x^{p-2}+\cdots+x+1$$

이다. 또한 $Q(\alpha^n)\subset Q(\alpha)$이다. 그러면

$$p-1=[\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha^n)][\mathbb{Q}(\alpha^n):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha^n)](p-1)$$

이다. 따라서 $[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha^n)]=1$이고 $\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha^n)$이다.

(별해) $\gcd(n,p)=1$이므로 적당한 정수 x,y에 대하여 $nx+py=1$이다.

$$\alpha=\alpha^{nx+py}=\alpha^{nx}\alpha^{py}=(\alpha^n)^x\in\mathbb{Q}(\alpha^n)$$

이므로 $\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha^n)$이다.

8.2.10 $\mathbb{Q}(\sqrt{p})=\{a+b\sqrt{p}\,|\,a,b\in\mathbb{Q}\}$, $\mathbb{Q}(\sqrt{q})=\{a'+b'\sqrt{q}\,|\,a',b'\in\mathbb{Q}\}$.
임의의 원소 $a+b\sqrt{p}\in\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\sqrt{q})$에 대하여 유리수 $a',b'\in\mathbb{Q}$가 존재해서

$$a+b\sqrt{p}=a'+b'\sqrt{q}$$

이다. 그러면

$$a-a'=-b\sqrt{p}+b'\sqrt{q}$$
$$(a-a')^2=pb^2-2bb'\sqrt{pq}+qb'^2$$

에서 p,q가 서로 다른 소수이므로 $\sqrt{pq}$가 무리수가 되어 $bb'=0$이어야 한다. $b=0$이거나 $b'=0$이다. 이때 $b'=0$이면 분명히 $b=0$이다. 따라서 $a+b\sqrt{p}=a\in\mathbb{Q}$이므로 $\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\sqrt{q})\subset\mathbb{Q}$이다. 그러므로 $\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\sqrt{q})=\mathbb{Q}$이다.

8.2.11 (1) $\mathbb{Q}(\sqrt{3}+\sqrt{7})\subset\mathbb{Q}(\sqrt{3},\sqrt{7})$은 분명히 성립한다. 다음에 분모 유리화하면

$$\frac{\sqrt{7}-\sqrt{3}}{4}=\frac{1}{\sqrt{3}+\sqrt{7}}=(\sqrt{3}+\sqrt{7})^{-1}\in\mathbb{Q}(\sqrt{3}+\sqrt{7})$$

이므로 $\sqrt{7}-\sqrt{3}=\dfrac{\sqrt{7}-\sqrt{3}}{4}\cdot 4\in\mathbb{Q}(\sqrt{3}+\sqrt{7})$이다. 따라서

$$\sqrt{3}=\frac{(\sqrt{7}+\sqrt{3})-(\sqrt{7}-\sqrt{3})}{2}\in\mathbb{Q}(\sqrt{3}+\sqrt{7})$$
$$\sqrt{7}=\frac{(\sqrt{7}+\sqrt{3})+(\sqrt{7}-\sqrt{3})}{2}\in\mathbb{Q}(\sqrt{3}+\sqrt{7})$$

이므로 $\mathbb{Q}(\sqrt{3}+\sqrt{7})\supset\mathbb{Q}(\sqrt{3},\sqrt{7})$, 즉, $\mathbb{Q}(\sqrt{3}+\sqrt{7})=\mathbb{Q}(\sqrt{3},\sqrt{7})$이다.

(별해) $\mathbb{Q}(\sqrt{3}+\sqrt{7})\subset\mathbb{Q}(\sqrt{3},\sqrt{7})$은 분명히 성립한다. 또한

$$irr(\sqrt{3}+\sqrt{7},\mathbb{Q})=x^4-20x^2+16$$

이고

$$[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=\deg(x^2-7)\deg(x^2-3)=4$$
$$[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}(\sqrt{3}+\sqrt{7})][\mathbb{Q}(\sqrt{3}+\sqrt{7}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}(\sqrt{3}+\sqrt{7})]\cdot 4$$

이므로

$$[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}(\sqrt{3}+\sqrt{7})]=1$$

즉, $\mathbb{Q}(\sqrt{3},\sqrt{7})=\mathbb{Q}(\sqrt{3}+\sqrt{7})$이다.

(2) (1)과 같은 방법으로 $\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{3}-\sqrt{2})$을 증명하면 된다.

8.2.12 먼저 $a=b$이면 성립한다. 따라서 $a\neq b$인 경우 증명하자.

$\mathbb{Q}(\sqrt{a}+\sqrt{b})\subset\mathbb{Q}(\sqrt{a},\sqrt{b})$은 분명히 성립한다. 다음에 분모 유리화하면

$$\frac{\sqrt{a}-\sqrt{b}}{a-b}=(\sqrt{a}+\sqrt{b})^{-1}\in\mathbb{Q}(\sqrt{a}+\sqrt{b})$$

이므로 $\sqrt{a}-\sqrt{b}=\frac{\sqrt{a}-\sqrt{b}}{a-b}\cdot(a-b)\in\mathbb{Q}(\sqrt{a}+\sqrt{b})$이다. 따라서

$$\sqrt{a}=\frac{(\sqrt{a}+\sqrt{b})+(\sqrt{a}-\sqrt{b})}{2}\in\mathbb{Q}(\sqrt{a}+\sqrt{b})$$
$$\sqrt{b}=\frac{(\sqrt{a}+\sqrt{b})-(\sqrt{a}-\sqrt{b})}{2}\in\mathbb{Q}(\sqrt{a}+\sqrt{b})$$

이므로 $\mathbb{Q}(\sqrt{a}+\sqrt{b})\supset\mathbb{Q}(\sqrt{a},\sqrt{b})$, 즉, $\mathbb{Q}(\sqrt{a}+\sqrt{b})=\mathbb{Q}(\sqrt{a},\sqrt{b})$이다.

8.2.13. (참조: 생성원의 사칙연산으로 대부분 구해진다.)

(1) $\mathbb{Q}(\sqrt{2},i\sqrt{3})=\mathbb{Q}(\sqrt{2}+i\sqrt{3})$을 보이면 된다.

$\mathbb{Q}(\sqrt{2}+i\sqrt{3})\subset\mathbb{Q}(\sqrt{2},i\sqrt{3})$은 분명히 성립한다. 다음에 분모 실수화하면

$$\frac{\sqrt{2}-i\sqrt{3}}{5}=(\sqrt{2}+i\sqrt{3})^{-1}\in\mathbb{Q}(\sqrt{2}i+\sqrt{3})$$

이므로 $\sqrt{2}-i\sqrt{3}=\frac{\sqrt{2}-i\sqrt{3}}{5}\cdot 5\in\mathbb{Q}(\sqrt{2}+i\sqrt{3})$이다. 따라서

$$\sqrt{2}=\frac{(\sqrt{2}i+\sqrt{3})+(\sqrt{2}-i\sqrt{3})}{2}\in\mathbb{Q}(\sqrt{2}+i\sqrt{3})$$
$$i\sqrt{3}=\frac{(\sqrt{2}i+\sqrt{3})-(\sqrt{2}-i\sqrt{3})}{2}\in\mathbb{Q}(\sqrt{2}+i\sqrt{3})$$

이므로 $\mathbb{Q}(\sqrt{2},i\sqrt{3})\subset\mathbb{Q}(\sqrt{2}+i\sqrt{3})$, 즉, $\mathbb{Q}(\sqrt{2},i\sqrt{3})=\mathbb{Q}(\sqrt{2}+i\sqrt{3})$이다.

그러므로 $c=\sqrt{2}+i\sqrt{3}$를 택하면 된다.

(2) $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})=\mathbb{Q}(\sqrt{2}\sqrt[3]{2})$을 보이자. 먼저 $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})\supset\mathbb{Q}(\sqrt{2}\sqrt[3]{2})$은 분명히 성립한다. 다음에

$$\sqrt{2}=\frac{(\sqrt{2}\sqrt[3]{2})^3}{4}\in\mathbb{Q}(\sqrt{2}\sqrt[3]{2})$$
$$\sqrt[3]{2}=\frac{(\sqrt{2}\sqrt[3]{2})^4}{8}\in\mathbb{Q}(\sqrt{2}\sqrt[3]{2})$$

이므로 $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})\subset\mathbb{Q}(\sqrt{2}\sqrt[3]{2})$이다. 따라서 $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})=\mathbb{Q}(\sqrt{2}\sqrt[3]{2})$이다. $c=\sqrt{2}\sqrt[3]{2}$이다.

(별해1) $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})=\mathbb{Q}(\sqrt[6]{2})$을 보이자. 먼저 $\sqrt[6]{2}=\frac{\sqrt{2}}{\sqrt[3]{2}}\in\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$이므로 $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})\supset\mathbb{Q}(\sqrt[6]{2})$은 분명히 성립한다. 다음에

$$\sqrt{2}=(\sqrt[6]{2})^3\in\mathbb{Q}(\sqrt[6]{2})$$
$$\sqrt[3]{2}=(\sqrt[6]{2})^2\in\mathbb{Q}(\sqrt[6]{2})$$

이므로 $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})\subset\mathbb{Q}(\sqrt[6]{2})$이다. 따라서 $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})=\mathbb{Q}(\sqrt[6]{2})$이다. $c=\sqrt[6]{2}$이다.

(별해2) 먼저 $\mathbb{Q}(\sqrt{2},\sqrt[3]{2}) \supset \mathbb{Q}(\sqrt[6]{2})$은 분명히 성립한다. 다음에 $irr(\sqrt[6]{2},\mathbb{Q}) = x^6-2$(아이젠슈타인 판정)이므로

$$[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = \deg(x^3-2)\deg(x^2-2) = 6$$
$$[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}(\sqrt[6]{2})]\,[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}(\sqrt[6]{2})]\cdot 6$$

이므로

$$[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}(\sqrt[6]{2})] = 1$$

즉, $\mathbb{Q}(\sqrt{2},\sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$이다. 그러므로 $c = \sqrt[6]{2}$이다.

(3) (2)번과 같은 방법으로 구할 수 있다. $\mathbb{Q}(\sqrt{3},\sqrt[3]{5}) = \mathbb{Q}(\sqrt{3}\,\sqrt[3]{5})$이다. 그러므로 $c = \sqrt{3}\,\sqrt[3]{5}$ 이다.

(4) (2)번과 같은 방법으로 구할 수 있다. $\mathbb{Q}(\sqrt[3]{2},i) = \mathbb{Q}(\sqrt[3]{2}\,i)$이다. 그러므로 $c = \sqrt[3]{2}\,i$이다.

8.2.14 (1) $p(x)$가 K안에서 근 $\alpha \in K$를 갖는다고 하자. 그러면 α는 F 위에서 대수적이고 $p(x)$가 기약이므로 가정에 의하여

$$r = [F(\alpha):F] = \deg(\alpha,F) = \deg(p(x)) \geqq 2$$

이고 $\gcd(r,[K:F]) = 1$이다. 그러면 $F(\alpha) < K$이고

$$[K:F] = [K:F(\alpha)][F(\alpha):F] = [K:F(\alpha)]r$$

이므로 $r|\gcd(r,[K:F]) = 1$이고 $r = 1$이 되어 모순이다. 따라서 $p(x)$가 K안에서 근을 갖지 않는다.

(2) $p(x)$의 한 근을 $\alpha \in \overline{F}$라 하자. 그러면 $p(\alpha) = 0$이고 $p(x) \in F[x] \subset K[x]$이다. 따라서 $irr(\alpha,K)(\alpha) = 0$이므로

$$irr(\alpha,K)|p(x)\text{이고 } [K(\alpha):K] = \deg(\alpha,K) \leqq \deg(p(x))$$

이다. 한편

$$[K(\alpha):F] = [K(\alpha):F(\alpha)][F(\alpha):F] = [K:F(\alpha)]\deg(p(x))$$
$$[K(\alpha):F] = [K(\alpha):K][K:F]$$

이므로

$$[K:F(\alpha)]\deg(p(x)) = [K(\alpha):K][K:F]$$

이다. $\gcd(\deg(p(x)),[K:F]) = 1$이므로

$$\deg(p(x))|[K(\alpha):K] \Rightarrow \deg(p(x)) \leqq [K(\alpha):K]$$

이어야 한다. 그러므로

$$\deg(\alpha,K) = [K(\alpha):K] = \deg(p(x)) = \deg(\alpha,F) = [F(\alpha):F]$$

이다. 따라서 $p(x)$는 K 위에서 기약이다(정리 8.1.15).

8.2.15 (1) E가 F의 유한확대체이므로 E는 F 위에서 대수적확대체이다. 또한 b가 E 위에서 대수적이므로 $F(\alpha)$와 $E(\alpha)$도 F 위에서 대수적확대체이다. $p(x) = irr(b,F)$라 하면 $p(x) \in F[x] \subset E[x]$이고 $p(b) = 0$이다. 그러므로 정리 8.1.15에 의하여

$$irr(b,E)|p(x)$$

이다. 그러므로 $\deg(b,E) \leq \deg(p(x))$이고

$$[E(b):E] = \deg(b,E) \leq \deg(p(x)) = \deg(b,F) = [F(b):F]$$

이다.

(2) $[E(b):F] = [E(b):E][E:F]$
$[E(b):F] = [E(b):F(b)][F(b):F]$

이므로 $[E(b):E][E:F] = [E(b):F(b)][F(b):F]$이다. (1)에 의하여 $[E(b):E] \leqq [F(b):F]$이므로 $[E(b):F(b)] \leq [E:F]$이다.

(3) $[E(b):F] = [E(b):F(b)][F(b):F]$이므로 $[F(b):F]|[E(b):F]$ 이다.

8.2.16

(1) 체의 차원정리에 의해 $[K:F]=[K:L][L:F]$ 인데, $[K:F]$는 소수이므로 $[K:L]=1$ 이거나 $[L:F]=1$ 이다. 따라서 $K=L$ 이거나 $L=F$ 이다.

(2) $F(u)<K$이므로 체의 차원정리에 의해 $[K:F]=[K:F(u)][F(u):F]$이다. 그리고 가정에 의하여 $u\in K-F$이므로 $\deg(u,F)\geq 2$이다. 이때 $[K:F]$가 소수이므로 $[K:F(u)]=1$이거나 $[F(u):F]=1$이다. 그런데 $[F(u):F]\geq 2$이므로 $[K:F(u)]=1$이다. 따라서 $K=F(u)$ 이다.

(3) (2)에 의하여 $[K:F(u)]=1$이므로

$$[K:F]=[K:F(u)]\left[F(u):F(u^n)\right]\left[F(u^n):F\right]=\left[F(u):F(u^n)\right]\left[F(u^n):F\right]$$

이다. $[K:F]$가 소수이므로 $\left[F(u):F(u^n)\right]=1$이거나 $\left[F(u^n):F\right]=1$이다. 따라서 $F(u)=F(u^n)$ 또는 $u^n\in F$이다.

8.2.17

(1) $F(au+b)\subset F(u)$임은 당연하므로 $F(u)\subset F(au+b)$임을 보이자.

F 가 체이므로 $a^{-1},-b\in F\subset F(au+b)$이다.

그러므로 $u=a^{-1}\{(au+b)-b\}\in F(au+b)$

따라서 $F(u)\subset F(au+b)$이고 $F(au+b)=F(u)$이다.

(2) $u\in F(u)$이고 $F(u)$는 체이므로 $u^{-1}\in F(u)$이다. 그러므로 $F(u^{-1})\subset F(u)$이다.

또한 $u^{-1}\in F(u^{-1})$는 체이므로 $u=(u^{-1})^{-1}\in F(u^{-1})$이다. 그러므로 $F(u)\subset F(u^{-1})$이고 $F(u)=F(u^{-1})$이다.

8.2.18

(1) $F(u^2)\neq F(u)$일 때, $[F(u):F(u^2)]=2$임을 보이자. 분명히 $u\notin F(u^2)$이다.

u가 F 위에서 대수적이므로 $\deg(u,F)=n\geqq 2$라 하면, $F(u)$의 F 위에서 기저는 $1,u,u^2,\cdots,u^{n-1}$이다.

$$F(u)=\left\{a_0+a_1u+\cdots+a_{n-1}u^{n-1}|a_i\in F\right\}$$

의 임의의 원소 $a_0+a_1u+\cdots+a_{2n}u^{2n}\in F(u)$(필요하면 계수 0을 추가하여 $2n+1$개의 항으로 함)에 대하여

$$b_0=a_0+a_2u^2+\cdots+a_{2n}u^{2n},\ b_1=a_1+a_3u^2+\cdots+a_{2n-1}u^{2n-2}\in F(u^2)$$

이라 하면

$$a_0+a_1u+\cdots+a_{2n}u^{2n}=(a_0+a_2u^2+\cdots+a_{2n}u^{2n})+u(a_1+a_3u^2+\cdots+a_{2n-2}u^{2n-2})=b_0+b_1u$$

이므로 $F(u)$의 $F(u^2)$ 위에서 기저는 $1,u$이다. 따라서 $[F(u^2):F(u)]=2$이다.

(별해) 체 K는 F의 유한확대체이므로 원소 $u\in K$에 대하여 $F(u)$는 F의 유한확대체이고 $u^2\in F(u)$이므로 $F(u^2)\subset F(u)$이다.

먼저 $u\in F(u^2)$이면 $F(u)\subset F(u^2)$이므로 $F(u)=F(u^2)$이다.

다음에 $u\notin F(u^2)$이면 u는 체 $F(u^2)$ 위의 다항식

$$p(x)=x^2-u^2\in F(u^2)[x]$$

의 근이고 $F(u^2)$ 위의 기약 다항식이다. 따라서

$$p(x)=irr(u,F(u^2))$$

이다. 그러므로 $[F(u):F(u^2)]=\deg(p(x))=2$이다.

(2) $[F(u):F]=[F(u):F(u^2)][F(u^2):F]$이므로 $[F(u):F]$가 홀수이면 $[F(u):F(u^2)]$가 홀수이다. 따라서 (1)에 의하여 $[F(u):F(u^2)]=1$이다. 그러므로 $F(u)=F(u^2)$이다

(3) 1) $F(u^2)=F(u)$인 예

$u=\sqrt[3]{2}$이라 하면, $u^2=\sqrt[3]{4}$이고 다음이 성립한다.

$$irr(u,\mathbb{Q})=x^3-2,\quad irr(u^2,\mathbb{Q})=x^3-4$$
$$[\mathbb{Q}(u):\mathbb{Q}]=[\mathbb{Q}(u^2):\mathbb{Q}]=3,$$
$$\mathbb{Q}(u^2)=\mathbb{Q}(u)$$

다음에 홀수인 소수 p에 대하여 $u=e^{\frac{2\pi}{p}i}=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$이라 하면 다음이 성립한다(연습문제 8.2.9 풀이 참조).

$$irr(u,\mathbb{Q})=irr(u^2,\mathbb{Q})=\frac{x^p-1}{x-1}$$
$$[\mathbb{Q}(u):\mathbb{Q}]=[\mathbb{Q}(u^2):\mathbb{Q}]=p-1,$$
$$\mathbb{Q}(u^2)=\mathbb{Q}(u)$$

2) $[F(u):F(u^2)]=2$인 예.

$u=\sqrt{2}$이라 하면, $u^2=2$이고 다음이 성립한다.

$$irr(u,\mathbb{Q})=x^2-2,\quad irr(u^2,\mathbb{Q})=x-2$$
$$[\mathbb{Q}(u):\mathbb{Q}]=2,\ [\mathbb{Q}(u^2):\mathbb{Q}]=1,$$
$$[\mathbb{Q}(u):\mathbb{Q}(u^2)]=[\mathbb{Q}(u):\mathbb{Q}]=2$$

8.2.19

(1) $F<L_1,F<L_2\Rightarrow F\le L_1\cap L_2$이다.

L_1,L_2가 모두 F의 유한확대체이므로

$$\infty>[L_1:F]=[L_1:L_1\cap L_2][L_1\cap L_2:F]$$

가 되어 $L_1\cap L_2$는 F의 유한 확대체이다.

(2) $[L_1:F]=[L_1:L_1\cap L_2][L_1\cap L_2:F]$
$[L_2:F]=[L_2:L_1\cap L_2][L_1\cap L_2:F]$

이므로 $[L_1\cap L_2:F]\mid[L_1:F]$이고 $[L_1\cap L_2:F]\mid[L_2:F]$이다. $[L_1:F]$와 $[L_2:F]$가 서로소이므로 $[L_1\cap L_2:F]=1$이고 $L_1\cap L_2=F$이다.

8.2.20

(1) 위 문제 15(1)에 의하여 $[F(u)(v):F(u)]\leqq[F(v):F]$이므로

$$[F(u,v):F]=[F(u,v):F(u)][F(u):F]=[F(u)(v):F(u)]m\leqq[F(v):F]m=nm$$

이다.

(별해) 정리 8.1.15(2)에 의하여 $irr(v,F(u))|irr(v,F)$이므로 $\deg(v,F(u))\leqq\deg(v,F)=n$이다.

그러므로 $[F(u,v):F(u)]\leqq[F(v):F]=n$이다.

$$[F(u,v):F]=[F(u,v):F(u)][F(u):F]=[F(u)(v):F(u)]m\leqq[F(v):F]m=nm$$

이다.

(2) $\gcd(m,n)=1$일 때, $[F(u,v):F(u)]=n$임을 보이자.

$$[F(u,v):F]=[F(u,v):F(u)][F(u):F]=[F(u,v):F(u)]m$$
$$[F(u,v):F]=[F(u,v):F(v)][F(v):F]=[F(u,v):F(v)]n$$

이므로

$$[F(u,v):F(u)]m=[F(u,v):F]=[F(u,v):F(v)]n$$

이다. $\gcd(m,n)=1$이므로 $n|[F(u,v):F(u)]$이다. 그러므로 $n\leqq[F(u,v):F(u)]$이다.

또한 위 문제 15(1)에 의하여 $[F(u,v):F(u)]\leqq[F(v):F]=n$이므로 $[F(u,v):F(u)]=n$이다. 따라서

$$[F(u,v):F]=[F(u,v):F(u)][F(u):F]=nm$$

이다.

8.2.21 E는 F의 유한확대체이므로 E는 F의 대수적확대체이다(정리 8.2.2).

α가 E 위에서 대수적이라 하자. 그러면 $f(\alpha)=0$인 $f(x)=a_0+a_1x+\cdots+a_nx^n\in E[x]$가 존재한다.$(a_0,a_1,\cdots,a_n\in E)$
$f(x)\in F(a_n,\cdots,a_0)[x]$가 되어 $\deg(\alpha,F(a_0,\cdots,a_n))=[F(a_0,\cdots,a_n,\alpha):F(a_0,\cdots,a_n)]$은 유한이다(정리 8.1.15(2)). 따라서

$$[F(a_0,\cdots,a_n,\alpha):F]=[F(a_0,\cdots,a_n,\alpha):F(a_0,\cdots,a_n)][F(a_0,\cdots,a_n):F]$$

은 유한이다(정리 8.2.9에 의하여 $[F(a_0,\cdots,a_n):F]$은 유한). 따라서 α는 F 위에서 대수적이다(정리 8.2.2).

8.2.22 α는 E_F위에서 대수적이라 하자.
그러면 $f(\alpha)=0$인 $f(x)=a_0+a_1x+\cdots+a_nx^n\in E_F[x]$가 존재한다. $(a_0,a_1,\cdots,a_n\in E_F)$
$f(x)\in F(a_n,\cdots,a_0)[x]$가 되어 $\deg(\alpha,F(a_0,\cdots,a_n))=[F(a_0,\cdots,a_n,\alpha):F(a_0,\cdots,a_n)]$은 유한이다(정리 8.1.15(2)). 따라서

$$[F(a_0,\cdots,a_n,\alpha):F]=[F(a_0,\cdots,a_n,\alpha):F(a_0,\cdots,a_n)][F(a_0,\cdots,a_n):F]$$

은 유한이다(정리 8.2.9에 의하여 $[F(a_0,\cdots,a_n):F]$은 유한). 따라서 α는 F 위에서 대수적이다(정리 8.2.2). 그러면 $\alpha\in E_F$가 되어 모순이다. 따라서 α는 E_F위에서 초월적이다.

8.2.23 1차 이상의 다항식 $f(x)\in E_F[x]$가 E_F에서 해가 존재함을 보이면 충분하다. $f(x)\in E[x]$이고 E가 대수적 폐체이므로 $f(x)$의 해 α는 E에서 갖는다. 따라서 $f(\alpha)=0$이고 α는 E_F 위에서 대수적이다.

만약 $\alpha\notin E_F$이면 위 문제 22에 의하여 α는 E_F 위에서 초월적이 되어 모순이다. 따라서 $\alpha\in E_F$이다. 그러므로 E_F는 대수적 폐체이다.

(별해) 1차 이상의 다항식 $f(x)=a_0+a_1x+\cdots+a_nx^n\in E_F[x]$가 E_F에서 해가 존재함을 보이면 충분하다.
$f(x)$의 해를 α라 하면, $f(x)\in E[x]$이고 E가 대수적 폐체이므로 $\alpha\in E$이다.
그리고 $\deg(\alpha,F(a_0,\cdots,a_n))=[F(a_0,\cdots,a_n,\alpha):F(a_0,\cdots,a_n)]$은 유한이다(정리 8.1.15(2)). 따라서

$$[F(a_0,\cdots,a_n,\alpha):F]=[F(a_0,\cdots,a_n,\alpha):F(a_0,\cdots,a_n)][F(a_0,\cdots,a_n):F]$$

은 유한이다(정리 8.2.9에 의하여 $[F(a_0,\cdots,a_n):F]$은 유한). 따라서 α는 F 위에서 대수적이다(정리 8.2.2). 그러면 $\alpha\in E_F$이다.

8.2.24 임의의 원소 $a\in F$는 $x-a\in F[x]$의 해이므로 $a\in F(x)_F$이다.

다음에 $F[x]$의 다항식 $f(x)$와 $g(x)$가 서로소인 $\dfrac{f(x)}{g(x)}\in F(x)-F$가
1차 이상의 다항식 $h(x)=a_nx^n+\cdots+a_1x+a_0\in F[x]$의 해가 아님을 보이면 증명이 완료된다. 즉,

$$h\left(\frac{f(x)}{g(x)}\right)=a_n\left(\frac{f(x)}{g(x)}\right)^n+\cdots+a_1\left(\frac{f(x)}{g(x)}\right)+a_0$$

가 0이 아님을 보이자. 만약 $h\left(\dfrac{f(x)}{g(x)}\right)=0$이면 양변에 $g^n(x)$를 곱하면

$$a_nf^n(x)+a_{n-1}f^{n-1}(x)g(x)+\cdots+a_1f(x)g^{n-1}(x)+a_0g^n(x)=0$$
$$a_nf^n(x)=-g(x)\left(a_{n-1}f^{n-1}(x)+\cdots+a_1f(x)g^{n-2}(x)+a_0g^{n-1}(x)\right)$$

이므로 $g(x)|f^n(x)$이고 $f(x)$와 $g(x)$가 서로소이므로 $g(x)|f(x)$이다(정리 7.2.4(2)). 그러면 적당한 다항식 $f_1(x)\in F[x]$가 존재하여 $f(x)=g(x)f_1(x)$이다. 또한 $f(x)$와 $g(x)$가 서로소이므로 정리 7.2.3에 의하여

$$1=f(x)f_2(x)+g(x)g_1(x)=f_1(x)g(x)f_2(x)+g(x)g_1(x)=g(x)(f_1(x)f_2(x)+g_1(x))$$

인 다항식 $f_2(x),g_1(x)\in F[x]$가 존재하므로 $g(x)\in F$(단원)이다. 이때 $c=g(x)$라 하자. 그러면 $f(x)\notin F$이므로 $\deg(f(x))\geqq 1$이어야하고 다음이 성립한다.

$$a_nf^n(x)+\cdots+a_1f(x)c^{n-1}+a_0c^n=0$$

여기서 $\deg(f(x))<\deg(f^2(x))<\cdots<\deg(f^n(x))$이므로 위 등식에서 최고차항을 생각하면 차례로 $(c\neq 0)$

$$a_n=0,\ a_{n-1}=0,\cdots,\ a_0=0$$

이다. 따라서 $h(x)=0$이 되어 모순이다. 그러므로 $\dfrac{f(x)}{g(x)}\in F(x)-F$는 F 위에서 초월적이다.
$\therefore F(x)$에서 F의 대수적 폐포는 F이다.

8.2.25. 체 F 위의 다항식환 $F[x]$에서 다음과 같이 정의된 미분 함수

$$D : F[x] \to F[x],\ D(f(x)) = f'(x)$$

에 대하여 다음 물음에 답하라. 단, $f'(x)$는 $f(x) \in F[x]$의 형식적 미분이다.

(2) 체 F의 표수가 0인 경우 D의 핵을 구하라.

(3) 체 F의 표수가 $p(\neq 0)$인 경우 D의 핵을 구하라.

(4) 모든 $f(x) \in F[x]$와 $a \in F$에 대해, $D(af(x)) = aD(f(x))$임을 보여라.

(5) 모든 $f(x), g(x) \in F[x]$에 대해, $D(f(x)g(x)) = f(x)g'(x) + f'(x)g(x)$임을 보여라.

(6) 모든 $f(x), g(x) \in F[x]$에 대해, $D(f(x)^m) = (m \cdot 1)f(x)^{m-1}f'(x)$임을 보여라.

8.2.25

(1) $\ker(D) = \{f(x) = a_n x^n + \cdots + a_0 \in F[x] \mid D(f(x)) = f'(x) = na_n x^{n-1} + \ldots + a_1 = 0\}$

한편 F의 표수가 0이므로 $F[x]$의 표수도 0이다.

그러므로 $f'(x) = na_n x^{n-1} + \ldots + a_1 = 0$이기 위해서는

$$a_n = a_{n-1} = \ldots = a_1 = 0$$

그러므로 $\ker(D) = \{a_0 \mid a_0 \in F\} = F$이다.

(2) F의 표수가 p이므로 $F[x]$의 표수가 p이다. 지수가 p의 배수인 항만 남는다.

$$\ker(D) = \left\{ f(x) = a_{bp}x^{bp} + \ldots + a_p x^p + a_0 \mid b = \left[\frac{n}{p}\right] \right\}$$

(3) 연습문제 5.3.16(1)에 의하여 $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$이므로 수학적 귀납법에 의하여 성립한다.

8.2.26

($\Rightarrow$) $m > 1$라 하자.

$$f(x) = (x-\alpha)^m g(x), g(x) \in F[x]$$

$$f'(x) = m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m g'(x) = (x-\alpha)(m(x-\alpha)^{m-2}g(x) + g'(x)(x-\alpha)^{m-1})$$

이므로 α가 $f'(x)$의 해이다.

($\Leftarrow$) α가 $f'(x)$의 해라고 하자.

$$f'(x) = (x-\alpha)g(x),\ g(x) \in F[x]$$

$f(\alpha) = 0$이므로 인수정리에 의해 $\exists h(x) \in F[x]$, $f(x) = (x-\alpha)h(x)$이다. 그러므로

$$f'(x) = h(x) + (x-\alpha)h(x)$$

이다. 한편 $0 = f'(\alpha) = h(\alpha)$이므로 인수정리에 의해 $\exists k(x) \in F[x]$, $h(x) = (x-\alpha)k(x)$이다. 따라서

$$f(x) = (x-\alpha)(x-\alpha)k(x) = (x-\alpha)^2 k(x)$$

이므로 $m \geq 2$이다.

== 연습문제 (8.3) ==

8.3.1 정리 8.3.4와 8.3.5(2)를 이용하자.

(1) 2와 3은 작도가능 $\Rightarrow \sqrt{2} + \sqrt{3}$ 작도가능

(2) 3은 작도가능 $\Rightarrow \sqrt{3}$ 작도가능 $\Rightarrow \sqrt{\sqrt{3}} = \sqrt[4]{3}$ 작도가능

(3) 2 작도가능 $\Rightarrow \sqrt[4]{2}$작도가능 ($\because$ (2)) $\Rightarrow \sqrt{3 + \sqrt[4]{2}}$ 작도가능

8.3.2 정n각형이 작도가능할 필요충분조건은 $\frac{360°}{n}$을 작도하는 것과 동치이다. 또한

정리 8.3.12에 의하여 $n=2^m$이거나 $n=2^k p_1\cdots p_r$(단, p_i는 페르마소수 (3, 5, 17, 257))이어야 한다. 그러므로

$360=2^3 3^2 5$에서 위 조건을 만족하는 최대 n은 $2^3\cdot 3\cdot 5=120$각형을 작도할 수 있으므로 $\frac{360°}{120}=3°$가 작도 가능한 최소 자연수이다.

8.3.3

정9각형이 작도 가능하면 $\frac{360°}{9}=40°$가 작도 가능하다. 또한 40°의 절반 20°도 작도 가능하다. 하지만 정리 8.3.11의 증명에서 20°는 작도 불가능하므오 정9각형도 작도 불가능하다.

(별해) (정리 8.3.12이용) 정n각형이 작도가능할 필요충분조건은 $n=2^m(m\geq 2)$또는
$n=2^n p_1\cdots p_r\ (k\geq 0)$ $p_1\cdots p_r$은 서로 다른 페르마 소수이어야한다.
이때 3은 페르마 소수이나 $n=9=3\times 3$은 서로 다른 페르마소수의 곱이 아니므로 작도 불가능하다.

8.3.4 30°가 작도 가능 $\Leftrightarrow$ $\cos 30°$ 작도가능 $\Leftrightarrow \frac{\sqrt{3}}{2}$작도가능 $\Leftrightarrow$ $2, \sqrt{3}$이 작도가능

$\therefore 30°$ 작도가능

(별해) (정리 8.3.12이용) $\frac{360°}{12}=30°$이므로 정$12=2^2\cdot 3$각형작도 가능하므로 $30°$ 작도가능하다.

8.3.5 (정리 8.3.12이용) 원에 내접한 정삼각형과 정육각형은 3×2이므로 작도가능하므로 $120°$와 $60°$는 작도가능하다.

$\frac{60°}{2}=30°$ 이므로 $30°$ 작도가능 $\Rightarrow$ $90°$ 작도가능

$\frac{30°}{2}=15°$ 이므로 $15°$ 작도가능 $\Rightarrow$ $45°$ 작도가능

8.3.6. 정리 8.3.4와 8.3.5(2)를 이용하면
$a(\geq 0)$가 작도가능 $\Rightarrow$ $\sqrt{a}$도 작도가능
$b(\geq 0)$가 작도가능 $\Rightarrow$ $\sqrt{b}$도 작도가능

$\sqrt{a}, \sqrt{b}$가 작도가능 $\Rightarrow$ $\sqrt{a}\cdot\sqrt{b}=\sqrt{ab}$도 작도가능
$\therefore$ a, b가 작도가능이면 $\sqrt{ab}$도 작도가능

8.3.7

(1) $\omega^5-1=(\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5})^5-1=\cos 2\pi+i\sin 2\pi-1=1-1=0$

(2) $p(w)=w^4+w^3+w^2+w+1=\frac{w^5-1}{w-1}=\frac{0}{w-1}(\because (1)\text{에 의해 } w^5-1)=0$

(3) $w^2+w+1+w^{-1}+w^{-2}=\frac{w^5-1}{w^2(w-1)}=\frac{0}{w^2(w-1)}=0$

(4) $\omega=\cos\frac{2\pi}{5}+isin\frac{2\pi}{5}$이면 $\frac{1}{\omega}=\cos\frac{2\pi}{5}-i\sin\frac{2\pi}{5}$이므로 $\omega+\omega^{-1}=\omega+\frac{1}{\omega}=2\cos\frac{2\pi}{5}$이다. 위 (3)에서

$$0=w^2+w+1+w^{-1}+w^{-2}=(w+w^{-1})^2-2+w+w^{-1}+1=4\cos^2\frac{2\pi}{5}+2\cos^2\frac{2\pi}{5}-1$$

이므로 $\cos\frac{2\pi}{5}$는 $4x^2+2x-1$의 근이다.

(5) 정리 8.3.12에 의하여 5는 페르마소수이므로 정5각형은 작도가능하다.

8.3.8. 방정식의 근은 $\sqrt{\frac{3\pm\sqrt{5}}{2}}$ 이다. $2, 3, \sqrt{5}$가 작도 가능하므로 정리 8.3.4와 8.3.5(2)에 의하여 모든 근은 작도 가능하다.

8.3.9 기약다항식 $p(x)$의 근이 a이므로 $\deg(a,\mathbb{Q})=\deg(p(x))\neq 2^n$ (가정)이다.
a가 작도가능하면 정리 8.3.7에 의하여 $\deg(a.\mathbb{Q})=[\mathbb{Q}(a):\mathbb{Q}]=2^m$이므로 가정에 모순
$\therefore a$는 작도불가능하다.

== 연습문제 (8.4) ==

8.4.1. (1) $p(1)=2, p(0)=1, p(-1)=2$이므로 $p(x)$는 일차인수를 갖지 않는다.
또한 $\deg(p(x))=2$이므로 인수정리에 의해 $p(x)$는 $\mathbb{Z}_3$위에서 기약다항식이다.
(2) 크로네커 정리에 의해

$$\mathbb{Z}_3(\alpha)=\{a\alpha+b|a,b\in\mathbb{Z}_3, \alpha^2+1=0\}=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$$

(3) 위수 8인 원소를 구하자. $x\in\mathbb{Z}_3(\alpha)$를 구하자. $\alpha^2=-1$이므로
$x=\alpha+1$일 때, 위수는 8의 약수이다.

$$x^2=(\alpha+1)^2=-1-\alpha+1=-\alpha,$$
$$x^4=(-\alpha)^2=-1$$

이다. 따라서 $\alpha+1$의 위수는 8이므로 원시8제곱근이다. 그러므로 나머지 원시8제곱근은 다음과 같다(정리 8.4.11(2)).

$$x^3=2\alpha+1=-\alpha+1,\quad x^5=2\alpha+2=-\alpha-1,\quad x^7=\alpha-1$$

8.4.2. (1) $\mathbb{Z}_5^*=\{1,2,3,4\}$, $2^2=4=-1, |2|=4$ 이므로 $\mathbb{Z}_5^*=\langle 2\rangle$이다. 따라서 생성원은 $2, 2^3$이다.
(2) $\mathbb{Z}_{13}^*=\{1,2,3,4,5,6,7,8,9,10,11,12\}$, $2^6=64=-1, |2|=6$이므로 $\mathbb{Z}_{13}^*=\langle 2\rangle$이다. 따라서 생성원은 $2, 2^5, 2^7, 2^{11}$이다.

8.4.3. (1) $\phi(3^2-1)=\phi(2^3)=2^3-2^2=4$이므로 4개.
(2) $\phi(17-1)=\phi(2^4)=2^4-2^3=8$이므로 8개.
(3) $\phi(23-1)=\phi(22)=\phi(2)\phi(11)=10$개

8.4.4. (1) $[\mathbb{Q}(\omega,\sqrt[3]{2}):\mathbb{Q}]=[\mathbb{Q}(\omega,\sqrt[3]{2}):\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=[\mathbb{Q}(\omega,\sqrt[3]{2}):\mathbb{Q}(\sqrt[3]{2})]\cdot 3.$
$x^3-1=(x-1)(x^2+x+1)$이고, $\omega\neq 1$이므로 ω는 x^2+x+1의 근이다.
또한 $\omega=\frac{-1\pm i\sqrt{3}}{2}\notin\mathbb{Q}(\sqrt[3]{2})$이고, $\deg(x^2+x+1)=2$이므로 $[\mathbb{Q}(\omega,\sqrt[3]{2}):\mathbb{Q}]=6$.
(2) $\omega=\frac{-1\pm i\sqrt{3}}{2}$이므로 $\mathbb{Q}(\omega,\sqrt[3]{2})\subset\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$이다. 따라서 $1+2\omega=\pm i\sqrt{3}$이다.
$\mathbb{Q}(\omega,\sqrt[3]{2})\supset\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$이므로 $\therefore\mathbb{Q}(\omega,\sqrt[3]{2})=\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$

8.4.5. (1) $p(\alpha)=\alpha^2+\alpha+2=\alpha^2+\alpha-1=0$이므로

$\alpha^2 = -\alpha - 2 = 2\alpha + 1$, $\alpha^4 = 2\alpha^2 + 2\alpha = 4\alpha + 2 + 2\alpha = 6\alpha + 2 = -1$. $\alpha^8 = \alpha^2 + \alpha = 2\alpha + 1 + \alpha = 1$
이다. (α는 $\mathbb{F}_9$의 원시원소이다.)

(2) α는 체 $\mathbb{F}_9$의 원시원소 이므로 $|\alpha^i| = \frac{|\alpha|}{\gcd(8,i)} = \frac{8}{\gcd(8,i)} = 8$인 α^i도 체 $\mathbb{F}_9$의 원시원소가 된다. 따라서 $\gcd(8,i) = 1$인 i를 찾아주면 $i = 1,3,5,7$ 이므로 체 $\mathbb{F}_9$의 원시원소는 $\alpha, \alpha^3, \alpha^5, \alpha^7$ 이다.

$\therefore$ 체 $\mathbb{F}_9$의 원시원소는 $\alpha, \alpha^3, \alpha^5, \alpha^7$이다.

이제 체 $\mathbb{F}_9$의 원시원소를 근으로 갖는 2차 원시다항식을 구하자.

그런데 α를 근으로 갖는 모닉 기약다항식은 $p(x)$인데, 정리에 의해 α^3도 $p(x)$의 근이 된다. 따라서 α^5, α^7을 근으로 갖는 2차 원시다항식을 찾아주면 된다. α^5를 근으로 갖는 원시 다항식은 $(\alpha^5)^3$도 근으로 갖는데 $(\alpha^5)^3 = \alpha^{15} = \alpha^8 \cdot \alpha^7 = \alpha^7$ 이므로 α^5를 근으로 갖는 원시 다항식은 α^7도 근으로 갖는다. 따라서 α^5를 근으로 갖는 2차 원시다항식을 구해보자.

$(\alpha^5)^2 + b(\alpha^5) + c = 0$ 이 되는 b, c를 구하면 된다. 이 때 $\alpha^5 = 2\alpha$이므로

$(2\alpha)^2 + b(2\alpha) + c = \alpha^2 + 2b\alpha + c = (2\alpha + 1) + 2b\alpha + c = (2b + 2)\alpha + (c + 1) = 0$이다.

이 식이 α에 상관없이 항상 0이 되기 위한 $b = -1, c = -1$ 이므로 α^5, α^7을 근으로 갖는 2차 원시다항식은 $x^2 - x - 1$ 이다.

$\therefore x^2 + x + 2,\ x^2 - x - 1$

8.4.6. $\mathbb{Z}_3 = \mathbb{F}_3 = \{0,1,2\}$이므로 $f(0) = f(1) = f(2) = 0$이다. 인수정리에 의하여

$x \mid (x^9 - x),\ (x-1) \mid (x^9 - x),\ (x+1) \mid (x^9 - x)$

이다. 그러면 $f(x) = x(x-1)(x+1)(x^2+1)g(x)$이고 $\deg(g(x)) = 6$이다.

한편 $x^2 + 1,\ x^2 + x + 2,\ x^2 + 2x + 2$는 $\mathbb{F}_3$ 위에서 모든 2차 기약다항식이다(문제 5.6.6).

$\alpha^2 + 1 = 0$. 즉 $\alpha^2 = -1$이고 $irr(\alpha, \mathbb{F}_3) = x^2 + 1$이다. 그러면

$\alpha^9 = (\alpha^2)^4 \alpha = (-1)^4 \alpha = \alpha$

이므로 $f(\alpha) = 0$이다. 정리 8.1.15(2)에 의하여 $(x^2+1) \mid (x^9 - x)$이다. 같은 방법으로

$\alpha^2 + \alpha + 2 = 0$. 즉 $\alpha^2 = -\alpha - 2 = -\alpha + 1$이고 $irr(\alpha, \mathbb{F}_3) = x^2 + x + 2$이다. 그러면

$\alpha^9 = (\alpha^2)^3 \alpha^2 \alpha = (-\alpha + 1)^3 (-\alpha + 1)\alpha = (-\alpha^3 + 1)(-\alpha^2 + \alpha) = (\alpha^2 - \alpha + 1)(-\alpha^2 + \alpha)$
$= (-\alpha + 1 - \alpha + 1)(\alpha - 1 + \alpha) = (\alpha - 1)(-\alpha - 1) = -\alpha^2 + 1 = \alpha - 1 + 1 = \alpha$

이므로 $f(\alpha) = 0$이다. 정리 8.1.15(2)에 의하여 $(x^2 + x + 2) \mid (x^9 - x)$이다. 같은 방법으로

$\alpha^2 + 2\alpha + 2 = 0$. 즉 $\alpha^2 = -2\alpha - 2 = \alpha + 1$이고 $irr(\alpha, \mathbb{F}_3) = x^2 + 2x + 2$이다. 그러면

$\alpha^9 = (\alpha^2)^3 \alpha^2 \alpha = (\alpha + 1)^3 (-\alpha + 1)\alpha = (\alpha^3 + 1)(\alpha^2 + \alpha) = (\alpha^2 + \alpha + 1)(\alpha + 1 + \alpha)$
$= (\alpha + 1 + \alpha + 1)(-\alpha + 1) = (-\alpha - 1)(-\alpha + 1) = \alpha^2 - 1 = \alpha + 1 - 1 = \alpha$

이므로 $f(\alpha) = 0$이다. 정리 8.1.15(2)에 의하여 $(x^2 + 2x + 2) \mid (x^9 - x)$이다.

그러면 $g(x) = (x^2+1)(x^2 + x + 2)(x^2 + 2x + 2)$가 된다.

따라서 $f(x) = x(x-1)(x+1)(x^2+1)(x^2 + x + 2)(x^2 + 2x + 2)$이다.

(별해1) $F = \left\{\alpha \in \overline{\mathbb{F}_3} \mid \alpha\text{는 } x^{3^2} - x\text{의 근}\right\}$

라 하면, F는 $\mathbb{F}_3$의 유한(2차)확대체이다. 따라서 모든 $\alpha \in F$은 $\mathbb{F}_3$ 위에서 대수적이고, $\deg(\alpha, \mathbb{F}_3) \mid 2$이다(정리 8.2.3 (차원정리)). 그러므로 모든 $\alpha \in F$은 2의 약수차수 모닉 기약다항식의 해이다.

역으로 2의 약수 m차수 모닉 기약다항식의 근 β는 위수 3^m인 $\mathbb{F}_3(\beta)$의 원소이고 $\mathbb{F}_3(\beta) \subset F$이다(참조 연습문제 9번). 따라서 F의 모든 원소는 2의 약수 차수인 모닉 기약다항식의 모든 근으로 구성된다. 즉 $x^9 - x$의 근이다.

한편 $x,\ x+1,\ x-1,\ x^2+1,\ x^2+x+2,\ x^2+2x+2$는 $\mathbb{F}_3$ 위에서 모든 2차 이하의 기약다항식이다(문제 5.6.6). 그러므로 2의 약수 차수인 모든 모닉 기약다항식의 곱은 $x(x+1)(x-1)(x^2+1)(x^2+x+2)(x^2+2x+2)$이므로

$x^9-x=\Pi_{\alpha\in F}(x-\alpha)=x(x+1)(x-1)(x^2+1)(x^2+x+2)(x^2+2x+2)$

이다.

(별해2) 우변 전개해 확인함.

$$\begin{aligned}&x(x+1)(x-1)(x^2+1)(x^2+x+2)(x^2+2x+2)\\=&\,x(x^2-1)(x^2+1)(x^2+x-1)(x^2-x-1)\\=&\,x(x^4-1)(x^4+1)\\=&\,x(x^8-1)\\=&\,x^9-x\end{aligned}$$

8.4.7. $|E|=16$, $|E^*|=15$이고, E는 유한체이므로 E^*는 위수 15인 순환군이다(정리 8.4.2).

따라서 위수가 3인 것의 개수는 $3=\frac{15}{\gcd(i,15)}$인 i의 개수이다(정리 2.3.4). $i=5,10$이므로 2개이다.

8.4.8. $\mathbb{Z}_2(\alpha)=\mathbb{Z}_2[x]/\langle x^3+x^2+1\rangle$($\because x^3+x^2+1$는 $\mathbb{Z}_2$ 위에서 근이 존재하지 않으므로 기약)이므로 $\mathbb{Z}_2(\alpha)$는 위수가 8인 체이다. $\mathbb{Z}_2(\beta)$역시 위와 같은 방식으로 위수가 8인 체이다. 따라서 $|\mathbb{Z}_2(\alpha)|=|\mathbb{Z}_2(\beta)|=8$이므로 $\mathbb{Z}_2(\alpha)\cong\mathbb{Z}_2(\beta)$이다(정리 8.4.21).

8.4.9. 위수 p^n인 유한체 $\mathbb{F}_{p^n}$는 표수가 p이므로 소체 $\mathbb{Z}_p$를 포함한다. $\mathbb{F}_{p^n}\subset\overline{\mathbb{Z}_p}$이다. 그러므로 정리 8.4.5에 의하여

$$\mathbb{F}_{p^n}=\left\{\alpha\in\overline{\mathbb{Z}_p}\,|\,\alpha\text{는 }x^{p^n}-x\in\mathbb{Z}_p[x]\text{의 근}\right\}$$

이다. 다음에 d가 n의 약수, 즉 $n=dm$이라 하자. 그러면 위수가 p^d인 유한체 $\mathbb{F}_{p^d}$의 모든 원소는 $x^{p^d}-x$의 근이므로 $\mathbb{F}_{p^d}=\left\{\alpha\in\overline{\mathbb{Z}_p}\,|\,\alpha\text{는 }x^{p^d}-x\in\mathbb{Z}_p[x]\text{의 근}\right\}$이다. 그러므로 $\alpha\in\mathbb{F}_{p^d}$에 대하여 $\alpha^{p^d}=\alpha$이다. 한편

$$\alpha^{p^n}=\alpha^{p^{dm}}=\left(\alpha^{p^d}\right)^{p^{d(m-1)}}=\alpha^{p^{d(m-1)}}=\left(\alpha^{p^d}\right)^{p^{d(m-2)}}=\;\cdots\;=\alpha^{p^d}=\alpha$$

이므로 $\alpha\in\mathbb{F}_{p^n}$이다. 따라서 $\mathbb{F}_{p^d}\subset\mathbb{F}_{p^n}$이고 정리 8.4.5(2)에 의하여 부분체는 유일하게 존재한다.

(별해) p^n인 유한체 F는 원시원소 α가 존재한다(정리 8.4.2). $F^*=\langle\alpha\rangle$, $|\alpha|=p^n-1$이다. 한편 $d|n$이므로 $p^d-1|p^n-1$이다. F^*는 곱셈 순환군이므로 라그랑주 정리에 의하여 $H^*<F^*$이고 $|H^*|=p^d-1$인 부분군 H^*가 유일하게 존재한다(정리 2.3.11). 그러면 $H=H^*\cup\{0\}$는 F의 유일한 부분체이다.

8.4.10. $|F|=m$일 때, 정리 8.4.5에 의하여 F의 n차 유한확대체 E에 대하여 다음이 성립한다.

$$E=\left\{\alpha\in\overline{\mathbb{Z}_p}\,|\,\alpha\text{는 }x^{m^n}-x\text{의 근}\right\}$$

($\Rightarrow$) $f(x)|x^{m^n}-x$이므로 $f(x)$의 근 α는 모두 $x^{m^n}-x$의 근이다. 그러므로 $\alpha\in E$이다. 또한 $f(x)$가 F 위에서 기약이므로 $\deg(f(x))=\deg(\alpha,F)$이다(정리 8.1.15(2)). 정리 8.2.3(차원정리)에 의하여

$$n=[E:F]=[E:F(\alpha)]\,[F(\alpha):F]=[E:F(\alpha)]\deg(\alpha,F)=[E:F(\alpha)]\deg(f(x))$$

이므로 $\deg(f(x))|n$이다.

($\Leftarrow$) $\deg(f(x))|n$라 하자. $d=\deg(f(x))$라 하고 $f(\alpha)=0$이라 하면 $f(x)$가 F 위에서 기약이므로

$$d=\deg(f(x))=\deg(\alpha,F)=[F(\alpha):F]$$

이다. 따라서 $|F(\alpha)|=m^d$이므로 정리 8.4.5에 의하여 $F(\alpha)=\{\alpha\in\overline{F}\,|\,\alpha\text{는}x^{m^d}-x\text{의 근}\}$이다. 그러므로 $\alpha^{m^d}=\alpha$이다. 위 연습문제 8.4.9와 같은 방법에 의하여 α는 $x^{m^n}-x$의 근이므로 $f(x)|x^{m^n}-x$ 이다.

8.4.11. (1) ($\Rightarrow$) $x^2\equiv a\pmod p$의 해가 $\mathbb{Z}$에서 존재할 필요충분조건은 $x^2=[a]_p$(단, $[a]_p$는 a를 p로 나눈 나머지)는 $\mathbb{Z}_p$에서 해 $\alpha\in\mathbb{Z}_p^*$ ($a\not\equiv0\pmod p$)가 존재하는 것이다. 곱셈 순환군 $\mathbb{Z}_p^*$의 위수는 짝수인 $p-1$이고 $[a]_p\in\mathbb{Z}_p^*$이므로 라그랑주 정리(또는 정리 2.3.4(2))에 의하여

$$1=\alpha^{p-1}=(\alpha^2)^{\frac{(p-1)}{2}}=[a]_p^{\frac{(p-1)}{2}}$$

그러면 $a \equiv [a]_p (\mathrm{mod}\, p)$이므로 $1 \equiv [a]_p^{\frac{(p-1)}{2}} \equiv a^{\frac{(p-1)}{2}} (\mathrm{mod}\, p)$이다.

($\Rightarrow$) 곱셈 순환군 $\mathbb{Z}_p^*$의 생성원을 b라 하면 위수는 $p-1$이다. 그러면 적당한 자연수 n에 대하여 $a = b^n$이다. 이 때 $1 \equiv a^{\frac{(p-1)}{2}} (\mathrm{mod}\, p)$이면 분명히

$$1 \equiv a^{\frac{(p-1)}{2}} \equiv b^{n\frac{(p-1)}{2}} (\mathrm{mod}\, p)$$

이므로 $p-1 | n\dfrac{(p-1)}{2}$이므로 $n\dfrac{(p-1)}{2} = (p-1)t \Rightarrow n = 2t$이다. 그러면

$$a = b^n = b^{2t} = (b^t)^2$$

이 되어 $\mathbb{Z}$에서 $x^2 \equiv a (\mathrm{mod}\, p)$의 해 b^t가 존재한다.

(2) $x^2 \equiv 6 (\mathrm{mod}\, 17)$의 해가 존재하지 않으면 1차인수가 없으므로 $\mathbb{Z}_{17}[x]$에서 기약이다. 한편 (1)에 의하여

$$x^2 \equiv 6 (\mathrm{mod}\, 17)\text{의 해가 존재} \Leftrightarrow 6^{\frac{17-1}{2}} \equiv 6^8 \equiv (36)^4 \equiv (17 \cdot 2 + 2)^4 \equiv 2^4 \equiv -1 (\mathrm{mod}\, 17)$$

이므로 $x^2 - 6$은 $\mathbb{Z}_{17}[x]$에서 기약이다.

(별해) $(\pm 1)^2 = 1,\ (\pm 2)^2 = 4,\ (\pm 3)^2 = 9,\ (\pm 4)^2 = -1,$
$(\pm 5)^2 = 10,\ (\pm 6)^2 = 2,\ (\pm 7)^2 = 15,\ (\pm 8)^2 = 13$

이므로 $x^2 \equiv 6 (\mathrm{mod}\, 17)$의 해가 존재하지 않아 인수정리에 의하여 1차인수가 없으므로 $\mathbb{Z}_{17}[x]$에서 기약이다.

8.4.12. (1) $f(x) = x^3 + x^2 + 1$은 $\mathbb{Z}_2$ 위에서 기약이고 α가 $f(x)$의 근이므로 0, 1이 아니고 위수 8인 유한체

$$\mathbb{F}_8 = \mathbb{Z}_2(\alpha) = \{a + b\alpha + c\alpha^2 \,|\, a, b, c \in \mathbb{Z}_2\}$$

를 얻는다. 이때 표수가 2이므로 α^2, α^4 또한 근이다(정리 6.3.13).

한편 $|\alpha| = 7$이 되어 $\mathbb{F}^* = \langle \alpha \rangle$(정리 8.4.12)이므로

$$\alpha \neq \alpha^2,\ \alpha \neq \alpha^4,\ \alpha^2 \neq \alpha^4$$

이다. 그러므로 $\alpha, \alpha^2, \alpha^4$은 $f(x)$의 서로 다른 세 근이다.

따라서 $f(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$이다.

(별해) $f(x)$의 한 근이 $\alpha \neq 0, \pm 1$이고 표수가 2이므로 α^2, α^4 또한 근이다(정리 6.3.13).

$i)$ $\alpha = \alpha^2$라 하자. $\alpha = 1 (\because \alpha \neq 0)$이므로 $0 = \alpha^3 + \alpha^2 + 1 = 1$(모순) $\therefore \alpha \neq \alpha^2$

$ii)$ $\alpha = \alpha^4$라 하자. $\alpha^3 = 1$이므로 $0 = \alpha^3 + \alpha^2 + 1 = \alpha^2$(모순) $\therefore \alpha \neq \alpha^4$

$iii)$ $\alpha^2 = \alpha^4$라 하자. $\alpha^2 = 1, 0 = \alpha^3 + \alpha^2 + 1 = \alpha$(모순) $\therefore \alpha^2 \neq \alpha^4$

그러므로 $\alpha, \alpha^2, \alpha^4$는 $f(x)$의 서로 다른 세 근이다.

따라서 $f(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$이다.

(2) $f(x) = x^3 + x + 1$은 $\mathbb{Z}_2$ 위에서 기약이고 α가 $f(x)$의 근이므로 0, 1이 아니고 위수 8인 유한체

$$\mathbb{F}_8 = \mathbb{Z}_2(\alpha) = \{a + b\alpha + c\alpha^2 \,|\, a, b, c \in \mathbb{Z}_2\}$$

를 얻는다. 이때 표수가 2이므로 α^2, α^4 또한 근이다(정리 6.3.13).

한편 $|\alpha| = 7$이 되어 $\mathbb{F}^* = \langle \alpha \rangle$(정리 8.4.12)이므로

$$\alpha \neq \alpha^2,\ \alpha \neq \alpha^4,\ \alpha^2 \neq \alpha^4$$

이다. 그러므로 $\alpha, \alpha^2, \alpha^4$은 $f(x)$의 서로 다른 세 근이다.

따라서 $f(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$이다.

(별해) $f(x)$의 한 근이 $\alpha \neq 0$이고 표수가 2이므로 α^2, α^4 또한 근이다(정리 6.3.13).

$i)$ $\alpha = \alpha^2$라 하자. $\alpha = 1 (\because \alpha \neq 0)$이므로 $0 = \alpha^3 + \alpha + 1 = 1$(모순) $\therefore \alpha \neq \alpha^2$

$ii)$ $\alpha = \alpha^4$라 하자. $\alpha^3 = 1$이므로 $0 = \alpha^3 + \alpha + 1 = \alpha$(모순) $\therefore \alpha \neq \alpha^4$

$iii)$ $\alpha^2=\alpha^4$라 하자. $\alpha^2=1, 0=\alpha^3+\alpha+1=1$(모순) $\therefore \alpha^2\neq\alpha^4$

그러므로 $\alpha, \alpha^2, \alpha^4$는 $f(x)$의 서로 다른 세 근이다.

따라서 $f(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^4)$이다.

8.4.13. $f(x)=x^3-x^2+1$은 $\mathbb{Z}_3$ 위에서 기약이고 α가 $f(x)$의 근이므로 0, 1, -1이 아니고 위수 27인 유한체

$$\mathbb{F}_{27}=\mathbb{Z}_3(\alpha)=\{a+b\alpha+c\alpha^2 \mid a,b,c\in\mathbb{Z}_3\}$$

를 얻는다. 이때 표수가 3이므로 α^3, α^{3^2} 또한 근이다(정리 6.3.13).

한편 $\alpha^3=\alpha^2-1$이므로

$$\alpha^{13}=(\alpha^4)^3\alpha=(\alpha^3-\alpha)^3\alpha=(\alpha^{3^3}-\alpha^3)\alpha=((\alpha^2-1)^3-\alpha^3)\alpha=(\alpha^6-1-\alpha^3)\alpha$$
$$=((\alpha^2-1)^2-1-\alpha^3)\alpha=(\alpha^4+\alpha^2+1-1-\alpha^3)\alpha=(\alpha^4+\alpha^2-\alpha^3)\alpha$$
$$=(\alpha^3-\alpha+\alpha^2-\alpha^3)\alpha=(-\alpha+\alpha^2)\alpha=-\alpha^2+\alpha^3=-\alpha^2+\alpha^2-1=-1$$

이다. 따라서 라그랑주의 정리에 의하여 $|\alpha|=26$이 되어 $\mathbb{F}^*=\langle\alpha\rangle$(정리 8.4.12)이므로

$$\alpha\neq\alpha^3,\ \alpha\neq\alpha^9,\ \alpha^3\neq\alpha^9$$

이다. 그러므로 $\alpha, \alpha^3, \alpha^9$은 $f(x)$의 서로 다른 세 근이다.

따라서 $f(x)=(x-\alpha)(x-\alpha^3)(x-\alpha^9)$이다.

(별해) $f(x)$의 한 근이 $\alpha\neq 0, \pm 1$이고 표수가 3이므로 α^3, α^{3^2} 또한 근이다(정리 6.3.13).

$i)$ $\alpha=\alpha^3$라 하자. $\alpha^2=1$이므로 $0=\alpha^3-\alpha^2+1=\alpha$(모순) $\therefore \alpha\neq\alpha^3$

$ii)$ $\alpha=\alpha^9$라 하자. $\alpha^8=1$이다.

$$1=\alpha^8=(\alpha^3)^2\alpha^2=(\alpha^2-1)^2\alpha^2=(\alpha^4+\alpha^2+1)\alpha^2=\alpha^6+\alpha^4+\alpha^2$$
$$=\alpha^4+\alpha^2+1+\alpha^4+\alpha^2=-\alpha^4-\alpha^2+1=-\alpha^3+\alpha-\alpha^2+1=-\alpha^2+1+\alpha-\alpha^2+1=\alpha^2+\alpha-1$$

이므로 $0=\alpha^2+\alpha-2=(\alpha-1)(\alpha+2)$이고 이는 $\alpha\neq\pm 1$에 모순이다. $\therefore \alpha\neq\alpha^9$

$iii)$ $\alpha^3=\alpha^9$라 하자. $\alpha^6=1$이다. 그러면

$$1=\alpha^6=\alpha^4-2\alpha^2+1 \Rightarrow \alpha^4+\alpha^2=0 \Rightarrow \alpha^2=-1 \Rightarrow \alpha^3=\alpha^2-1=1 \Rightarrow \alpha^3=1=-\alpha^2 \Rightarrow \alpha=-1$$

이므로 모순이다. 그러므로 $\therefore \alpha^3\neq\alpha^9$이고 $\alpha, \alpha^3, \alpha^9$는 $f(x)$의 서로 다른 세 근이다.

따라서 $f(x)=(x-\alpha)(x-\alpha^3)(x-\alpha^9)$이다.

8.4.14. (수정) **위수 p^n인 유한체 F에서 모든 원소는 단 한 개의 p-제곱근을 가짐을 보여라.** 단, p는 소수

(풀이) $\sigma_p : F\to F, \sigma_p(a)=a^p$ 라 하자.

(i) $\forall a,b\in F$, $\sigma_p(a+b)=(a+b)^p=a^p+b^p=\sigma_p(a)+\sigma_p(b)$ ($\because$ $\mathrm{char}F=0$)

$$\sigma_p(ab)=(ab)^p=a^pb^p=\sigma_p(a)\sigma_p(b)$$

즉, σ_p는 준동형사상이다.

(ii) $a\in\ker\sigma_p$, $\sigma_p(a)=a^p=0$ 이거, F는 체이므로 영인자가 없고, $a=0$ 이다.

즉, $\ker\sigma_p=\{0\}$ 이므로 σ_p는 단사이고, F는 유한체이고, 정의역과 공역의 위수가 같으므로 σ_p는 전사이다

따라서 σ_p는 전단사이므로 σ_p는 자기동형사상이다.

$\mathrm{Im}\sigma_p=\sigma_p(F)=F$이므로 $a\in F, \sigma_p(a)=a^p$ 이므로 $\exists\, b\in F, b^p=a$ 이므로 b는 a의 p-제곱근이다.

따라서 a는 단 하나의 p-제곱근을 갖는다.

(1의 p-제곱근은 1개의 증명) 위수 p^n인 체 F에 대하여 $|F^*|=p^n-1$이다. 단위원 1에 대하여 $1^p=1$이다. 한편 $\alpha(\neq 1)\in F^*$에 대하여 $\alpha^p=1$이면 p가 소수이므로 α의 위수는 p이다. 그러면 라그랑주 정리에 의하여

$$p|p^n-1$$

이고 $p|1$이 되어 모순이다. 따라서 p제곱근은 1로 유일하게 존재한다.

8.4.15. 체 $\mathbb{F}_q$ 위에서 모닉 2차다항식 $f(x)=x^2+ax+b$의 개수는 q^2개 이고 이중에서

$$f(x)=(x+c)^2,\ c\in\mathbb{F}_q$$

또는

$$f(x)=(x+c)(x+d),\ c,\ d\in\mathbb{F}_q$$

와 같은 형태로 인수분해되는 다항식의 개수는

$$q+\binom{q}{2}=q+\frac{q(q-1)}{2}=\frac{q(q+1)}{2}$$

이다. 따라서 모닉 2차 기약다항식의 개수는 다음과 같다.

$$q^2-\frac{q(q+1)}{2}=\frac{q(q-1)}{2}$$

8.4.16.

(1) $char(F)=p$(소수)임을 보이자. F가 유한체이므로 문제 6.3.4에 의하여 표수는 0이 아니다. 따라서 정리 6.3.6에 의하여 F의 표수는 소수 p가 된다. 그러므로 임의의 원소 $a\in F$에 대하여 $pa=0$이다.

(별해) 위수가 q인 F의 부분 집합

$$A=\{1,\ 2\cdot 1,\ \cdots,\ (q+1)\cdot 1\}\subset F$$

를 생각하면 F의 위수가 q이므로 적당한 자연수 $i<j$가 존재하여

$$i\cdot 1=j\cdot 1\ \Rightarrow\ (j-i)\cdot 1=0,\ j-i>0$$

이다. 따라서 정리 6.3.3(2)에 의하여 F의 표수는 0이 아니다. 따라서 정리 6.3.6에 의하여 F의 표수는 소수 p가 된다. 그러므로 임의의 원소 $a\in F$에 대하여 $pa=0$이다.

(2) F의 표수는 소수 p이므로 $\mathbb{Z}_p<F$이다. $[F:\mathbb{Z}_p]=n$이라 하면 정리 8.4.3에 의하여 $q=|F|=p^n$이다.

(3) (2)와 정리 8.4.5에 의하여

$$F=\{\alpha\in\overline{\mathbb{Z}_p}\,|\,\alpha\text{는 } x^q-x\text{의 근}\}$$

이므로 $a^q-a=0$이다. 즉, $a^q=a$이다.

(4) $b\in K$가 F 위에서 대수적이므로 b는 $p(x)=irr(b,F)$의 해이다. $\deg(b,F)=m$이라하면

$$[F(b):F]=\deg(b,F)=m$$

이므로 $|F(b)|=q^m$이다(정리 8.4.2). 그러면 (3)에 의하여 $b^{q^m}=b$이다.

8.4.17. $p(x)=x^2+x+2$는 $p(0)=2,\ p(1)=1,\ p(-1)=2$이므로 인수정리에 의하여 $\mathbb{Z}_3=\mathbb{F}_3$ 위에서 모닉 기약다항식이다. $\overline{\mathbb{F}_3}$에서 $p(x)$의 한 근을 α라 하면

$$[\mathbb{F}_3(\alpha):\mathbb{F}_3]=\deg(\alpha,\mathbb{F}_2)=2$$

이므로 $\mathbb{F}_3(\alpha)=\mathbb{F}_{3^2}$이다. 그러므로

$$\mathbb{F}_{3^2}=\mathbb{F}_3(\alpha)=\{a+b\alpha\,|\,a,\ b\in\mathbb{F}_3,\ \alpha^2+\alpha+2=0\}$$

이다. 한편 $|\mathbb{F}_9{}^*|=8$이고

$$\alpha^2=-\alpha-2=-\alpha+1,$$
$$\alpha^4=(-\alpha+1)^2=\alpha^2-2\alpha+1=-\alpha+1-2\alpha+1=2=-1$$

이므로 $|\alpha|=8$이다. 따라서

$$\mathbb{F}_9{}^*=\langle\alpha\rangle=\{1,\ \alpha,\ \alpha^{2,}\ \cdots,\ \alpha^7\}$$

이므로 $\mathbb{F}_9$의 원시 원소는 $\alpha,\ \alpha^3,\ \alpha^5,\ \alpha^7$이다.

== 연습문제 (9.1) ==

9.1.1 (1) $3+\sqrt{2}$, $3-\sqrt{2}$ (2) $\sqrt{2}+i$, $-\sqrt{2}+i$, $\sqrt{2}-i$, $-\sqrt{2}-i$

(3) $\sqrt{2}+i$, $\sqrt{2}-i$ (4) $\pm\sqrt[4]{2}$, $\pm\sqrt[4]{2}i$

9.1.2 (1) $\sigma_5(\sqrt{2}+\sqrt{5})=\sqrt{2}-\sqrt{5}$

(2) $\sigma_3\sigma_2(\sqrt{2}+3\sqrt{5})=\sigma_3(\sigma_2(\sqrt{2}+3\sqrt{5}))=\sigma_3(-\sqrt{2}+3\sqrt{5})=-\sqrt{2}+3\sqrt{5}$

(3) $\sigma_5\left(\sigma_3\left(\frac{\sqrt{2}-3\sqrt{6}}{3\sqrt{2}+\sqrt{3}}\right)\right)=\sigma_5\left(\frac{\sqrt{2}+3\sqrt{6}}{3\sqrt{2}-\sqrt{3}}\right)=\frac{\sqrt{2}-3\sqrt{6}}{3\sqrt{2}-\sqrt{3}}$

(4) $\sigma_3\sigma_5(\sqrt{2}-\sqrt{5}+(\sigma_5\sigma_2)(\sqrt{30}))=\sigma_3(\sigma_5(\sqrt{2}-\sqrt{5}+\sqrt{30}))=\sigma_3(\sqrt{2}+\sqrt{5}-\sqrt{30})=\sqrt{2}+\sqrt{5}+\sqrt{30}$

9.1.3 ⅰ) $E_s \supset E_{<s>}$ (자명)

ⅱ) $E_s=\{a\in E\mid\sigma(a)=a,\ \forall\sigma\in S\}$

$\forall a\in E_s \Rightarrow \forall\sigma\in S\subset <S>,\ \sigma(a)=a$ (가정)

임의의 $\sigma'\in <S>$와 $a\in E$에 대하여

$\sigma'=\sigma_1^{a_1}\sigma_2^{a_2}\cdots\sigma_n^{a_n}\quad \exists\sigma_1,\cdots,\sigma_n\in S,\ a_1,\cdots,a_n\in\mathbb{Z}$

$\sigma'(a)=\sigma_1^{a_1}\sigma_2^{a_2}\cdots\sigma_n^{a_n}(a)=\sigma_1^{a_1}\cdots\sigma_{n-1}^{a_{n-1}}(a)=\cdots=a \quad (\because \sigma_1(a)=a,\cdots,\sigma_n(a)=a)$

이다. 따라서 $a\in E_{<s>}$이므로 $E_s\subset E_{<s>}$이다.

$\therefore E_s=E_{<s>}$

9.1.4 자기동형사상을 $\sigma\in Aut(F(\alpha_1,\cdots,\alpha_n)),\quad \sigma:F(\alpha_1,\cdots,\alpha_n)\to F(\alpha_1,\cdots,\alpha_n)$라 하자. 체 $F(\alpha_1,\cdots,\alpha_n)$의 F 위에서 생성원은 $\alpha_1^{a_1},\alpha_2^{a_2},\cdots,\alpha_n^{a_n}$, $a_i\in\mathbb{N}\cup\{0\}$인 형태이다. 그러면 임의의 원소 $\beta\in F(\alpha_1,\cdots,\alpha_n)$에 대하여 $\beta=f(\alpha_1,\cdots,\alpha_n)$, $\exists f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$이고, σ는 F 고정 환 동형사상이므로

$$\sigma(\beta)=\sigma(f(\alpha_1,\cdots,\alpha_n))=f(\sigma(\alpha_1),\cdots,\sigma(\alpha_n))$$

이다. 따라서 σ는 $\sigma(\alpha_i)$로 결정된다.(정리 3.2.25)

9.1.5 문제 9.1.3을 이용하자. 예 9.1.15 참조.

(1) $E_{\{\sigma_3\}}=\mathbb{Q}(\sqrt{5})$ (2) $E_{\{\sigma_5\}}=\mathbb{Q}(\sqrt{3})$ (3) $E_{\{\sigma_{15}\}}=\mathbb{Q}(\sqrt{15})$

(4) $E_{<\sigma_3,\sigma_5>}=\mathbb{Q}$ (5) $E_{<\sigma_3,\sigma_{15}>}=\mathbb{Q}$ (6) $E_{<\sigma_5,\sigma_{15}>}=\mathbb{Q}$

9.1.6 $K=\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$의 원소는 $\sqrt{2}$, $\sqrt[3]{2}$와 대수적 켤레이어야 하므로 예 9.1.13과 예 9.1.14에 의하여

$$G(K/\mathbb{Q})=\{id,\ \Psi_{\sqrt{2},-\sqrt{2}},\ \Psi_{\sqrt[3]{2},-\sqrt[3]{2}},\ \Psi_{\sqrt{2},-\sqrt{2}}\cdot\Psi_{\sqrt[3]{2},-\sqrt[3]{2}}\}$$

이다. $\sigma_1=id$, $\sigma_2=\Psi_{\sqrt{2},-\sqrt{2}}$, $\sigma_3=\Psi_{\sqrt[3]{2},-\sqrt[3]{2}}$ 이라 하자. 예 9.1.15 참조.

$K_{\{\sigma_1\}}=K$

$K_{\{\sigma_2\}}=\mathbb{Q}(\sqrt[3]{2})$

$K_{\{\sigma_3\}}=\mathbb{Q}(\sqrt{2})$

$K_{\{\sigma_2\cdot\sigma_3\}}=\mathbb{Q}(\sqrt[6]{2^5})=\mathbb{Q}(\sqrt[6]{2})$

이다.

9.1.7 (1) α의 $\mathbb{Q}$ 위에서 대수적 켤레를 $\beta(\neq\alpha)$라 하자.

$$irr(\alpha,\mathbb{Q})=irr(3+\sqrt{2},\mathbb{Q})=irr(3-\sqrt{2},\mathbb{Q})=x^2-6x+7$$

이므로 $\beta = 3-\sqrt{2}$ 이다.

(2) $\Psi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}),\quad \Psi_{\sqrt{2},-\sqrt{2}}(a+b\sqrt{2}) = a-b\sqrt{2}$

$\Psi_{\alpha,\beta} = \Psi_{3+\sqrt{2},3-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}),\quad \Psi_{\alpha,\beta}(a+b(3+\sqrt{2})) = a+b(3-\sqrt{2})$

라 하자. 그러면 임의의 $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$에 대하여

$$\begin{aligned}\Psi_{\alpha,\beta}(a+b\sqrt{2}) = \Psi_{\alpha,\beta}(a-3b+b(3+\sqrt{2})) &= a-3b+b(3-\sqrt{2}) \\ &= a-3b+3b-b\sqrt{2} \\ &= a-b\sqrt{2} = \Psi_{\sqrt{2},-\sqrt{2}}(a+b\sqrt{2})\end{aligned}$$

이다. 그러므로 $\Psi_{\sqrt{2},-\sqrt{2}}$와 $\Psi_{\alpha,\beta}$는 같다.

9.1.8 i) $\sigma_p(a+b) = (a+b)^p = a^p + b^p = \sigma_p(a) + \sigma_p(b)$

$\sigma_p(ab) = a^p b^p = \sigma_p(a)\sigma_p(b)$

$\therefore \sigma_p$는 준동형사상이다.

ii) $\forall a \in \ker(\sigma_p),\ 0 = \sigma_p(a) = a^p$이므로 $a = 0$이다.

$\therefore \ker(\sigma_p) = \{0\}$

$\therefore \sigma_p$는 단사이다.

하지만 σ_p는 전사가 아니다.

(반례) $F = \mathbb{Z}_p(x) = \left\{ \dfrac{g(x)}{f(x)} : f(x)(\neq 0),\ g(x) \in \mathbb{Z}_p[x] \right\}$이라 하고 σ_p가 전사라 하자.

그러면 $x \in \mathbb{Z}_p(x)$에 대한 역상이 존재한다. 즉, $\exists \dfrac{g(x)}{f(x)} \in \mathbb{Z}_p(x)$

$$x = \sigma_p\left(\frac{g(x)}{f(x)}\right) = \left(\frac{g(x)}{f(x)}\right)^p \Rightarrow (g(x))^p = x(f(x))^p$$

$p \mid \deg(g(x)^p)$이지만 $p \mid \deg(xf(x)^p)$이므로 모순이다. 따라서 σ_p는 전사가 아니다.

9.1.9 $F(\alpha) = \left\{ \dfrac{g(\alpha)}{f(\alpha)} : f(\alpha), g(\alpha) \in F[\alpha],\ f(\alpha) \neq 0 \right\},\ F(\beta) = \left\{ \dfrac{k(\beta)}{h(\beta)} : h(\beta), k(\beta) \in F[\beta], h(\beta) \neq 0 \right\}$라 할 때

$\Psi_{\alpha,\beta} : F(\alpha) \to F(\beta),\ \Psi_{\alpha,\beta}\left(\dfrac{g(\alpha)}{f(\alpha)}\right) = \dfrac{g(\beta)}{f(\beta)}$라 하자.

$$\Psi_{\alpha,\beta}\left(\frac{g_1(\alpha)}{f_1(\alpha)} + \frac{g_2(\alpha)}{f_2(\alpha)}\right) = \Psi_{\alpha,\beta}\left(\frac{f_2(\alpha)g_1(\alpha) + g_2(\alpha)f_1(\alpha)}{f_1(\alpha)f_2(\alpha)}\right) = \frac{f_2(\beta)g_1(\beta) + g_2(\beta)f_1(\beta)}{f_1(\beta)f_2(\beta)}$$

$$= \frac{g_1(\beta)}{f_1(\beta)} + \frac{g_2(\beta)}{f_2(\beta)} = \Psi_{\alpha,\beta}\left(\frac{g_1(\alpha)}{f_1(\alpha)}\right) + \Psi_{\alpha,\beta}\left(\frac{g_2(\alpha)}{f_2(\alpha)}\right)$$

$$\Psi_{\alpha,\beta}\left(\frac{g_1(\alpha)}{f_1(\alpha)} \cdot \frac{g_2(\alpha)}{f_2(\alpha)}\right) = \Psi_{\alpha,\beta}\left(\frac{g_1(\alpha)g_2(\alpha)}{f_1(\alpha)f_2(\alpha)}\right) = \frac{g_1(\beta)g_2(\beta)}{f_1(\beta)f_2(\beta)} = \frac{g_1(\beta)}{f_1(\beta)} \cdot \frac{g_2(\beta)}{f_2(\beta)} = \Psi_{\alpha,\beta}\left(\frac{g_1(\beta)}{f_1(\beta)} \cdot \frac{g_2(\beta)}{f_2(\beta)}\right)$$

이므로 $\Psi_{\alpha,\beta}$는 준동형사상이다.

ii) $\forall \dfrac{g(\alpha)}{f(\alpha)} \in \ker(\Psi_{\alpha,\beta}),\ 0 = \Psi_{\alpha,\beta}\left(\dfrac{g(\alpha)}{f(\alpha)}\right) = \dfrac{g(\beta)}{f(\beta)}$이다. 그러면 $g(\beta) = 0$이다.

$g(x) \in F[x]$라 하면 $g(\beta) = 0$이고 β가 초월적이므로 $g(x) = 0$이다. 그러면 $g(\alpha) = 0$이다.

$\therefore \ker(\Psi_{\alpha,\beta}) = \{0\}$

$\therefore \Psi_{\alpha,\beta}$는 단사이다.

iii) 정의에 의하여 $\forall \dfrac{g(\beta)}{f(\beta)} \in F(\beta)$에 대해 $\dfrac{g(\beta)}{f(\beta)} = \Psi_{\alpha,\beta}\left(\dfrac{g(\alpha)}{f(\alpha)}\right)$이므로

$\therefore \Psi_{\alpha,\beta}$는 전사이다.

$\therefore$ i), ii), iii)에 의해 $\Psi_{\alpha,\beta}$는 동형사상이다.

9.1.10 $G(K/\mathbb{Q})=\{\sigma\in Aut(K)|\sigma$는 $\mathbb{Q}$를 고정$\}$라 하면 $G(K/\mathbb{Q})\subset Aut(K)$이다.
다음에 임의의 $\sigma\in Aut(K)$에 대하여 예 5.3.12에 의해 σ는 $\mathbb{Q}$를 고정한다. $Aut(K)\subset G(K/\mathbb{Q})$이다.
따라서 $G(K/\mathbb{Q})=Aut(K)$ 이다.

9.1.11 i) $\exists\alpha\in\mathbb{Q}$, $d=\alpha^2$일 때
$$\mathbb{Q}(\sqrt{d})=\{a+b\sqrt{d}\,|\,a,b\in\mathbb{Q}\}=\{a+b\alpha|a,b\in\mathbb{Q}\}=\mathbb{Q}$$
이므로 예 5.3.12에 의해 $G(\mathbb{Q}(\sqrt{d})/\mathbb{Q})=G(\mathbb{Q}/\mathbb{Q})=\{id\}$이다.
(별해) $\exists\alpha\in\mathbb{Q}$, $d=\alpha^2$일 때 $irr(\sqrt{d},\mathbb{Q})=x-\sqrt{d}=x-\alpha$이므로 정리 9.1.3(켤레동형사상)와 따름정리 9.1.4(1)에 의하여 $G(\mathbb{Q}(\sqrt{d})/\mathbb{Q})=\{id\}$이다.
ii) $\forall\alpha\in\mathbb{Q}$, $d\neq\alpha^2$일 때 $irr(\sqrt{d},\mathbb{Q})=x^2-d$이므로 따름정리 9.1.4에 의하여
$$G(\mathbb{Q}(\sqrt{d})/\mathbb{Q})=\{id,\ \Psi_{\sqrt{d},-\sqrt{d}}\}$$
이다. 따라서 $G(\mathbb{Q}(\sqrt{d}/\mathbb{Q})\cong\mathbb{Z}_2$이다.
$$\therefore G(\mathbb{Q}(\sqrt{d}/\mathbb{Q})\text{는 }\{id\}\text{또는 }\mathbb{Z}_2\text{와 동형이다.}$$

9.1.12 자기동형사상을 $\sigma:\mathbb{R}\to\mathbb{R}$라 하자.
(1) 양수 $a\in\mathbb{R}^+$에 대하여
$$f(a)=f((\sqrt{a})^2)=f(\sqrt{a})^2\geq 0$$
이므로 $f(a)$는 양수이다.
(2) $a<b\ \Rightarrow\ b-a>0$이다. (1)에 의하여
$$0<\sigma(b-a)=\sigma(b)-\sigma(a)\ \Rightarrow\ \sigma(a)<\sigma(b)\ \text{이다.}$$

(3) 예 5.3.12에 의해 σ는 $\mathbb{Q}$를 고정한다. 다음에 $\forall a\in\mathbb{R}-\mathbb{Q}$, $f(a)=a$임을 보이자. $f(a)\neq a$라 하자.
i) $f(a)<a\ \Rightarrow\exists b\in\mathbb{Q}, f(a)<b<a$이다(유리수의 조밀성). (2)에 의하여
$b<a$이므로 $b=f(b)<f(a)$이다. 따라서 $f(a)<b<f(a)$이므로 모순이다. 따라서 $f(a)\not<a$이다.

ii) $f(a)>a$인 경우 위와 같은 방법으로 $f(a)\not>a$을 증명할 수 있다.
따라서 $f(a)=a$, $\forall a\in\mathbb{R}-\mathbb{Q}$이다.

(4) (3)에 의하여 $G(\mathbb{R}/\mathbb{Q})=\{id\}$이다.
한편 $\mathbb{C}=\mathbb{R}(i)$(예 8.1.9)이고 $irr(i,\mathbb{R})=x^2+1$이므로 연습문제 9.1.11과 같은 방법으로 $G(\mathbb{C}/\mathbb{R})=\{id,\ \Psi_{i,-i}\}\cong\mathbb{Z}_2$을 증명할 수 있다.

9.1.13 (1) $\deg\phi_p(x)=p-1$이므로 $\phi_p(x)$의 해의 개수는 $p-1$개이다.

α가 Φ_p의 해이므로 $0=\Phi_p(\alpha)=\dfrac{\alpha^p-1}{\alpha-1}$이다. 그러면 $1\leq i\leq p-1$인 i에 대해
$$\Phi_p(\alpha^i)=\frac{(\alpha^i)^p-1}{\alpha^i-1}=\frac{(\alpha^{pi}-1)}{(\alpha^i-1)}=\frac{(\alpha^p-1)(\alpha^{p(i-1)}+\cdots+\alpha^p+1)}{(\alpha-1)(\alpha^{i-1}+\cdots+\alpha+1)}=\Phi_p(\alpha)\cdot\frac{a^{p(i-1)}+\cdots+\alpha^p+1}{\alpha^{i-1}+\cdots+\alpha+1}=0$$
이므로 $\alpha,\cdots,\alpha^{p-1}$은 $\Phi_p(x)$의 근이다.
한편 $\alpha^i=\alpha^j(1\leq i<j\leq p-1)$이면 $\alpha^{j-i}=1$이고
$$0=\Phi_p(\alpha^{j-i})=\Phi_p(1)=p$$
가 되어 모순이다. 따라서 $\alpha^i\neq\alpha^j$이다. 따라서 $\Phi_p(x)$은 서로다른 근 $\alpha,\cdots,\alpha^{p-1}$를 갖는다.

(별해) α가 Φ_p의 해이므로 $0=\Phi_p(\alpha)=\dfrac{\alpha^p-1}{\alpha-1}$이다. 그러면 $\alpha^p-1=0$, $\alpha^p=1$이고 p가 소수이므로 $|\alpha|=p$이다.
그러면 $\alpha^i=\alpha^j(1\leq i<j\leq p-1)$이면 $\alpha^{j-i}=1$이고 $p|j-i$이므로 $j=i$이다. 즉 $\alpha,\cdots,\alpha^{p-1}$는 서로 다르고

$1 \le i \le p-1$이면 $\alpha^i \neq 1$이다. 하지만

$$(\alpha^i)^p = (\alpha^p)^i = 1^i = 1$$

이므로 α^i는 $x^p - 1 = (x-1)\Phi_p(x)$의 근이다. 즉, α^i는 $\alpha^i \neq 1$이므로 $\Phi_p(x)$의 근이다. 따라서 $\Phi_p(x)$은 서로다른 근 $\alpha, \cdots, \alpha^{p-1}$를 갖는다.

(2) $irr(\alpha, \mathbb{Q}) = \Phi_p(x)$이므로 정리 8.1.17에 의하여 $\mathbb{Q}(\alpha)$의 기저는 $1, \alpha, \cdots, \alpha^{p-2}$이다. $\alpha \neq 0$이므로 $\alpha, \cdots, \alpha^{p-2}, \alpha^{p-1}$도 기저이다.

$$\mathbb{Q}(\alpha) = \left\{a_0 + a_1\alpha + \cdots + a_{p-2}\alpha^{p-2} \mid a_0, \cdots, a_{p-2} \in \mathbb{Q}, \Phi_p(\alpha) = 0\right\}$$

이고 임의의 $\sigma \in G(\mathbb{Q}(\alpha)/\mathbb{Q})$에 대하여 정리 따름정리 9.1.4와 (1)로부터 $|G(\mathbb{Q}(\alpha)/\mathbb{Q})| = p-1$이고 각 원소는 α와 대수적 켤레이므로 $\Psi_{\alpha,\alpha^i} (1 \le i \le p-1)$이다.

임의의 원소 Ψ_{α,α^i}, $\Psi_{\alpha,\alpha^j} \in G(\mathbb{Q}(\alpha)/\mathbb{Q})$에 대하여

$$\Psi_{\alpha,\alpha^i}\Psi_{\alpha,\alpha^j}(\alpha) = \Psi_{\alpha,\alpha^i}(\alpha^j) = \alpha^{ij},$$
$$\Psi_{\alpha,\alpha^j}\Psi_{\alpha,\alpha^i}(\alpha) = \Psi_{\alpha,\alpha^j}(\alpha^i) = \alpha^{ji}$$

이고 α가 생성원이므로 $\Psi_{\alpha,\alpha^i}\Psi_{\alpha,\alpha^j} = \Psi_{\alpha,\alpha^j}\Psi_{\alpha,\alpha^i}$이다. 따라서 $G(\mathbb{Q}(\alpha)/\mathbb{Q})$는 위수 $p-1$인 가환군이다.

(3) $\mathbb{Q}(\alpha) = \left\{a_0 + a_1\alpha + \cdots + a_{p-2}\alpha^{p-2} \mid a_0, \cdots, a_{p-2} \in \mathbb{Q}, \phi_p(\alpha) = 0\right\}$이다.

$\mathbb{Q}(\alpha)$의 기저는 $1, \alpha, \cdots, \alpha^{p-2}$이다. $\alpha \neq 0$이므로 $\alpha, \cdots, \alpha^{p-2}, \alpha^{p-1}$도 $\mathbb{Q}(\alpha)$의 기저(최대 일차독립)이다.

다음에 $\forall \Psi_{\alpha,\alpha^i} \in G(\mathbb{Q}(\alpha)/\mathbb{Q})$ $(1 \le i \le p-1)$에 대하여 고정되는 원소 $a_1\alpha + a_2\alpha^2 + \cdots + a_{p-1}\alpha^{p-1} \in \mathbb{Q}(\alpha)$를 찾자.

$$a_1\alpha + a_2\alpha^2 + \cdots + a_{p-1}\alpha^{p-1} = \Psi_{\alpha,\alpha^i}(a_1\alpha + a_2\alpha^2 + \cdots + a_{p-1}\alpha^{p-1}) = a_1\alpha^i + a_2\alpha^{2i} + \cdots + a_{p-1}\alpha^{i(p-1)}$$

에서 $a_i\alpha^i = a_1\alpha^i \Rightarrow a_1 = a_i (1 \le i \le p-1)$이어야 한다. 따라서

$$a_1\alpha + a_2\alpha^2 + \cdots + a_{p-1}\alpha^{p-1} = a_1(\alpha + \alpha^2 + \cdots + \alpha^{p-1}) = a_1(-1) = -a_1 \in \mathbb{Q}$$

이므로 $G(\mathbb{Q}(\alpha)/\mathbb{Q})$의 고정체는 $\mathbb{Q}$뿐이다.

9.1.14 (1) 아이젠슈타인 판정에 의해 $f(x)$는 $\mathbb{Q}$ 위에서 기약이므로 크로네커정리에 의해

$$\begin{aligned}\mathbb{Q}(\theta) &= \mathbb{Q}[x]/ < x^3 + 2x + 2 >' \\ &= \left\{f(x) + < x^3 + 2x + 2 >' \mid f(x) \in \mathbb{Q}[x]\right\} \\ &= \left\{ax^2 + bx + c + < x^3 + 2x + 2 >' \mid a,b,c \in \mathbb{Q}\right\} \\ &= \left\{a\theta^2 + b\theta + c \mid a,b,c \in \mathbb{Q}, \theta^3 + 2\theta + 2 = 0\right\}\end{aligned}$$

(2) $0 = \theta^3 + 2\theta + 2 = (\theta+2)(\theta^2 - 2\theta + 6) - 10$이므로 $(\theta+2)^{-1} = \dfrac{1}{10}(\theta^2 - 2\theta + 6)$

(3) $f(-2) = -2$, $f(0) = 2$이므로 중간값 정리에 의하여 실근 θ가 존재한다. 한편 $f'(x) = 3x^2 + 2 > 0$이므로 $f(x)$는 증가함수이다. 그러므로 나머지 두 근은 허근이고, 모두 $\mathbb{Q}(\theta) < \mathbb{R}$에 속하지 않는다.

따라서 동형사상의 수는 켤레근 $\mathbb{Q}(\theta)$에 속하는 $f(x)$의 근의 수와 일치하므로 $G(\mathbb{Q}(\theta)/\mathbb{Q})$의 위수는 1이다.

9.1.15 (1) $irr(\sqrt[3]{2}, \mathbb{Q}(\sqrt{3})) = x^3 - 2$ ($\because \mathbb{Q}(\sqrt{3})$위에서 해가 없으므로 인수정리에 의해)

$irr(\sqrt{3}, \mathbb{Q}) = x^2 - 3$ ($\because$ 아이젠슈타인 기약판정)이므로

$$[K : G] = [K : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \deg(x^3 - 2)\deg(x^2 - 3) = 3 \cdot 2 = 6$$

이다.

$\mathbb{Q}(\sqrt{3})$ 위에서 $\mathbb{Q}(\sqrt[3]{2})$의 기저는 $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$

$\mathbb{Q}$위에서 $\mathbb{Q}(\sqrt{3})$의 기저는 $\{1, \sqrt{3}\}$ 이므로

$\mathbb{Q}$위에서 $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$의 기저는 $\{\{1,\ \sqrt{3},\ \sqrt[3]{2},\ \sqrt{3}\sqrt[3]{2},\ (\sqrt[3]{2})^2,\ \sqrt{3}(\sqrt[3]{2})^2\}$이다.

(2) 따름정리 9.1.4를 이용하자. $irr(\sqrt[3]{2}, \mathbb{Q}(\sqrt{3})) = x^3 - 2$의 세 근 중 K에 속하는 근은 $\sqrt[3]{2}$뿐이다. 또한 $irr(\sqrt{3}, \mathbb{Q}(\sqrt{3})) = x^2 - 3$의 두 근 $\pm\sqrt{3} \in K$이므로 $G(K/\mathbb{Q}(\sqrt[3]{2})) = \left\{id,\ \phi_{\sqrt{3},-\sqrt{3}}\right\}$이다(따름정리 9.1.4).

한편 $irr(\sqrt[3]{2},\mathbb{Q})=x^3-2$의 세 근 중 K에 속하는 근은 $\sqrt[3]{2}$뿐이다. 또한
$irr(\sqrt{3},\mathbb{Q})=x^2-3$의 두 근 $\pm\sqrt{3}\in K$이므로 $G(K/\mathbb{Q})=\{id,\ \phi_{\sqrt{3},-\sqrt{3}}\}$이다(따름정리 9.1.4).

$G(K/\mathbb{Q})=G(K/\mathbb{Q}(\sqrt[3]{2}))$이다.

(별해) $G(K/\mathbb{Q})$의 원소 σ는 $K=\mathbb{Q}(\sqrt{3},\sqrt[3]{2})$의 생성원 $\sqrt{3},\sqrt[3]{2}$의 대수적 켤레에 의해 결정되는데

$\sigma(\sqrt{3})$은 $\sqrt{3}$의 K에서 대수적 켤레원소 $\sqrt{3},-\sqrt{3}$이고

$\sigma(\sqrt[3]{2})$은 $\sqrt[3]{2}$의 K에서 대수적 켤레원소 $\sqrt[3]{2}$이다.

따라서 $G(K/\mathbb{Q})=\{id,\Psi_{\sqrt{3},-\sqrt{3}}\}$ (단, $\Psi_{\sqrt{3},-\sqrt{3}}(\sqrt{3})=-\sqrt{3}$, id는 항등사상)(따름정리 9.1.4).

9.1.16 $irr(\sqrt[3]{3},\mathbb{Q})=x^3-3$ ($\because$ 아이젠슈타인 기약판정)이므로

$[\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}]=\deg(x^3-3)=3$이다.

한편 $irr(\sqrt[3]{3},\mathbb{Q})=x^3-3$의 세 근(대수적 켤레) $\sqrt[3]{3},\ \alpha=\sqrt[3]{3}\dfrac{-1+i\sqrt{3}}{2},\ \beta=\sqrt[3]{3}\dfrac{-1-i\sqrt{3}}{2}$중 $\mathbb{Q}(\sqrt[3]{3})$에 속하는 근은 $\sqrt[3]{3}$뿐이므로

$|G(\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q})|=|\{id\}|=1$

이다.

9.1.17 (1) $irr(i,\mathbb{Q})=x^2+1$의 $\mathbb{Q}(i,\sqrt{2})$에서 두 근(대수적 켤레)은 $\pm i$이고

$irr(\sqrt{2},\mathbb{Q})=x^2-2$의 $\mathbb{Q}(i,\sqrt{2})$에서 두 근(대수적 켤레)은 $\pm\sqrt{2}$이므로 따름정리 9.1.4를 이용하면

$G(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})=\{id,\ \Psi_{\sqrt{2},-\sqrt{2}}\Psi_{i,i},\ \Psi_{\sqrt{2},\sqrt{2}}\Psi_{i,-i},\ \Psi_{\sqrt{2},-\sqrt{2}}\Psi_{i,-i}\}$

이다. 각 원소의 위수가 2이하이므로 $\mathbb{Z}_2\times\mathbb{Z}_2$와 동형이다.

(2) $irr(\sqrt[3]{2},\mathbb{Q}(\sqrt{2}))=x^3-2$의 세 근 중 $\mathbb{Q}(\sqrt[3]{2},\sqrt{2},i)$에서 근(대수적 켤레)은 $\sqrt[3]{2}$이고

$irr(i,\mathbb{Q}(\sqrt{2}))=x^2+1$의 $\mathbb{Q}(\sqrt[3]{2},\sqrt{2},i)$에서 두 근(대수적 켤레)은 $\pm i$이므로 따름정리 9.1.4를 이용하면

$G(\mathbb{Q}(\sqrt[3]{2},\sqrt{2},i)/\mathbb{Q}(\sqrt{2}))=\{id,\ \Psi_{i,-i}\}$

이다. 각 원소의 위수가 2이하이므로 $\mathbb{Z}_2$와 동형이다.

9.1.18

(1) $irr(i\sqrt{3},\mathbb{Q}(\sqrt[3]{2}))=x^2+3$의 두 근 $\pm i\sqrt{3}$은 모두 $\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$에 속하고 따름정리 9.1.4를 이용하면

$G(\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})/\mathbb{Q}(\sqrt[3]{2}))=\{id,\ \Psi_{i\sqrt{3},-i\sqrt{3}}\}$

이므로 위수는 2이다.

$irr(\sqrt[3]{2},\mathbb{Q}(i\sqrt{3}))=x^3-2$의 세 근 $\sqrt[3]{2},\ \alpha=\sqrt[3]{2}\dfrac{-1+i\sqrt{3}}{2},\ \beta=\sqrt[3]{2}\dfrac{-1-i\sqrt{3}}{2}$은 모두 $\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$에 속하고 따름정리 9.1.4를 이용하면

$G(\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})/\mathbb{Q}(i\sqrt{3}))=\{id,\ \Psi_{\sqrt[3]{2},\alpha},\ \Psi_{\sqrt[3]{2},\beta}\}$

이므로 위수는 3이다.

(2) $irr(i\sqrt{3},\mathbb{Q})=x^2+3$의 두 근 $\pm i\sqrt{3}$은 모두 $\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$에 속하고

$irr(\sqrt[3]{2},\mathbb{Q})=x^3-2$의 세 근 $\sqrt[3]{2},\ \alpha=\sqrt[3]{2}\dfrac{-1+i\sqrt{3}}{2},\ \beta=\sqrt[3]{2}\dfrac{-1-i\sqrt{3}}{2}$은 모두 $\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$에 속하고 따름정리 9.1.4를 이용하면

$G(\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})/\mathbb{Q})=\{id,\ \Psi_{i\sqrt{3},-i\sqrt{3}},\ \Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},i\sqrt{3}},\ \Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}},\ \Psi_{\sqrt[3]{2},\beta}\Psi_{i\sqrt{3},i\sqrt{3}},\ \Psi_{\sqrt[3]{2},\beta}\Psi_{i\sqrt{3},-i\sqrt{3}}\}$

이므로 위수는 6이다. 그러면 $G(\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})/\mathbb{Q})$는 $\mathbb{Z}_6$, S_3중의 하나와 동형이다. 각 원소의 위수를 구하자.

예를 들면 $\Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}}$의 위수는 1, 2, 3, 6에서 존재하므로, 생성원 $\sqrt[3]{3}$, $i\sqrt{3}$에 대한 것만 계산하면

$i)\ \Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}}(\sqrt[3]{2})=\Psi_{\sqrt[3]{2},\alpha}(\sqrt[3]{2})=\alpha,$

$ii)\ (\Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}})^2(\sqrt[3]{2})=\Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}}(\alpha)=\Psi_{\sqrt[3]{2},\alpha}(\beta)$

$=\Psi_{\sqrt[3]{2},\alpha}\left(\sqrt[3]{2}\,\frac{-1-i\sqrt{3}}{2}\right)=\alpha\left(\frac{-1-i\sqrt{3}}{2}\right)=\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right)\left(\frac{-1-i\sqrt{3}}{2}\right)=\sqrt[3]{2}$

$i)\ \Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}}(i\sqrt{3})=\Psi_{\sqrt[3]{2},\alpha}(-i\sqrt{3})=-i\sqrt{3},$

$ii)\ (\Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}})^2(i\sqrt{3})=\Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}}(-i\sqrt{3})=-(-i\sqrt{3})=i\sqrt{3}$

가 되어 $\Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}}$의 위수는 2이다. 나머지 원소에 대한 위수는 같은 방법으로 구하면 다음과 같다.

원소	id	$\Psi_{i\sqrt{3},-i\sqrt{3}}$	$\Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},i\sqrt{3}}$	$\Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}}$	$\Psi_{\sqrt[3]{2},\beta}\Psi_{i\sqrt{3},i\sqrt{3}}$	$\Psi_{\sqrt[3]{2},\beta}\Psi_{i\sqrt{3},-i\sqrt{3}}$
위수	1	2	3	2	3	2

위수 6인 군 $\mathbb{Z}_6$, S_3 중의 하나와 동형이다. 위에서 순환군이 아니므로 $G(\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})/\mathbb{Q})\cong S_3$이다.

9.1.19 분명히 $id\in G(K/E)$이다.

다음에 임의의 원소 $\sigma,\tau\in G(K/E)$에 대하여 $\sigma\tau$와 σ^{-1}은 자기동형사상이다(정리 3.2.19). 또한 임의의 원소 $a\in E$에 대하여 $\sigma(a)=a,\ \tau(a)=a$이므로 $a\in F\subset E$이면

$$\sigma\tau(a)=\sigma(\tau(a))=\sigma(a)=a,\ \sigma^{-1}(a)=a$$

이다. 따라서 $\sigma\tau,\ \sigma^{-1}\in G(K/F)$이다. 그러므로 $G(K/E)<G(K/F)$이다(정리 2.2.3).

== 연습문제 (9.2) ==

9.2.1. (1) x^2+3의 근은 $\pm\sqrt{3}i$이므로 분해체는 $K=\mathbb{Q}(\sqrt{3}i)$이다.

$irr(\sqrt{3}i,\mathbb{Q})=x^2+3$이므로 $[K:\mathbb{Q}]=[\mathbb{Q}(\sqrt{3}i):\mathbb{Q}]=\deg(x^2+3)=2$이다.

(2) x^3-3의 근은 $\sqrt[3]{3},\ \sqrt[3]{3}\,\frac{-1+i\sqrt{3}}{2},\ \sqrt[3]{3}\,\frac{-1-i\sqrt{3}}{2}$이므로 분해체 K는 $\mathbb{Q}(\sqrt[3]{3},\sqrt{3}i)$이다.

$irr(\sqrt[3]{3},\mathbb{Q})=x^3-3,\ irr(\sqrt{3}i,\mathbb{Q}(\sqrt[3]{3}))=x^2+3$이므로

$$[K:\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{3},\sqrt{3}i):\mathbb{Q}(\sqrt[3]{3})]\,[\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}]=\deg(x^2+3)\deg(x^3-3)=6$$

이다(연습문제 9.1.18(2) 참조).

(3) x^3-1의 근은 $1,\ \frac{-1+i\sqrt{3}}{2},\ \frac{-1-i\sqrt{3}}{2}$이므로 분해체 K는 $\mathbb{Q}(\sqrt{3}i)$이다.

$irr(\sqrt{3}i,\mathbb{Q})=x^2+3$이므로 $[K:\mathbb{Q}]=[\mathbb{Q}(\sqrt{3}i):\mathbb{Q}]=\deg(x^2+3)=2$이다.

(4) x^4-1의 근은 $\pm1,\ \pm i$이므로 분해체 K는 $\mathbb{Q}(i)$이다.

$irr(i,\mathbb{Q})=x^2+1$이므로 $[K:\mathbb{Q}]=[\mathbb{Q}(i):\mathbb{Q}]=\deg(x^2+1)=2$이다.

(5) x^3+5의 근은 $-\sqrt[3]{5},\ \sqrt[3]{5}\,\frac{1+i\sqrt{3}}{2},\ \sqrt[5]{5}\,\frac{1-i\sqrt{3}}{2}$이므로 분해체 K는 $\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i)$이다.

$irr(\sqrt[3]{5},\mathbb{Q})=x^3-5,\ irr(\sqrt{3}i,\mathbb{Q}(\sqrt[3]{5}))=x^2+3$이므로

$$[K:\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i):\mathbb{Q}(\sqrt[3]{5})]\,[\mathbb{Q}(\sqrt[3]{5}):\mathbb{Q}]=\deg(x^2+3)\deg(x^3-5)=6$$

이다.

(6) $x^3-7x+6=(x-1)(x-2)(x+3)$의 근은 $1,\ 2,\ -3$이므로 분해체 $K=\mathbb{Q}$이고 $[K:\mathbb{Q}]=1$이다.

(7) $(x^2-x)(x^3-2)$의 근은 $0,\ 1,\ \sqrt[3]{2},\ \sqrt[3]{2}\dfrac{-1+i\sqrt{3}}{2},\ \sqrt[3]{2}\dfrac{-1-i\sqrt{3}}{2}$이므로 분해체 K는 $\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i)$이다.
$[K:\mathbb{Q}]=6$이다. ((2)번 참조)

(8) $(x^2-3)(x^3-1)$의 근은 $\pm\sqrt{3},\ 1,\ \dfrac{-1+i\sqrt{3}}{2},\ \dfrac{-1-i\sqrt{3}}{2}$이므로 분해체 K는 $\mathbb{Q}(\sqrt{3},i)$이다.
$irr(\sqrt{3},\mathbb{Q})=x^2-3,\ irr(i,\mathbb{Q}(\sqrt{3}))=x^2+1$이므로

$$[K:\mathbb{Q}]=[\mathbb{Q}(\sqrt{3},i):\mathbb{Q}(\sqrt{3})]\,[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=\deg(x^2+1)\deg(x^2-3)=4$$

이다.

9.2.2.

$$S_{\mathbb{Q}}((x^2-2x-2)(x^2+1))=S_{\mathbb{Q}}((x-1+\sqrt{3})(x-1-\sqrt{3})(x-i)(x+i))=\mathbb{Q}(-1\pm\sqrt{3},\pm i)=\mathbb{Q}(\sqrt{3},i)$$

9.2.3.

$$S_{\mathbb{Q}(\sqrt{2})}(x^2-2\sqrt{2}x+3)=S_{\mathbb{Q}(\sqrt{2})}((x-\sqrt{2}-i)(x-\sqrt{2}+i))=\mathbb{Q}(\sqrt{2}\pm i)=\mathbb{Q}(\sqrt{2},i)$$

9.2.4.

$x^2-3=(x+\sqrt{3})(x-\sqrt{3})$의 분해체 $\mathbb{Q}(\sqrt{3})$이다.
$x^2-2x-2=(x-(1-\sqrt{3}))(x-(1+\sqrt{3}))$의 분해체는 $\mathbb{Q}(1-\sqrt{3},1+\sqrt{3})$이다.

$$1-\sqrt{3},1+\sqrt{3}\in\mathbb{Q}(\sqrt{3})$$

이므로 $\mathbb{Q}(1-\sqrt{3},1+\sqrt{3})\subset\mathbb{Q}(\sqrt{3})$이다.
다음에

$$\sqrt{3}=2\frac{(1+\sqrt{3})-(1-\sqrt{3})}{2}\in\mathbb{Q}(1-\sqrt{3},1+\sqrt{3})$$

이므로 $\mathbb{Q}(\sqrt{3})\subset\mathbb{Q}(1-\sqrt{3},1+\sqrt{3})$이다. 따라서 $\mathbb{Q}(1-\sqrt{3},1+\sqrt{3})=\mathbb{Q}(\sqrt{3})$이다.
x^2-3과 x^2-2x-2의 분해체는 $\mathbb{Q}(\sqrt{3})$으로 같다.

9.2.5.

$$S_{\mathbb{Q}}(x^4-9)=S_{\mathbb{Q}}((x^2-3)(x^2+3))=S_{\mathbb{Q}}((x-\sqrt{3})(x+\sqrt{3})(x-\sqrt{3}i)(x+\sqrt{3}i))$$
$$=\mathbb{Q}(\pm\sqrt{3},\pm\sqrt{3}i)=\mathbb{Q}(\sqrt{3},\sqrt{3}i)=\mathbb{Q}(\sqrt{3},i)$$
$$(\because i=(\sqrt{3}i)\sqrt{3}\frac{1}{3}\in\mathbb{Q}(\sqrt{3},\sqrt{3}i),\ \sqrt{3}i=\sqrt{3}(i)\in\mathbb{Q}(\sqrt{3},i))$$

$$S_{\mathbb{R}}(x^4-9)=S_{\mathbb{R}}((x-\sqrt{3})(x+\sqrt{3})(x-\sqrt{3}i)(x+\sqrt{3}i))=\mathbb{R}(\pm\sqrt{3},\pm\sqrt{3}i)=\mathbb{R}(\sqrt{3}i)=\mathbb{R}(i)=\mathbb{C}$$
$$(\because i=\sqrt{3}i\frac{1}{\sqrt{3}}\in\mathbb{R}(\sqrt{3}i),\ \sqrt{3}i=\sqrt{3}(i)\in\mathbb{R}(i))$$

9.2.6.

x^2-3의 분해체는 $\mathbb{Q}(\sqrt{3})=\{a+b\sqrt{3}\mid a,b\in\mathbb{Q}\}$이다.
유리수 a,b는 작도가능하고 3이 작도가능하므로 $\sqrt{3}$도 작도가능하다(정리 8.3.4와 정리 8.3.5). 그러므로 분해체의 원소 $a+b\sqrt{3}$은 작도 가능하다.

9.2.7. $p(x)=x^4-10x^2+1$ 의 근을 구하자. $x^2=t$로 치환하자.

$p(t)=t^2-10t+1$ 에서 $t=5\pm2\sqrt{6}$ 이므로 $x=\pm\sqrt{5\pm2\sqrt{6}}=\pm(\sqrt{3}\pm\sqrt{2})$이다.
$p(x)$의 근은 $\sqrt{3}+\sqrt{2}, \sqrt{3}-\sqrt{2}, -\sqrt{3}+\sqrt{2}, -\sqrt{3}-\sqrt{2}$ 이므로 분해체는 $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$이다.
따라서 $G(K/\mathbb{Q})=\{id,\ \psi_{\sqrt{2},-\sqrt{2}},\ \psi_{\sqrt{3},-\sqrt{3}},\ \psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{3},-\sqrt{3}}\}$이다(예 9.1.15 참조).

9.2.8. (1) $f(x)$의 근은 $\pm i,\ \pm\sqrt{2}$ 이므로 분해체는 $K=\mathbb{Q}(i,\sqrt{2})$이다.
$irr(i,\mathbb{Q}(\sqrt{2}))=x^2+1,\ irr(\sqrt{2},\mathbb{Q})=x^2-2$이므로

$$[K:\mathbb{Q}]=[\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}]=[\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=\deg(x^2+1)\deg(x^2-2)=4$$

이다.

(2) $\sigma\in G(K/\mathbb{Q})$는 K의 생성원 $i,\sqrt{2}$의 대수적 켤레에 의해 결정된다. 따라서

$$id,\quad \psi_{\sqrt{2},-\sqrt{2}}=\begin{cases}\mathbb{Q}(\sqrt{2})=-\sqrt{2}\\ \mathbb{Q}(i)=i\end{cases},\qquad \psi_{i,-i}=\begin{cases}\mathbb{Q}(\sqrt{2})=\sqrt{2}\\ \mathbb{Q}(i)=-i\end{cases},\ \psi_{\sqrt{2},-\sqrt{2}}\psi_{i,-i}=\begin{cases}\mathbb{Q}(\sqrt{2})=-\sqrt{2}\\ \mathbb{Q}(i)=-i\end{cases}$$

이다. 그러므로 $G(K/\mathbb{Q})\cong\mathbb{Z}_4$이거나 $G(K/\mathbb{Q})\cong V$이다.
한편 $|id|=1,\ |\psi_{\sqrt{2},-\sqrt{2}}|=2,\ |\psi_{i,-i}|=2,\ |\psi_{\sqrt{2},-\sqrt{2}}\psi_{i,-i}|=2$이므로 $G(K/\mathbb{Q})\cong V$이 되어 $G(K/\mathbb{Q})$의 부분군은 5개이다(예2.2.11).

9.2.9. (1) $f(x)=x^4-8x^2+15=(x^2-3)(x^2-5)$의 근은 $\pm\sqrt{3},\ \pm\sqrt{5}$ 이므로 분해체는 $K=\mathbb{Q}(\sqrt{3},\sqrt{5})$이다. 그러면 연습문제 8.2.12에 의하여 $K=\mathbb{Q}(\sqrt{3},\sqrt{5})=\mathbb{Q}(\sqrt{3}+\sqrt{5})$이므로 K는 $\mathbb{Q}$ 위에서 단순확대체이다.

(2) $irr(\sqrt{5},\mathbb{Q}(\sqrt{3}))=x^2-5,\ irr(\sqrt{3},\mathbb{Q})=x^2-3$이므로

$$[K:\mathbb{Q}]=[\mathbb{Q}(\sqrt{5},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{5},\sqrt{3}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=\deg(x^2-5)\deg(x^2-3)=4$$

이다.

9.2.10. (1) $irr(\sqrt{5},\mathbb{Q}(\sqrt{2},\sqrt{3}))=x^2-5,\ irr(\sqrt{3},\mathbb{Q}(\sqrt{2}))=x^2-3,\ irr(\sqrt{2},\mathbb{Q})=x^2-2$이므로

$$\begin{aligned}[K:\mathbb{Q}]&=[\mathbb{Q}(\sqrt{5},\sqrt{3},\sqrt{2}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{5},\sqrt{3},\sqrt{2}):\mathbb{Q}(\sqrt{3},\sqrt{2})][\mathbb{Q}(\sqrt{3},\sqrt{2}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]\\&=\deg(x^2-5)\deg(x^2-3)\deg(x^2-2)=8\end{aligned}$$

이다.

$$\begin{aligned}[K:\mathbb{Q}(\sqrt{2})]&=[\mathbb{Q}(\sqrt{5},\sqrt{3},\sqrt{2}):\mathbb{Q}(\sqrt{2})]=[\mathbb{Q}(\sqrt{5},\sqrt{3},\sqrt{2}):\mathbb{Q}(\sqrt{3},\sqrt{2})][\mathbb{Q}(\sqrt{3},\sqrt{2}):\mathbb{Q}(\sqrt{2})]\\&=\deg(x^2-5)\deg(x^2-3)=4\end{aligned}$$

이고

$$[K:\mathbb{Q}(\sqrt{2},\sqrt{3})]=[\mathbb{Q}(\sqrt{5},\sqrt{3},\sqrt{2}):\mathbb{Q}(\sqrt{2},\sqrt{3})]=\deg(x^2-5)=2$$

이다.
다음에 **K의 $\mathbb{Q}$-기저 : $\{1,\ \sqrt{2},\ \sqrt{3},\ \sqrt{5},\ \sqrt{2}\sqrt{3},\ \sqrt{2}\sqrt{5},\ \sqrt{3}\sqrt{5},\ \sqrt{2}\sqrt{3}\sqrt{5}\}$이다.**

(2) (예 9.1.15 참조).

$$\begin{aligned}G(K/\mathbb{Q})=\{&id,\ \psi_{\sqrt{2},-\sqrt{2}},\ \psi_{\sqrt{3},-\sqrt{3}},\ \psi_{\sqrt{5},-\sqrt{5}},\ \psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{3},-\sqrt{3}},\\&\psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{5},-\sqrt{5}},\ \psi_{\sqrt{3},-\sqrt{3}}\psi_{\sqrt{5},-\sqrt{5}},\ \psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{3},-\sqrt{3}}\psi_{\sqrt{5},-\sqrt{5}}\}\end{aligned}$$

(3) $G(K/\mathbb{Q})$의 위수는 8이므로 $\mathbb{Z}_8,\ \mathbb{Z}_4\times\mathbb{Z}_2,\ \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,\ D_4,\ Q_8$ 중의 하나와 동형이다. 하지만 항등사상 id를 제외한 모든 원소의 위수는 2이므로 $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$와 동형이다.

9.2.11. $f(x)=x^3-5$의 근은 $\sqrt[3]{5},\ \alpha=\sqrt[3]{5}\dfrac{-1+i\sqrt{3}}{2},\ \beta=\sqrt[5]{5}\dfrac{-1-i\sqrt{3}}{2}$이다.
(1) 분해체 K는 $\mathbb{Q}(\sqrt[3]{5},\alpha,\beta)\subset\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i),\ \mathbb{Q}(\sqrt[3]{5},\alpha)\subset\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i)$은 성립한다.
한편

$$\frac{\alpha}{\sqrt[3]{5}}=\frac{-1+i\sqrt{3}}{2},\quad \frac{\beta}{\sqrt[3]{5}}=\frac{-1-i\sqrt{3}}{2}\quad\Rightarrow\quad \frac{\alpha}{\sqrt[3]{5}}-\frac{\beta}{\sqrt[3]{5}}=\frac{-1+i\sqrt{3}}{2}-\frac{-1-i\sqrt{3}}{2}=i\sqrt{3}$$

이므로

$$i\sqrt{3}\in\mathbb{Q}(\sqrt[3]{5},\alpha,\beta),\quad \sqrt[3]{5}=\alpha/\frac{\beta}{\alpha}\in\mathbb{Q}(\sqrt[3]{5},\alpha,\beta)$$

이므로 $\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i)\subset\mathbb{Q}(\sqrt[3]{5},\alpha,\beta)$이다. 따라서 $\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i)=\mathbb{Q}(\sqrt[3]{5},\alpha,\beta)$이다.

한편

$$\alpha^2=\sqrt[3]{5}\beta\quad\Rightarrow\quad \beta=\alpha^2/\sqrt[3]{5}\in\mathbb{Q}(\sqrt[3]{5},\alpha)$$

이다. 그러므로

$$\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i)=\mathbb{Q}(\sqrt[3]{5},\alpha,\beta)\subset\mathbb{Q}(\sqrt[3]{5},\alpha)\subset\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i)$$

이다. 따라서 $\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i)=\mathbb{Q}(\sqrt[3]{5},\alpha,\beta)=\mathbb{Q}(\sqrt[3]{5},\alpha)$이다.

(별해)

$$\frac{\alpha}{\beta}=\frac{-1-i\sqrt{3}}{2},\quad \frac{\beta}{\alpha}=\frac{-1+i\sqrt{3}}{2}\quad\Rightarrow\quad \frac{\beta}{\alpha}-\frac{\alpha}{\beta}=\frac{-1+i\sqrt{3}}{2}-\frac{-1-i\sqrt{3}}{2}=i\sqrt{3}\in\mathbb{Q}(\sqrt[3]{5},\alpha,\beta)$$

(2) $\alpha,\beta\notin\mathbb{Q}(\sqrt[3]{5})$이므로 따름정리 9.1.4에 의하여 $\mathbb{Q}(\sqrt[3]{5})$의 자기동형사상은 항등사상뿐이다.

(3) 예 9.2.9와 같은 방법으로 구하면 $|G(K/\mathbb{Q})|=6$이다.

$irr(\sqrt[3]{5},\mathbb{Q})=x^3-5,\ irr(\sqrt{3}i,\mathbb{Q}(\sqrt[3]{5}))=x^2+3$이므로

$$[K:\mathbb{Q}]=[\mathbb{Q}\sqrt[3]{5},\mathbb{Q}(\sqrt{3}i):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{5},\mathbb{Q}(\sqrt{3}i):\mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}):\mathbb{Q}]=\deg(x^2+3)\deg(x^3-5)=6$$

이다.

(4) 연습문제 9.1.18번 참조. $irr(\sqrt[3]{5},\mathbb{Q})=x^3-5$의 세 근을 $\sqrt[3]{5},\ \alpha=\sqrt[3]{5}\frac{-1+i\sqrt{3}}{2},\ \beta=\sqrt[3]{5}\frac{-1-i\sqrt{3}}{2}$라 하자.

$$G(\mathbb{Q}(\sqrt[3]{5},i\sqrt{3})/\mathbb{Q})=\{id,\ \Psi_{i\sqrt{3},-i\sqrt{3}},\ \Psi_{\sqrt[3]{5},\alpha}\Psi_{i\sqrt{3},i\sqrt{3}},\ \Psi_{\sqrt[3]{5},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}},\ \Psi_{\sqrt[3]{5},\beta}\Psi_{i\sqrt{3},i\sqrt{3}},\ \Psi_{\sqrt[3]{5},\beta}\Psi_{i\sqrt{3},-i\sqrt{3}}\}$$

의 위수를 구하면 다음과 같다.

원소	id	$\Psi_{i\sqrt{3},-i\sqrt{3}}$	$\Psi_{\sqrt[3]{5},\alpha}\Psi_{i\sqrt{3},i\sqrt{3}}$	$\Psi_{\sqrt[3]{5},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}}$	$\Psi_{\sqrt[3]{5},\beta}\Psi_{i\sqrt{3},i\sqrt{3}}$	$\Psi_{\sqrt[3]{5},\beta}\Psi_{i\sqrt{3},-i\sqrt{3}}$
위수	1	2	3	2	3	2

위수 2인 원소수는 3이다.

(5) (3)에 의하여 $K=\mathbb{Q}(\sqrt[3]{5},i\sqrt{3})$이고 위수가 6이므로 군 $\mathbb{Z}_6$, S_3 중의 하나와 동형이다. 순환군이 아니므로 (4)에 의하여 $G(\mathbb{Q}(\sqrt[3]{5},i\sqrt{3})/\mathbb{Q})\cong S_3$이다.

9.2.12. 연습문제 9.1.18번 참조. $f(x)=x^3+2$의 근은 $-\sqrt[3]{2},\ \alpha=\sqrt[3]{2}\frac{1+i\sqrt{3}}{2},\ \beta=\sqrt[5]{2}\frac{1-i\sqrt{3}}{2}$이므로

$K=S_{\mathbb{Q}}(x^2+2)=\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$이다.

(1) $irr(i\sqrt{3},\mathbb{Q}(\sqrt[3]{2}))=x^2+3$의 두 근 $\pm i\sqrt{3}$은 모두 $\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$에 속하고

$irr(\sqrt[3]{2},\mathbb{Q})=x^3-2$의 세 근 $\sqrt[3]{2},\ \alpha=\sqrt[3]{2}\frac{-1+i\sqrt{3}}{2},\ \beta=\sqrt[3]{2}\frac{-1-i\sqrt{3}}{2}$은 모두 $\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$에 속하므로 따름정리 9.1.4를 이용하면

$$G(\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})/\mathbb{Q})=\{id,\ \Psi_{i\sqrt{3},-i\sqrt{3}},\ \Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},i\sqrt{3}},\ \Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}},\ \Psi_{\sqrt[3]{2},\beta}\Psi_{i\sqrt{3},i\sqrt{3}},\ \Psi_{\sqrt[3]{2},\beta}\Psi_{i\sqrt{3},-i\sqrt{3}}\}$$

원소	id	$\Psi_{i\sqrt{3},-i\sqrt{3}}$	$\Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},i\sqrt{3}}$	$\Psi_{\sqrt[3]{2},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}}$	$\Psi_{\sqrt[3]{2},\beta}\Psi_{i\sqrt{3},i\sqrt{3}}$	$\Psi_{\sqrt[3]{2},\beta}\Psi_{i\sqrt{3},-i\sqrt{3}}$
위수	1	2	3	2	3	2

(2) (1)에서 순환군이 아니므로 $G(K/\mathbb{Q})\cong S_3$이다.

9.2.13. $irr(\sqrt[3]{2}, \mathbb{Q}(i\sqrt{3})) = x^3 - 2$의 세 근 $\sqrt[3]{2}$, $\alpha = \sqrt[3]{2}\dfrac{-1+i\sqrt{3}}{2}$, $\beta = \sqrt[3]{2}\dfrac{-1-i\sqrt{3}}{2}$은 모두 $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$에 속하고 따름정리 9.1.4를 이용하면

$$G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(i\sqrt{3})) = \{id,\ \Psi_{\sqrt[3]{2},\alpha},\ \Psi_{\sqrt[3]{2},\beta}\}$$

이므로 $G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(i\sqrt{3})) \cong \mathbb{Z}_3$이다.

9.2.14. (1) $S_{\mathbb{Q}}(f(x)) = S_{\mathbb{Q}}(x^3 - 10) = \mathbb{Q}\left(\sqrt[3]{10}, \sqrt[3]{10}\dfrac{-1 \pm \sqrt{3}i}{2}\right) = \mathbb{Q}(\sqrt[3]{10}, \sqrt{3}i)$

$irr(i\sqrt{3}, \mathbb{Q}(\sqrt[3]{10})) = x^2 + 3$의 두 근 $\pm i\sqrt{3}$은 모두 $\mathbb{Q}(\sqrt[3]{10}, i\sqrt{3})$에 속하고

$irr(\sqrt[3]{10}, \mathbb{Q}) = x^3 - 10$의 세 근 $\sqrt[3]{10}$, $\alpha = \sqrt[3]{10}\dfrac{-1+i\sqrt{3}}{2}$, $\beta = \sqrt[3]{10}\dfrac{-1-i\sqrt{3}}{2}$은 모두 $\mathbb{Q}(\sqrt[3]{10}, i\sqrt{3})$에 속하므로 따름정리 9.1.4를 이용하면

$$G(\mathbb{Q}(\sqrt[3]{10}, \sqrt{3}i)/\mathbb{Q}) = \{id,\ \Psi_{i\sqrt{3},-i\sqrt{3}},\ \Psi_{\sqrt[3]{10},\alpha}\Psi_{i\sqrt{3},i\sqrt{3}},\ \Psi_{\sqrt[3]{10},\alpha}\Psi_{i\sqrt{3},-i\sqrt{3}},\ \Psi_{\sqrt[3]{10},\beta}\Psi_{i\sqrt{3},i\sqrt{3}},\ \Psi_{\sqrt[3]{10},\beta}\Psi_{i\sqrt{3},-i\sqrt{3}}\}$$

(2) $S_{\mathbb{Q}(\sqrt{3})}(f(x)) = S_{\mathbb{Q}(\sqrt{3})}(x^3 - 10) = \mathbb{Q}(\sqrt{3})\left(\sqrt[3]{10}, \sqrt[3]{10}\dfrac{-1 \pm \sqrt{3}i}{2}\right) = \mathbb{Q}(\sqrt{3})(\sqrt[3]{10}, i)$

$irr(i, \mathbb{Q}(\sqrt{3})(\sqrt[3]{10})) = x^2 + 1$의 두 근 $\pm i$은 모두 $\mathbb{Q}(\sqrt{3})(\sqrt[3]{10}, i)$에 속하고

$irr(\sqrt[3]{10}, \mathbb{Q}(\sqrt{3})) = x^3 - 10$의 세 근 $\sqrt[3]{10}$, $\alpha = \sqrt[3]{10}\dfrac{-1+i\sqrt{3}}{2}$, $\beta = \sqrt[3]{10}\dfrac{-1-i\sqrt{3}}{2}$은 모두 $\mathbb{Q}(\sqrt{3})(\sqrt[3]{10}, i)$에 속하므로

$$G(\mathbb{Q}(\sqrt{3})(\sqrt[3]{10}, i)/\mathbb{Q}(\sqrt{3})) = \{id,\ \Psi_{i,-i},\ \Psi_{\sqrt[3]{10},\alpha}\Psi_{i,i},\ \Psi_{\sqrt[3]{10},\alpha}\Psi_{i,-i},\ \Psi_{\sqrt[3]{10},\beta}\Psi_{i,i},\ \Psi_{\sqrt[3]{10},\beta}\Psi_{i,-i}\}$$

이고 각 원소의 위수는 다음과 같다.

원소	id	$\Psi_{i,-i}$	$\Psi_{\sqrt[3]{10},\alpha}\Psi_{i,i}$	$\Psi_{\sqrt[3]{10},\alpha}\Psi_{i,-i}$	$\Psi_{\sqrt[3]{10},\beta}\Psi_{i,i}$	$\Psi_{\sqrt[3]{10},\beta}\Psi_{i,-i}$
위수	1	2	3	2	3	2

위수 6인 군 $\mathbb{Z}_6$, S_3 중의 하나와 동형이다. 위에서 순환군이 아니므로 $G(\mathbb{Q}(\sqrt{3})(\sqrt[3]{10}, i)/\mathbb{Q}(\sqrt{3})) \cong S_3$이다.

9.2.15.

(1) $p(1) = -1 \neq 0$, $p(-1) = 1 \neq 0$이므로 인수정리와 정리 5.6.4, 따름정리 5.6.9에 의하여 $p(x)$는 $\mathbb{Q}$ 위에서 기약이다.

(2) $p(u^2 - 2) = (u^2 - 2)^3 + (u^2 - 2)^2 - 2(u^2 - 2) - 1 = u^6 - 5u^4 + 6u^2 - 1 = 0$임을 보이자.

u가 $p(x)$의 근이므로 $0 = p(u) = u^3 + u^2 - 2u - 1 \ \Rightarrow\ u^3 = -u^2 + 2u + 1$이다.

$$\begin{cases} u^4 = -u^3 + 2u^2 + u = -(-u^2 + 2u + 1) + 2u^2 + u = 3u^2 - u - 1, \\ u^5 = 3u^3 - u^2 - u = 3(-u^2 + 2u + 1) - u^2 - u = -4u^2 + 5u + 3, \\ u^6 = -4u^3 + 5u^2 + 3u = -4(-u^2 + 2u + 1) + 5u^2 + 3u = 9u^2 - 5u - 4 \end{cases}$$

이므로

$$p(u^2 - 2) = u^6 - 5u^4 + 6u^2 - 1 = (9u^2 - 5u - 4) - 5(3u^2 - u - 1) + 6u^2 - 1 = 0$$

이다. 따라서 $u^2 - 2$는 $p(x)$의 근이다. 근과 계수와의 관계에서

$$u + v + w = -1 \ \Rightarrow\ u + (u^2 - 2) + w = -1 \ \Rightarrow\ w = -u^2 - u - 1$$

이다.

(3) 위 (2)에 의하여 $p(x)$의 근 $u, v, w \in \mathbb{Q}(u)$이므로 $p(x)$의 분해체는

$$K = \mathbb{Q}(u, v, w) = \mathbb{Q}(u)$$

이다. 또한

$$p(x) = irr(u, \mathbb{Q})$$

이므로 $[K : \mathbb{Q}] = 3$이다. 그러므로

$$K = \{a + bu + cu^2 \mid a, b, , c \in \mathbb{Q}\}$$

이다. 그리고 따름정리 9.1.4에 의하여 $G(K/\mathbb{Q}) = G(\mathbb{Q}(u)/\mathbb{Q}) = \{id,\ \Psi_{u,v},\ \Psi_{u,w}\}$이다.

생성원을 구해보자. $\Psi_{u,v}(u) = v = u^2 - 2$이므로

$\Psi_{u,v}^2(u) = \Psi_{u,v}(u^2-2) = v^2-2 = (u^2-2)^2-2 = u^4-4u^2+2 = (3u^2-u-1)-4u^2+2 = -u^2-u+1$

$\Psi_{u,v}^3(u) = \Psi_{u,v}(-u^2-u+1) = -v^2-v+1 = -(u^2-2)^2-(u^2-2)+1 = -(u^4-4u^2+4)-(u^2-2)+1$

$= -((3u^2-u-1)-4u^2+4)-(u^2-2)+1 = u$

이므로 $\Psi_{u,v}$의 위수는 3이다. 따라서

$$G(K/\mathbb{Q}) = G(\mathbb{Q}(u)/\mathbb{Q}) = \{id,\ \Psi_{u,v},\ \Psi_{u,w}\} = \langle \Psi_{u,v} \rangle$$

이므로 $G(K/\mathbb{Q}) \cong \mathbb{Z}_3$이다.

9.2.16. $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$의 기저는 $\{1,\ \sqrt[3]{2},\ \sqrt[3]{2^2},\ \sqrt{3},\ \sqrt[3]{2^2}\sqrt{3},\ \sqrt[3]{2^2}\sqrt{3}\}$이다.

$irr(\sqrt[3]{2}, \mathbb{Q}) = x^3-2$의 대수적 켤레근은 $\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2$ $\left(\text{단, } w = \dfrac{-1+i\sqrt{3}}{2}\right)$이고,

$irr(\sqrt{3}, \mathbb{Q}) = x^2-3$의 대수적 켤레근은 $\sqrt{3}, -\sqrt{3}$이다. 따라서 $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$의 생성원 $\sqrt[3]{2}$, $\sqrt{3}$에 대한 자기동형사상은 다음과 같다.

$$id,\ \psi_{\sqrt[3]{2},\sqrt[3]{2}w},\ \psi_{\sqrt[3]{2},\sqrt[3]{2}w^2},\ \psi_{\sqrt{3},-\sqrt{3}},\ \psi_{\sqrt[3]{2},\sqrt[3]{2}w}\psi_{\sqrt{3},-\sqrt{3}},\ \psi_{\sqrt[3]{2},\sqrt[3]{2}w^2}\psi_{\sqrt{3},-\sqrt{3}}$$

하지만 $w \notin \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$이므로

$$G(\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})/\mathbb{Q}) = \{id,\ \psi_{\sqrt{3},-\sqrt{3}}\} \cong \mathbb{Z}_2$$

9.2.17. (예 9.2.9 참조) 유한 확대체 $F \le E \le K$들의 관계에서 각각의 체가 바로 아래 체의 분해체일 때, 다음이 성립함을 증명하라.

$$|G(K/F)| = |G(K/E)|\,|G(E/F)|$$

$F \le E \le K$이고, E는 F의 분해체이고, K는E의 분해체이므로, $|G(K/F)| = \{E:F\}$이고,
$|G(K/E)| = \{K:E\}$이다(따름정리 9.2.19). 즉, $\{K:E\}\{E:F\} = \{K:F\}$(따름정리 9.2.16)이므로

$$\{K:F\} = |G(K/E)|\,|G(E/F)|$$

이다.

K는 F의 분해체 임을 보이자. 유한 확대체 E가 F의 분해체이므로 다항식 $f(x) \in F[x]$가 존재해서 $f(x)$의 근을 $\alpha_1, \cdots, \alpha_m \in E$라 할 때,

$$S_F(f(x)) = E = F(\alpha_1, \cdots, \alpha_m)$$

이다. 또한 유한 확대체 K가 E의 분해체이므로 다항식 $g(x) \in E[x]$가 존재해서 $g(x)$의 근을 $\beta_1, \cdots, \beta_n \in K$라 할 때, $S_E(g(x)) = K = E(\beta_1, \cdots, \beta_n)$이다. 한편 K는 F의 유한 확대체이므로 대수적 확대체이다. 따라서 임의의 $\beta_i (1 \le i \le n)$은 F 위에서 대수적이다. 그러므로 $p_i(x) = irr(\beta_i, F)$가 존재한다. 그러면 $p_i(x) \in F[x] \subset E[x]$이고 K는 E의 분해체이므로 정리 9.2.18에 의하여 $p_i(x)$의 켤레근은 모두 K의 원소이다. 따라서

$$K = E(\beta_1, \cdots, \beta_n) = F(\alpha_1, \cdots, \alpha_m)(\beta_1, \cdots, \beta_n) = F(\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n)$$

이므로 K는 F의 분해체이다. $|G(K/E)| = \{K:E\}$이다(따름정리 9.2.19). 그러므로 다음이 성립한다.

$$|G(K/F)| = |G(K/E)|\,|G(E/F)|$$

9.2.18. $u \in K-F$에 대하여 $1, u, u^2$은 F위에서 1차종속이고 $K = F(u)$이다.

따라서 모두는 0이 아닌 적당한 $a, b, c \in F$에 대하여 $au^2+bu+c = 0$이다. 여기서 $a = 0$이면, $b \neq 0$이어야 하므로 $u = c/b \in F$가 되어 모순이다.

따라서 $f(x) = ax^2+bx+c \in F[x]$는 2차다항식이고, $f(u) = 0$이다. 한편 $f(x)$의 나머지 근을 v라 하면, $u+v = -b/a \in F$이므로 $v = -b/a-u \in F(u)$이다.

따라서 $K = F(u)$는 $f(x)$의 분해체이다.

9.2.19. $f(0) = 1, f(1) = 2, f(-1) = 2$은 0이 아니므로 정리 5.6.4에 의하여 $\mathbb{Z}_3$ 위에서 기약 다항식이다. $\overline{\mathbb{Z}_3}$에서 $f(x)$의 한 근을 $\alpha \in \overline{\mathbb{Z}_3}$라 하자. 즉, $\alpha^2+1 = 0$, $\alpha^2 = -1$이다. 정리 6.3.13에 의하여 α^3도 $f(x)$의 근이다.

$\alpha^3 = -\alpha$이므로 $\alpha \neq -\alpha$

이다. 따라서 $f(x)$의 분해체는 $\mathbb{Z}_3(\alpha, \alpha^3) = \mathbb{Z}_3(\alpha)$이다.

9.2.20. (1) $f(0) = f(1) = 1 \neq 0$이므로 $\mathbb{Z}_2$ 위에서 기약 다항식이다. $\overline{\mathbb{Z}_2}$에서 $f(x)$의 한 근을 $\alpha \in \overline{\mathbb{Z}_2}$라 하자. 그러면 $\alpha \neq 0, 1$이고 $\alpha^3 + \alpha^2 + 1 = 0$, $\alpha^3 = \alpha^2 + 1$이다. 정리 6.3.13에 의하여 α^2, α^4도 $f(x)$의 근이다.

$$\begin{aligned}
&\alpha = \alpha^2 \;\Rightarrow\; \alpha = 1 (\text{모순}) \;\Rightarrow\; \alpha \neq \alpha^2, \\
&\alpha = \alpha^4 \;\Rightarrow\; \alpha^3 = 1 \;\Rightarrow\; \alpha^2 + 1 = 1 \;\Rightarrow\; \alpha = 0 (\text{모순}) \;\Rightarrow\; \alpha \neq \alpha^4, \\
&\alpha^2 = \alpha^4 \;\Rightarrow\; \alpha^2 = 1 \;\Rightarrow\; \alpha = 1 (\text{모순}) \;\Rightarrow\; \alpha^2 \neq \alpha^4
\end{aligned}$$

따라서 $f(x)$는 $\mathbb{Z}_2(\alpha)$에서 분해된다.

(2) 위 (1)에 의하여 $f(x)$의 분해체 $K = \mathbb{Z}_2(\alpha, \alpha^2, \alpha^4) = \mathbb{Z}_2(\alpha)$이다.
그리고 차원은 $[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = \deg(f) = 3$이다.

9.2.21. (1) 표수가 3이므로

$$\begin{aligned}
f(\alpha+1) &= (\alpha+1)^3 + 2(\alpha+1) + 1 = \alpha^3 + 1 - \alpha - 1 + 1 = \alpha^3 + 2\alpha + 1 = 0, \\
f(\alpha+2) &= (\alpha-1)^3 + 2(\alpha-1) + 1 = \alpha^3 - 1 - \alpha + 1 + 1 = \alpha^3 + 2\alpha + 1 = 0
\end{aligned}$$

이다.

(별해) α가 $f(x)$의 근이므로 $\alpha^3 + 2\alpha + 1 = 0$, $\alpha^3 = \alpha - 1$이다. 정리 6.3.13에 의하여 α^3, α^9도 $f(x)$의 근이다. 표수가 3이므로

$$\begin{aligned}
\alpha^3 &= \alpha - 1 = \alpha + 2, \\
\alpha^9 &= (\alpha^3)^3 = (\alpha - 1)^3 = \alpha^3 - 1 = \alpha - 1 - 1 = \alpha + 1
\end{aligned}$$

따라서 $\alpha+1$, $\alpha+2$도 $f(x)$의 해이다.

(2) 위 (1)에 의하여 $f(x)$는 서로 다른 3개의 해 $\alpha, \alpha+1, \alpha+2$를 가지므로 분해체 $K = \mathbb{Z}_2(\alpha, \alpha+1, \alpha+2) = \mathbb{Z}_2(\alpha)$이다. 그리고 차원은 $[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = \deg(f) = 3$이이다.

9.2.22. (1) $f(x) = x^2 + x + 1$이라 하자. $f(0) = f(1) = 1 \neq 0$이므로 $\mathbb{Z}_2$ 위에서 기약 다항식이다. $\overline{\mathbb{Z}_2}$에서 $f(x)$의 한 근을 $\alpha \in \overline{\mathbb{Z}_2}$라 하자. 그러면 $\alpha \neq 0, 1$이고 $\alpha^2 + \alpha + 1 = 0$, $\alpha^2 = \alpha + 1$이다. 정리 6.3.13에 의하여 α^2도 $f(x)$의 근이다.

$$\alpha = \alpha^2 \;\Rightarrow\; \alpha = 1 (\text{모순}) \;\Rightarrow\; \alpha \neq \alpha^2$$

따라서 α, α^2은 $f(x)$의 근이므로 $f(x)$의 분해체는 $\mathbb{Z}_2(\alpha)$이다. 한편

$$\mathbb{Z}_2(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Z}_2, \alpha^2 = \alpha + 1\} = \mathbb{F}_4$$

이다. 따라서 $\mathbb{F}_4$는 $x^2 + x + 1$의 분해체이다.

(2) 정리 8.4.5에 의하여 $\mathbb{F}_4 = \{\alpha \in \overline{\mathbb{Z}_2} \mid \alpha$는 $x^4 - x$의 근$\}$이므로 $\mathbb{F}_4$는 $f(x) = x^4 - x$의 분해체이다.

(별해) $f(x) = x^4 - x \in \mathbb{Z}_2[x]$라 하자.

$f(x) = x^4 - x = x(x-1)(x^2 + x + 1)$의 0과 1이 아닌 근을 α라 하면 α는 $x^2 + x + 1$의 근이 되므로 (1)에 의하여 $\mathbb{F}_4$는 $f(x) = x^4 - x$의 분해체이다.

== 연습문제 (9.3) ==

9.3.1(1) (연습문제 8.2.13) $\mathbb{Q}(\sqrt[6]{2})$ 또는 $\mathbb{Q}(\sqrt{2}\,\sqrt[3]{2})$

(2) (연습문제 8.2.12) $\mathbb{Q}(\sqrt{2} + \sqrt{3})$

(3) (연습문제 8.2.13) $\mathbb{Q}(i\sqrt[3]{2})$

9.3.2. (1) α가 분리가능이므로 정리 9.3.9에 의하여 $S_F(irr(\alpha,F))=F(\alpha)$는 F의 분리확대체이다. α,β가 F 위에서 분리가능하고 $F<F(\alpha)<F(\alpha,\beta)$, $F<F(\alpha+\beta)<F(\alpha,\beta)$이므로 정리 9.3.13에 의하여 $F(\alpha,\beta)$, $F(\alpha+\beta)$도 F 위에서 분리가능확대체이다. 따라서 $\alpha+\beta$도 F 위에서 분리가능이다.

같은 방법으로 $\alpha\pm\beta,\ \alpha\beta,\ \alpha/\beta(\beta\neq 0)$도 F 위에서 분리가능이다.

(2) 위 (1)에 의하여 F 위에서 분리가능한 E의 모든 원소들의 집합은 E의 부분체이다.

9.3.3. $|E|=p^n$이므로 정리 8.4.5에 의하여 E는 $\mathbb{Z}_p$의 분해체이고, $\forall a\in E,\ a^{p^n}=a$이다. 또한 정리 8.4.18에 의하여 E는 $\mathbb{Z}_p$의 분리확대체이다. 따라서 정리 9.3.9에 의하여 $|G(E/\mathbb{Z}_p)|=[E:\mathbb{Z}_p]=n$이다.

(1)(2) $\sigma_p\in G(E/\mathbb{Z}_p)$이고 $|\sigma_p|=m$이라 하자. $m=n$이면 σ_p는 위수가 n이고 $G(E/\mathbb{Z}_p)$의 생성원이 되어 $G(E/\mathbb{Z}_p)$는 위수가 n인 순환군이다.

E는 유한체이고 위수가 p^n이므로 정리 8.4.12에 의하여 $\exists\alpha\in E,\ E^*=<\alpha>$이다. 그러면

$$|\alpha|=p^n-1\ \Rightarrow\ \alpha^{p^n}=\alpha$$

이다. 또한 $|\sigma_p|=m$이므로

$$\alpha=\sigma_p^m(\alpha)=\alpha^{p^m}\ \Rightarrow\ \alpha^{p^n}=\alpha=\alpha^{p^m}$$

이다. 따라서 $m=n$이다.

9.3.4. 기약다항식 $q(x)$에 대하여 다음이 성립한다.

$q(x)$가 분리가능하지 않다.

$\Leftrightarrow$ $q(x)$는 중근을 갖는다.

$\Leftrightarrow$ $\gcd(q(x),q'(x))\neq 1$ ($\because$ 정리 8.2.25)

$\Leftrightarrow$ $q'(x)=0$ ($\because$ $q(x)$가 기약 다항식)

$\Leftrightarrow$ $q(x)$의 각 항의 지수가 p로 나눠진다.

9.3.5. $[\mathbb{Z}_p(y):\mathbb{Z}_p(y^p)]\leqq p$이다. 이때 $S=\{1,\ y,\ y^2,\ \cdots,\ y^{p-1}\}$가 $\mathbb{Z}_p(y^p)$ 위에서 (최대)1차독립이면 정리 8.1.7에 의하여 S는 $\mathbb{Z}_p(y^p)$ 위에서 기저가 된다. 그러면 $[\mathbb{Z}_p(y):\mathbb{Z}_p(y^p)]=p$가 되고 $irr(y,\mathbb{Z}_p(y^p))=x^p-y^p$이어야 한다. 따라서 S가 1차독립임을 보이자.

적당한 $r_i(y^p),\ s_i(y^p)\in\mathbb{Z}_p[y^p],\ i=0,\ 1,\ 2,\ ,\cdots,\ p-1$가 존재하여

$$\frac{r_0(y^p)}{s_0(y^p)}\cdot 1+\frac{r_1(y^p)}{s_1(y^p)}\cdot y+\frac{r_2(y^p)}{s_{i2(y)}^p}\cdot y^2+\ \cdots\ +\frac{r_{p-1}(y^p)}{s_{p-1}(y^p)}\cdot y^{p-1}=0$$

이라 하자. 분모의 모든 곱을 양변에 곱하면 계수는 모두 $\mathbb{Z}_p[x]$의 계수가 되므로 $s_i(y^p)=1,\ i=0,\ 1,\ 2,\ ,\cdots,\ p-1$이라 해도 좋다. 즉

$$r_0(y^p)\cdot 1+r_1(y^p)\cdot y+r_2(y^p)\cdot y^2+\ \cdots\ +r_{p-1}(y^p)\cdot y^{p-1}=0$$

이다. y의 지수가 p의 배수인 항은 $r_0(y^p)\cdot 1$에만 나타나므로 다항식의 성질(계수비교)에 의하여 $r_0(y^p)=0$이어야 한다. 그러므로

$$r_1(y^p)\cdot y+r_2(y^p)\cdot y^2+\ \cdots\ +r_{p-1}(y^p)\cdot y^{p-1}=0$$

이다. 양변을 y로 나눈 후 같은 방법을 적용하면 $r_i(y^p)=0,\ i=1,\ 2,\ \cdots,\ p-1$이다. 따라서 $S=\{1,\ y,\ y^2,\ \cdots,\ y^{p-1}\}$는 $\mathbb{Z}_p(y^p)$ 위에서 기저가 된다.

9.3.6. $\alpha\in K$가 $g(x)$의 근이면

$$f(\alpha)=d(\alpha)g(\alpha)=d(\alpha)\cdot 0=0$$

이므로 α는 $f(x)$의 근이다.

역으로 $\alpha \in K$가 $f(x)$의 근일 때, 중복도를 m이라 하자. 이 때,

$$f(x) = (x-\alpha)^m h(x),\ h(\alpha) \neq 0$$

인 다항식이 존재한다. 그리고 다음이 성립한다.

$$f'(x) = m(x-\alpha)^{m-1}h(x) + (x-\alpha)^m h'(x)$$

K의 표수는 0이므로 $m \neq 0$이다. 따라서 $h(\alpha) \neq 0$이므로

$$(x-\alpha)^{m-1} | f'(x),\ (x-\alpha)^m \nmid f'(x)$$

이다. 그리고 다음이 성립한다.

$$(x-\alpha)^m | f(x),\ (x-\alpha)^{m-1} | d(x),\ (x-\alpha)^m \nmid d(x)$$

여기서 $f(x) = d(x)g(x)$이므로

$$(x-\alpha) | g(x),\ (x-\alpha)^2 \nmid g(x)$$

이어야만 한다. 따라서 $g(\alpha) = 0$이고 α는 $g(x)$의 단근이다.

== 연습문제 (9.4) ==

9.4.1

(1) $[K:\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3},i):\mathbb{Q}(\sqrt{2},\sqrt{3})][\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]$

$= \deg(x^2+1) \cdot \deg(x^2+2) \cdot \deg(x^2+3) = 2 \cdot 2 \cdot 2 = 8$

($\because x^2+1$의 근이 $\mathbb{Q}(\sqrt{2},\sqrt{3})$에 존재하지 않고, x^2+2의 근이 $\mathbb{Q}(\sqrt{3})$에 존재하지 않는다. x^2+3의 근도 $\mathbb{Q}$에 속하지 않는다.)

(2) $|G(K/\mathbb{Q})| = [K:\mathbb{Q}] = 8$ ($\because K$가 $\mathbb{Q}$의 유한 정규확대체)

(3) $|\Phi(\mathbb{Q})| = |G(K/\mathbb{Q})| = 8$

(4) $|\Phi(\mathbb{Q}(\sqrt{2},\sqrt{3})| = |G(K/\mathbb{Q}(\sqrt{2},\sqrt{3}))| = 2$

(5) $\mathbb{Q}(\sqrt{2},\sqrt{3},i) = \mathbb{Q}(\sqrt{2},\sqrt{6},i)$이므로 $|\Phi(\mathbb{Q}(\sqrt{6})| = |G(K/\mathbb{Q}(\sqrt{6}))| = 4$

(6) $\mathbb{Q}(\sqrt{2},\sqrt{3},i) = \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{6}i)$이므로 $|\Phi(\mathbb{Q}(\sqrt{6}i)| = |G(K/\mathbb{Q}(\sqrt{6}i))| = 4$

9.4.2 $f(x) = x^8 - 1$의 한 해를 $x = e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}} = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{1+i}{\sqrt{2}} = \alpha$라 하자. 그러면 $f(x)$의 분해체는

$$K = S_{\mathbb{Q}}(f(x)) = \mathbb{Q}(\alpha,\alpha^2,\cdots) = \mathbb{Q}(\alpha) = \mathbb{Q}\left(\frac{\sqrt{2}(1+i)}{2}\right)$$
$$= \mathbb{Q}(\sqrt{2}(1+i)) = \mathbb{Q}(\sqrt{2}(1+i),\sqrt{2}(1-i)) = \mathbb{Q}(\sqrt{2},i)$$

이다. $\sqrt{2}$의 켤레근은 $\sqrt{2},-\sqrt{2}$이고 i의 켤레근은 $i,-i$이므로

$$G(K/\mathbb{Q}) = \{id,\ \Psi_{\sqrt{2},-\sqrt{2}},\ \Psi_{i,-i},\ \Psi_{\sqrt{2},-\sqrt{2}}\Psi_{i,-i}\}$$

이다.

9.4.3

(1) $K = S_{\mathbb{Q}}(x^4 - x^2 - 2) = S_{\mathbb{Q}}((x^2-2)(x^2+1)) = \mathbb{Q}(\sqrt{2},i)$

(2) $G(K/\mathbb{Q}) = \{id,\ \Psi_{\sqrt{2},-\sqrt{2}},\ \Psi_{i,-i},\ \Psi_{\sqrt{2},-\sqrt{2}}\Psi_{i,-i}\}$은 개수가 4개 이므로 $\mathbb{Z}_4$ 또는 V와 동형이다. 이 때, 각 원소의 위수가 1, 2, 2, 2이므로 V_4와 동형이다.

(3) $G(K/\mathbb{Q})$의 부분군은

$$G(K/\mathbb{Q}),\ \{id\},\ \{id,\ \Psi_{i,-i}\},\ \{id,\ \Psi_{\sqrt{2},-\sqrt{2}}\},\ \{id,\ \Psi_{i,-i}\Psi_{\sqrt{2},-\sqrt{2}}\}$$

으로 5개 존재한다. 각각은 K의 생성원 1, i, $\sqrt{2}$, $\sqrt{2}i$들 중 고정되는 것이

$G(K/\mathbb{Q})$는 1,

$\{id,\ \Psi_{i,-i}\}$는 1, $\sqrt{2}$,

$\{id,\ \Psi_{\sqrt{2},-\sqrt{2}}\}$는 1, i,

$\{id,\ \Psi_{i,-i}\Psi_{\sqrt{2},-\sqrt{2}}\}$는 $1, \sqrt{2}i,$

$\{id\}$는 $1, i, \sqrt{2}, \sqrt{2}i$

이므로 갈루아 기본정리에 의해 부분체는 5개를 가지며

$$K_{id} = \mathbb{Q}(\sqrt{2}, i),\ K_{\{id,\Psi_{i,-i}\}} = \mathbb{Q}(\sqrt{2}),\ K_{\{id,\Psi_{\sqrt{2},-\sqrt{2}}\}} = \mathbb{Q}(i),\ K_{\{id,\Psi_{i,-i}\Psi_{\sqrt{2},-\sqrt{2}}\}} \equiv \mathbb{Q}(\sqrt{2}i),\ K_{G(K/\mathbb{Q})} = \mathbb{Q}$$

가 된다.

9.4.4

(1) $f(x) = x^4 - 4x^2 - 1$의 해를 구하자. $x^2 = \frac{4 \pm \sqrt{16+4}}{2} = 2 \pm \sqrt{5}$이므로 해는 다음과 같다.

$$x = \pm\sqrt{2 \pm \sqrt{5}} = \pm\sqrt{2+\sqrt{5}},\ \pm\sqrt{\sqrt{5}-2}\,i$$

그러므로 $f(x)$의 분해체 K는 다음과 같다.

$$K = \mathbb{Q}(\pm\sqrt{2+\sqrt{5}},\ \pm\sqrt{\sqrt{5}-2}\,i) = \mathbb{Q}(\alpha, i),\ \text{단},\ \alpha = \sqrt{2+\sqrt{5}},\ \alpha^{-1} = \sqrt{\sqrt{5}-2},$$

(2) α의 대수적 켤레근은 $\pm\alpha,\ \pm\alpha^{-1}i$이고 i의 대수적 켤레근은 $\pm i$이므로 갈루아 군 $G(K/\mathbb{Q}) = \{\sigma_1, \cdots, \sigma_8\}$의 원소는 다음과 같다.

동형사상	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
α의 상	α	$-\alpha$	$\alpha^{-1}i$	$-\alpha^{-1}i$	α	$-\alpha$	$\alpha^{-1}i$	$-\alpha^{-1}i$
i의 상	i	i	i	i	$-i$	$-i$	$-i$	$-i$
σ_i의 위수	1	2	2	2	2	2	4	4

예를 들어 σ_4의 위수는 다음과 같이 구한다. K의 생성원 α, i에 대해서만 계산하면 된다(정리 3.2.25).

$$\sigma_4(\alpha) = -\alpha^{-1}i,$$
$$\sigma_4^2(\alpha) = \sigma_4(-\alpha^{-1}i) = -\sigma_4(\alpha)^{-1}\sigma_4(i) = -(-\alpha^{-1}i)^{-1}i = \alpha i^{-1}i = \alpha(-i)i = \alpha,$$
$$\sigma_4(i) = i$$

이므로 σ_4의 위수는 2이다.

따라서 $G(K/\mathbb{Q})$는 $\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ D_4,\ Q_8$중의 하나와 동형이다. 위수가 4인 원소가 2개이므로

$$G(K/\mathbb{Q}) \cong D_4$$

이다.

9.4.5

(1) ① $\sqrt[4]{8} = \sqrt[4]{2^3} = (\sqrt[4]{2})^3 \in \mathbb{Q}(\sqrt[4]{2})$이므로 $\mathbb{Q}(\sqrt[4]{8}) \subset \mathbb{Q}(\sqrt[4]{2})$

$\sqrt[4]{2} = \frac{(\sqrt[4]{8})^3}{4} \in \mathbb{Q}(\sqrt[4]{8})$이므로 $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{8})$

$\therefore \mathbb{Q}(\sqrt[4]{8}) = \mathbb{Q}(\sqrt[4]{2})$

② $\sqrt[4]{8}\,i = \sqrt[4]{2^3}\,i = -(\sqrt[4]{2}\,i)^3$이므로 $\mathbb{Q}(\sqrt[4]{8}\,i) \subset \mathbb{Q}(\sqrt[4]{2}\,i)$

$\sqrt[4]{2}\,i = -\frac{(\sqrt[4]{8i})^3}{4} \in \mathbb{Q}(\sqrt[4]{8}\,i)$ 이므로 $\mathbb{Q}(\sqrt[4]{2}\,i) \subset \mathbb{Q}(\sqrt[4]{8}\,i)$

$\therefore \mathbb{Q}(\sqrt[4]{8}\,i) = \mathbb{Q}(\sqrt[4]{2}\,i)$

(2) $f(x) = x^4 - 2 = (x^2 + \sqrt{2})(x^2 - \sqrt{2}) = (x + \sqrt[4]{2}\,i)(x - \sqrt[4]{2}\,i)(x + \sqrt[4]{2})(x - \sqrt[4]{2})$의 근은 $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}\,i$이다.

그러면 $f(x)$의 분해체는 $\mathbb{Q}(\sqrt[4]{2}, i)$이고 $\mathbb{Q}(i)$ 위에서 $\mathbb{Q}(\sqrt[4]{2}, i)$의 기저는 $1,\ \sqrt[4]{2},\ \sqrt[4]{2^2},\ \sqrt[4]{2^3}$이다. $\mathbb{Q}(i)$ 위에서 $\mathbb{Q}(\sqrt[4]{2}, i)$의 생성원은 $\sqrt[4]{2}$이고 $irr(\sqrt[4]{2}, \mathbb{Q}(i)) = x^4 - 2$이므로 $\sqrt[4]{2}$의 대수적 켤레근은 $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}\,i$이다. 그러므로 갈로아 군 $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}(i))$은 다음과 같다.

$$G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}(i)) = \{id,\ \Psi_{\sqrt[4]{2},-\sqrt[4]{2}},\ \Psi_{\sqrt[4]{2},\sqrt[4]{2}i},\ \Psi_{\sqrt[4]{2},-\sqrt[4]{2}i}\}$$

(3) 위 (2)를 참조하면 $f(x)$의 분해체는 $\mathbb{Q}(\sqrt[4]{2},i)$이다. $\mathbb{Q}(\sqrt{2})$ 위에서 $\mathbb{Q}(\sqrt[4]{2},i)$의 기저는 1, $\sqrt[4]{2}$, i, $\sqrt[4]{2}i$이다. $\mathbb{Q}(\sqrt{2})$위에서 $\mathbb{Q}(\sqrt[4]{2},i)$의 생성원은 $\sqrt[4]{2}$, i이고 $irr(\sqrt[4]{2},\mathbb{Q}(\sqrt{2}))=x^2-\sqrt{2}$, $irr(i,\mathbb{Q}(\sqrt{2}))=x^2+1$이므로 $\sqrt[4]{2}$의 대수적 켤레근은 $\pm\sqrt[4]{2}$이고 i의 대수적 켤레근은 $\pm i$이다. 그러므로 갈로아 군 $G(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q}(\sqrt{2}))$은 다음과 같다.

$$G(K/\mathbb{Q}(\sqrt{2}))=\{id,\ \Psi_{\sqrt[4]{2},-\sqrt[4]{2}},\ \Psi_{i,-i},\ \Psi_{\sqrt[4]{2},-\sqrt[4]{2}}\Psi_{i,-i}\}$$

(4) x^8-1의 한 근을 $\alpha=e^{\frac{2\pi i}{8}}=\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}=\frac{\sqrt{2}+\sqrt{2}i}{2}$라 하면 $\sqrt[8]{4}$, $\sqrt[8]{4}\alpha$, $\cdots$, $\sqrt[8]{4}\alpha^7$은 x^8-4의 근이다. 이 중에서 $\sqrt[8]{4}\alpha$, $\sqrt[8]{4}\alpha^3$, $\sqrt[8]{4}\alpha^5$, $\sqrt[8]{4}\alpha^7$이 x^4+2의 근이다. 그러므로 x^4+2의 분해체는 $\alpha^2=i$이고 $(\sqrt[4]{2})^2=\sqrt{2}$이므로

$$S_{\mathbb{Q}}(x^4+2)=\mathbb{Q}(\sqrt[8]{4}\alpha,\ \sqrt[8]{4}\alpha^3,\ \sqrt[8]{4}\alpha^5,\ \sqrt[8]{4}\alpha^7)=\mathbb{Q}(\sqrt[4]{2}\alpha,\ -\sqrt[4]{2}\alpha i)=\mathbb{Q}(\sqrt[4]{2}\alpha,i)=\mathbb{Q}(\sqrt[4]{2},i)$$

이다.

9.4.6

$irr(\sqrt[3]{5},\mathbb{Q})=x^3-5$이므로 $\sqrt[3]{5}$의 대수적 켤레원소는 $\sqrt[3]{5},\sqrt[3]{5}w,\sqrt[3]{5}w^2$ $(w=\frac{-1+\sqrt{3}i}{2})$이다. 그러면 $\sqrt[3]{5}$를 포함하는 최소 갈루아 확대체 K는 표수가 0이므로 분리가능(정리 9.3.16)하므로 분해체가 되어야 한다. 따라서

$$K=\mathbb{Q}(\sqrt[3]{5},\sqrt[3]{5}w,\sqrt[3]{5}w^2)=\mathbb{Q}(\sqrt[3]{5},w)=\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i)$$

이다. 그러므로 갈루아 군은

$$G(\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i)/\mathbb{Q})=\{id,\ \Psi_{\sqrt[3]{5},\ \sqrt[3]{5}w},\ \Psi_{\sqrt[3]{5},\sqrt[3]{5}w^2},\ \Psi_{\sqrt{3}i,-\sqrt{3}i},\ \Psi_{\sqrt[3]{5},\sqrt[3]{5}w}\Psi_{\sqrt{3}i,-\sqrt{3}i},\ \Psi_{\sqrt[3]{5},\sqrt[3]{5}w^2}\Psi_{\sqrt{3}i,-\sqrt{3}i}\}$$

이다. 갈루아 군의 위수는 $|\mathbb{Q}(\sqrt[3]{5},\sqrt{3}i)|=6$이므로 $\mathbb{Z}_6$, D_3 중의 하나와 동형이다. 각 원소의 위수는 1,3,3,2,2,2이므로 D_3와 동형이다. 그러므로 부분군은 위수가 1인 것이 1개, 2인 것이 3개, 3인 것이 1개, 6인 것이 1개로 모두 6개이다(예 2.4.18).

9.4.7

(1) $K=\mathbb{F}_{p^8}$는 $\mathbb{Z}_p$의 유한확대체이므로 갈루아확대체이다.

$$|G(K/\mathbb{Z}_p)|=[K:\mathbb{Z}_p]=2^3$$

이고 정리 9.4.14에 의하여 $G(K/\mathbb{Z}_p)=\langle\sigma_p\rangle$(단, $|\sigma_p|=8$)는 위수 8인 순환군이다. 따라서 라그랑주 정리와 정리 2.3.11에 의해 위수가 1, 2, 4, 8인 부분군

$$\langle\sigma_p^8=id\rangle,\ \langle\sigma_p^4\rangle,\ \langle\sigma_p^2\rangle,\ \langle\sigma_p\rangle$$

이 하나씩만 존재한다.

(2) 위 (1)에 의하여 갈루아 기본정리에 의하여 K의 모든 부분체는 다음과 같다(예 9.4.15 참조).

$$K_{\langle\sigma_p^8=id\rangle}=\mathbb{F}_{p^8},\ K_{\langle\sigma_p^4\rangle}=\mathbb{F}_{p^4},\ K_{\langle\sigma_p^2\rangle}=\mathbb{F}_{p^2},\ K_{\langle\sigma_p\rangle}=\mathbb{F}_p=\mathbb{Z}_p$$

9.4.8

$K=\mathbb{F}_{2^{30}}$ 라 하자. $[\mathbb{F}_{2^{30}}:\mathbb{F}_2]=30$ 이므로 $G(K/\mathbb{F}_2)=<\sigma_2>\cong(\mathbb{Z}_{30},+)$ (단, $|\sigma_2|=30$)이다(정리 9.4.14).

라그랑주 정리와 정리 2.3.11에 의해 30의 약수 1, 2, 3, 5, 6, 10, 15, 30에 대해 대응하는 부분군

$$\langle\sigma_2\rangle=G(\mathbb{F}_{2^{30}}/\mathbb{F}_2),\ \langle\sigma_2^2\rangle,\ \langle\sigma_2^3\rangle,\ \langle\sigma_2^5\rangle,\ \langle\sigma_2^6\rangle,\ \langle\sigma_2^{10}\rangle,\ \langle\sigma_2^{15}\rangle,\ \langle\sigma_2^{30}\rangle=\langle id\rangle$$

이 하나씩 존재한다. 따라서 이 부분군의 고정체는 다음과 같다.

$$K_{\langle\sigma_2\rangle}=\mathbb{F}_2,\ K_{\langle\sigma_2^2\rangle}=\mathbb{F}_{2^2},\ K_{\langle\sigma_2^3\rangle}=\mathbb{F}_{2^3},\ K_{\langle\sigma_2^5\rangle}=\mathbb{F}_{2^5},\ K_{\langle\sigma_2^6\rangle}=\mathbb{F}_{2^6},\ K_{\langle\sigma_2^{10}\rangle}=\mathbb{F}_{2^{10}},\ K_{\langle\sigma_2^{15}\rangle}=\mathbb{F}_{2^{15}},\ K_{\{id\}}=\mathbb{F}_{2^{30}}$$

9.4.9 위수가 256이므로 표수가 2이다.

$K=\mathbb{F}_{2^8}$ 라 하자. $[\mathbb{F}_{2^8}:\mathbb{F}_2]=8$ 이므로 $G(K/\mathbb{F}_2)=<\sigma_2>\cong(\mathbb{Z}_8,+)$ (단, $|\sigma_2|=8$)이다(정리 9.4.14).

라그랑주 정리와 정리 2.3.11에 의해 8의 약수 1, 2, 4, 8에 대해 대응하는 부분군

$$\langle \sigma_2 \rangle = G(\mathbb{F}_{2^8}/\mathbb{F}_2),\ \langle \sigma_2^2 \rangle,\ \langle \sigma_2^4 \rangle,\ \langle \sigma_2^8 \rangle = \langle id \rangle$$

이 하나씩 존재한다. 따라서 이 부분군의 고정체는 다음과 같다.

$$K_{\langle \sigma_2 \rangle} = \mathbb{F}_2,\ K_{\langle \sigma_2^2 \rangle} = \mathbb{F}_{2^2},\ K_{\langle \sigma_2^4 \rangle} = \mathbb{F}_{2^4},\ K_{\{id\}} = \mathbb{F}_{2^8}$$

9.4.10 (1) $G(K/F)$는 순환군이고 $G(K/E) < G(K/F)$이므로 $G(K/E)$는 순환군이다(정리 2.3.5). 그러므로 K는 E의 순환확대체이다.

다음에 E는 F의 정규확대체이므로 $G(E/F) \cong \dfrac{G(K/F)}{G(K/E)}$이다(정리 9.4.11). 순환군의 잉여군은 순환군이므로 $G(E/F)$는 순환군이다. 따라서 E는 K의 순환확대체이다.

(2) 갈루아 기본정리에 의하여 갈루아 군 $G(K/F)$의 부분군 H와 K의 중간체 K_H는 1대1대응이다. $G(K/F)$는 순환군이므로 정리 2.3.11에 의하여 위수 d인 부분군이 유일하게 존재하므로 $[K_H : F] = d$인 중간체(정리 9.4.11)도 유일하게 존재한다.

(3) $G(K/F)$는 위수 10인 순환군이므로 정리 2.3.11에 의해 위수가 1, 2, 5, 10인 부분군 4개가 존재하므로 중간체는 4개가 존재한다.

9.4.11 $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(\sqrt{3})$ (연습문제 7.3.9)이다. 하지만

$$G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id, \Psi_{\sqrt{2},-\sqrt{2}}\} \cong \mathbb{Z}_2 \cong G(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \{id, \Psi_{\sqrt{3},-\sqrt{3}}\}$$

이므로 $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong G(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$이다.

9.4.12 (1) $charF = 0$ or $p\ (p|n)$라 하자.

α가 단위원의 원시 n제곱근이므로 $|\alpha| = n$ 이고 $x^n - 1 \in F[x]$의 근이다.

$f(x) = x^n - 1$의 근은 $1, \alpha, \cdots, \alpha^{n-1}$(정리 8.4.11)이고 $|\alpha| = n$이므로 $\alpha^i \neq \alpha^j\ (1 \leqq i \neq j \leqq n)$이다.

그러므로 $f(x)$는 F의 분리다항식이다.

다음에 $irr(\alpha, F) | x^n - 1$이므로 $irr(\alpha, F)$도 분리다항식이다.

$F(\alpha) = S_F(f(x))$이고 $irr(\alpha, F)$가 분리다항식이므로 $F(\alpha)$는 F의 분리확대체이다(정리 9.3.9).

그러므로 $F(\alpha)$는 정규확대체이다.

(2) $1 \leq \deg(\alpha, F) = m < n$이다. $irr(\alpha, F) | x^n - 1$이므로 α의 서로 다른 m개의 켤레근은

$$\alpha = \alpha^{a_1},\ \alpha^{a_2},\ \cdots,\ \alpha^{a_m},\quad a_1 = 1 \leqq a_2,\ \cdots,\ a_m < n$$

이다. 따라서

$$G(F(\alpha)/F) = \{\Psi_{\alpha, \alpha^{a_i}} | 1 \leqq i \leqq m\}$$

이다. 그러면 $\forall \Psi_{\alpha, \alpha^{a_i}},\ \Psi_{\alpha, \alpha^{a_j}} \in G(F(\alpha)/F)$에 대하여

$$\Psi_{\alpha, \alpha^{a_i}} \circ \Psi_{\alpha, \alpha^{a_j}}(\alpha) = \alpha^{a_i a_j} = (\alpha^{a_j})^{a_i} = \Psi_{\alpha, \alpha^{a_j}} \circ \Psi_{\alpha, \alpha^{a_i}}(\alpha)$$

이므로 $G(F(\alpha)/F)$는 가환군이다.

9.4.13

(1) K가 F의 유한 정규확대체이므로 $a_1, \cdots, a_n \in K$가 존재하여 $K = F(a_1, \cdots, a_n)$이고 $K_{G(K/F)} = F$ 이다. 즉, K는 F의 갈루아확대체이다.

$$\forall \sigma \in G(K/F)\ \ \sigma : K \to K,\quad \bar{\tau} : K[x] \to K[x]\quad \bar{\tau}(g(x)) = g_\sigma(x)$$

$$g(x) = b_0 + b_1 x + \cdots + b_m x^m,\ \ g_\sigma(x) = \sigma(b_0) + \sigma(b_1)x + \cdots + \sigma(b_m)x^m$$

이라 정의하면 $\bar{\tau}$는 동형사상이다(정리 9.2.11).

$\forall \tau \in G(K/F)$에 대하여 $\{a_1, \cdots, a_n\} = \{\tau(a_1), \cdots, \tau(a_n)\}$이고, 임의의 $c \in F$에 대하여 $f(c) = c$이다. 또한 $G(K/F) = \tau G(K/F)$이므로

$$\bar{\tau}(f(x))=\bar{\tau}\left(\prod_{\sigma\in G(K/F)}(x-\sigma(\alpha))\right)=\prod_{\sigma\in G(K/F)}(x-\tau(\sigma(\alpha)))=f(x)$$

이다. 그러므로 $f(x)=\prod_{\sigma\in G(K/F)}(x-\sigma(\alpha))=h_0(a_1,\cdots,a_n)+h_{1(a_1},\cdots,a_n)x+\cdots+h_m(a_1,\cdots,a_n)x^m\in K[x]$의 각 항의 계수 $h_i(a_1,\cdots,a_n)\in K$에 대하여

$$\tau(h_i(a_1,\cdots,a_n))=h_i(a_1,\cdots,a_n)$$

이다. 따라서 $f(x)$는 F 계수 다항식이어야 한다.

(예를 들어, $f(x)$의 1차항 x의 계수는 $G(K/F)=\{\sigma_1,\ \cdots,\ \sigma_r\}$일 때, $-(\sigma_1(\alpha)+\cdots+\sigma_r(\alpha))$이다. 그러면 임의의 $\tau\in G(K/F)$에 대하여 $G(K/F)=\tau G(K/F)=\{\tau(\sigma_1),\ \cdots,\ \tau(\sigma_r)\}$이므로(정리 2.1.10 군의 소약율))

$$\tau(-(\sigma_1(\alpha)+\cdots+\sigma_r(\alpha)))=-(\tau(\sigma_1(\alpha))+\cdots+\tau(\sigma_r(\alpha)))=-(\sigma_1(\alpha)+\cdots+\sigma_r(\alpha))$$

이다. 따라서 $-(\sigma_1(\alpha)+\cdots+\sigma_r(\alpha))\in F$이다.)

(2) 따름정리 9.1.4에 의하여 $\sigma\in G(K/F)$에 대하여 $\sigma(\alpha)$는 α의 켤레이다. 그리고 $f(\alpha)=\prod_{\sigma\in G(K/F)}(\alpha-\sigma(\alpha))=0$이므로 $p(x)=irr(\alpha,F)|f(x)$이다. 위 (1)에 의하여 $f(x)\in F[x]$이고, $p(x)|f(x)$이므로 적당한 $g_1(x)\in F[x]$가 존재하여

$$f(x)=p(x)g_1(x)$$

이다. $g_1(x)\notin F$이면 $g_1(x)$는 α의 켤레를 한 근 $\sigma(\alpha)$으로 가지므로 $p(x)=irr(\sigma(\alpha),F)$이다. 그러므로 적당한 $g_2(x)\in F[x]$가 존재하여 $g_1(x)=p(x)g_2(x)$이다. 따라서

$$f(x)=p(x)^2g_2(x)$$

위와 같은 방법을 계속하면 적당한 $c\in F$와 $s\in\mathbb{N}$가 존재하여

$$f(x)=p(x)^sc$$

가 된다. $f(x)$와 $p(x)$는 모닉이므로 $c=1$이어야 한다. 따라서

$$f(x)=p(x)^s$$

이다.

(3) $f(x)=irr(\alpha,F)$

$\Leftrightarrow\ [F(\alpha):F]=\deg(\alpha,F)=\deg(f(x))=|G(K/F)|=[K:F]$

$\Leftrightarrow\ [F(\alpha):F]=[K:F]$

$\Leftrightarrow\ [K:F(\alpha)]=1\ (\because [K:F]=[K:F(\alpha)][F(\alpha):F])$

$\Leftrightarrow\ K=F(\alpha)$

9.4.14 $f(x)$의 n개의 근은 $\alpha_1,\ \cdots,\ \alpha_n$이다.

(1) ($\Longrightarrow$) $\Delta(f)=0$이면 $\alpha_i=\alpha_j\ (i\neq j)$이다. 그러면 $irr(\alpha_i,F)=irr(\alpha_j,F)$이고 $f(x)$가 분리 가능이므로 $f(x)$의 기약 다항식 인수는 중근을 가질 수 없다. 따라서 $f(x)$는 $irr(\alpha_i,F)^2$을 인수로 가져야 한다.

($\Longleftarrow$) 중근을 가지므로 분명히 성립한다.

(2) $\forall\sigma\in G(K/F)$에 대하여 α_i와 $\sigma(\alpha_i)$는 켤레 관계이므로

$$\sigma((\Delta(f))^2)=\sigma\left(\left(\prod_{i<j}(\alpha_i-\alpha_j)\right)^2\right)=\left(\prod_{i<j}\sigma(\alpha_i-\alpha_j)\right)^2=\left(\prod_{i<j}(\sigma(\alpha_i)-\sigma(\alpha_j))\right)^2=(\Delta(f))^2$$

이다. 따라서 $\sigma(\Delta f^2)=(\Delta f)^2$이므로 $(\Delta f)^2\in F$이다.

(3) $\tau=(ij)\in G(K/F)$는 첨자의 위치를 바꾸는 호환이라 할 때

① $k<i<j$

$$\tau(\alpha_k-\alpha_i)(a_i-a_j)(a_k-a_j)=(\alpha_k-\alpha_j)(a_j-a_i)(a_k-a_j)=-(\alpha_k-\alpha_i)(a_i-a_j)(a_k-a_j)$$

② $i<k<j$

$$\tau(a_i-a_k)(\alpha_k-\alpha_j)(a_i-a_j)=(a_j-a_k)(\alpha_k-\alpha_i)(a_j-a_i)=-(a_i-a_k)(\alpha_k-\alpha_j)(a_i-a_j)$$

③ $i<j<k$

$$\tau(a_i-a_j)(a_j-a_k)(a_i-a_k)=(a_j-a_i)(a_i-a_k)(a_j-a_k)=-(a_i-a_j)(a_j-a_k)(a_i-a_k)$$

이므로 $\tau(\Delta f)=-\Delta f$이다.

그러므로 $\Delta(f)\in F$이면 임의의 $\sigma\in G(K/F)$에 대하여 $\sigma(\Delta(f))=\Delta(f)$일 필요충분조건은 σ가 우치환이 되어야 한다. 즉, $\sigma\in A_n$이다.

9.4.15

(1) $\alpha\in\mathbb{Q}(\alpha)$이고 $\alpha^{-1}\in\mathbb{Q}(\alpha)$이므로 $\alpha+\alpha^{-1}\in\mathbb{Q}(\alpha)$이다. 따라서 $\mathbb{Q}(\alpha+\alpha^{-1})<\mathbb{Q}(\alpha)$이다.

(2) $\sigma^2(\alpha)=\sigma(\alpha^{-1})=(\sigma^{-1})^{-1}=\alpha$이므로 $|\alpha|=2$이다.

(3) $\sigma(\alpha+\alpha^{-1})=\sigma(\alpha)+\sigma(\alpha^{-1})=\alpha^{-1}+\alpha$이므로 $\alpha+\alpha^{-1}$은 σ에 의해 고정된다.

(4) $|\alpha|=2$ 이므로 $|K_{\{\sigma\}}|=50$이다. 따라서 $[K:K_{\{\sigma\}}]=2$이다.

(5) $[K:F]=\deg(\alpha,\mathbb{Q}(\alpha+\alpha^{-1}))\leqq\deg(x^2-(\alpha+\alpha^{-1})x+1)=2$

($\because x^2-(\alpha+\alpha^{-1})x+1$은 기약인지 모른다.)

(6) $F=\mathbb{Q}(\alpha+\alpha^{-1})\subseteq K_{\{\sigma\}}$ ($\because$ (3))

$$2\geq[K:F]=[K:K_{\{\sigma\}}][K_{\{\sigma\}}:F]=2[K_{\{\sigma\}}:F]$$

이므로 $[K_{\{\sigma\}}:F]=1$이다. 즉, $K_{\{\sigma\}}=F$이다.

(7) $100=[K:\mathbb{Q}]=[K:K_{\{\sigma\}}][K_{\{\sigma\}}:\mathbb{Q}]=[K:K_{\{\sigma\}}][F:\mathbb{Q}]=2[F:\mathbb{Q}]$이므로 $[F:\mathbb{Q}]=50$이다.

== 연습문제 (9.5) ==

9.5.1.

$x^8-1=\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)$이고,

$$\Phi_1(x)=x-1,\ \Phi_2(x)=\frac{x^2-1}{x-1},\ \Phi_4(x)=\frac{x^4-1}{(x-1)(x^2-1)}=x^2+1$$

이다. 따라서 $x^8-1=(x-1)(x+1)(x^2+1)\Phi_8(x)$이므로 $\Phi_8(x)=x^4+1$이다.

9.5.2. $\phi(12)=\phi(2^2)\phi(3)=4$이므로 $\Phi_{12}(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$이다.

$x^{12}-1$의 원시 12제곱근을 $\alpha=e^{\frac{\pi}{6}i}=\frac{\sqrt{3}}{2}+\frac{1}{2}i$라 하자. 그럼 원시 12제곱근은 모두 $\alpha,\alpha^5,\alpha^7,\alpha^{11}$이다.

그러므로 $\Phi_{12}(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)=x^4-x^2+1$이 된다.

(별해) 예 9.5.8을 참조하면

$$\begin{aligned}x^{12}-1&=\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x)\\&=(x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)\Phi_{12}(x)\\&=(x^4-1)(x^4+x^2+1)\Phi_{12}(x)\\&=(x^8+x^6-x^2-1)\Phi_{12}(x)\end{aligned}$$

이다. 다항식의 나눗셈을 이용하면 $\Phi_{12}(x)=x^4-x^2+1$이다.

다음에 $\Phi_{12}(x)=x^4-x^2+1$가 $\mathbb{Q}$ 위에서 기약다항식임을 보이자.

$\Phi_{12}(1)=\Phi_{12}(-1)=1\neq0$이므로 1차 인수가 존재하지 않는다(따름정리 5.6.9).

그리고 $\Phi_{12}(x)=(x^2+ax+b)(x^2+cx+d)$ $a,b,c,d\in\mathbb{Z}$라 하자(정리 5.6.7).

정리하면 $a+c=0,\ ac+b+d=-1,\ ad+bc=0,\ bd=1$이 된다.

그러므로 $b=d=1$이거나 $b=d=-1$이다.

i) $b=d=1$인 경우. $c^2=3$가 되어 $c\notin\mathbb{Z}$가 되어 모순이다.

ii) $b=d=-1$인 경우. $c^2=-1$이 되어 $c\notin\mathbb{Z}$가 되어 모순이다.
따라서 $\Phi_{12}(x)$는 2차인수를 갖지 않는다. 그러므로 $\Phi_{12}(x)$는 $\mathbb{Q}$위에서 기약이다.

9.5.3. (1) x^7-1의 한 근을 $\alpha=e^{\frac{2\pi i}{7}}$이라 하자.
그러면 x^7-1의 근은 $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$이다. α는 $\Phi_7(x)=x^6+x^5+\cdots+x+1$의 근이고, $\mathbb{Q}$ 위에서 기약이다(정리 9.5.4). 그러므로 $irr(\alpha,\mathbb{Q})=\Phi_7(x)$이고 x^7-1의 분해체는 $K=\mathbb{Q}(\alpha)$이다. 표수가 0이므로 분해체는 갈루아 확대체이다(정리 9.5.9). 따라서

$$[K:\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg(\alpha,\mathbb{Q})=6$$

이다.
(2) 위 (1)에 의하여 x^7-1의 분해체는 $K=\mathbb{Q}(\alpha)$이고 α^3이 α의 켤레근이므로 $\sigma_3\in G(K/\mathbb{Q})$, $\sigma_3(\alpha)=\alpha^3$이라 하고 $\alpha^7=1$을 이용하면

$$\sigma_3^2(\alpha)=\sigma_3(\alpha^3)=\alpha^9=\alpha^2,$$
$$\sigma_3^3(\alpha)=\sigma_3(\alpha^2)=\alpha^6$$

이므로 $|\sigma_3|=6$이다. 따라서 $G(K/\mathbb{Q})$는 생성원 σ_3을 갖는 순환군이다.

9.5.4. x^p-1의 원시근을 $\alpha=e^{\frac{2\pi i}{p}}$라 하면, x^p-1의 근은 $1, \alpha, \alpha^2, \cdots, \alpha^{p-1}$이다. 그러므로 분해체는 $K=\mathbb{Q}(\alpha)$이고 $irr(\alpha,\mathbb{Q})=x^{p-1}+\cdots+x+1$(정리 5.6.17)이다. 따라서

$$[K:\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg(\alpha,\mathbb{Q})=p-1$$

이다. 다음에 다항식 $x^{p-1}+\cdots+x+1$은 $\alpha, \cdots, \alpha^{p-1}$을 해로 가지므로 α의 켤레원소는 $\alpha, \alpha^2, \cdots, \alpha^{p-1}$이다.
따라서 $G(K/\mathbb{Q})=\{\psi_{\alpha,\alpha^i}|1\le i\le p-1\}$이다.

9.5.5. x^6-1의 한 해를 $\alpha=e^{\frac{2\pi i}{6}}=\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}=\frac{1}{2}+i\frac{\sqrt{3}}{2}$라 하면, x^6-1의 근은 $1, \alpha, \alpha^2, \cdots, \alpha^{p-1}$이다. 그러므로 분해체는

$$K=\mathbb{Q}(\alpha)=\mathbb{Q}\left(\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)=\mathbb{Q}(\sqrt{3}i)$$

이고 $irr(\sqrt{3}i,\mathbb{Q})=x^2+3$이다. 따라서 다음이 성립한다.

$$[K:\mathbb{Q}]=[\mathbb{Q}(\sqrt{3}i):\mathbb{Q}]=\deg(x^2+3)=2$$

9.5.6. 1의 원시 6제곱을 $\alpha=e^{\frac{2\pi i}{6}}=\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}=\frac{1}{2}+i\frac{\sqrt{3}}{2}$라 하면, x^6-2의 해는 $\sqrt[6]{2}, \sqrt[6]{2}\alpha, \cdots, \sqrt[6]{2}\alpha^5$이다(정리 9.5.13). 이 때 $\alpha^3=-1$이다.

$$E=\mathbb{Q}(\sqrt[6]{2}, \sqrt[6]{2}\alpha, \cdots, \sqrt[6]{2}\alpha^5)=\mathbb{Q}(\sqrt[6]{2}, \alpha, \cdots, \alpha^5)$$
$$=\mathbb{Q}(\sqrt[6]{2}, \alpha)=\mathbb{Q}(\sqrt[6]{2}, \sqrt{3}i)$$

이다. 다음에

$$irr(\sqrt[6]{2},\mathbb{Q})=x^6-2$$
$$irr(\sqrt{3}i,\mathbb{Q})=x^2+3$$

이므로 $\sqrt[6]{2}$의 켤레근은 6개이고, $\sqrt{3}i$의 켤레근은 2개이다. 따라서 $|G(K/\mathbb{Q})|=12$이다.
(별해) E의 기저를 구해보면

$$\{1, \sqrt[6]{2}, \sqrt[6]{2^2}, \cdots \sqrt[6]{2^5}, \alpha, \sqrt[6]{2}\alpha, \sqrt[6]{2^2}\alpha, \cdots \sqrt[6]{2^5}\alpha\}$$

인 12개의 원소를 갖는다. 또한 E는 $\mathbb{Q}$의 갈루아 확대체이므로

$$|G(E/\mathbb{Q})|=[E:\mathbb{Q}]=12$$

이다.

9.5.7. $f(x) = x^6 - 1$
$= (x^3+1)(x^3-1)$
$= (x+1)(x^2-x+1)(x-1)(x^2+x+1)$
$= (x+1)(x^2+2x+1)(x-1)(x^2-2x+1)$
$= (x+1)^3(x-1)^3$

그러므로 분해체 $K = \mathbb{Z}_3(1,-1) = \mathbb{Z}_3$이므로 $|K| = |\mathbb{Z}_3| = 3$이다.

9.5.8. 1의 원시 nm-제곱근 $\alpha = e^{\frac{2\pi i}{mn}}$이라 하면 $x^{mn}-1$의 근은 $1, \alpha, \cdots, \alpha^{mn-1}$이다.

따라서 $x^{mn}-1$의 분해체는 다음과 같다.

$$S_{\mathbb{Q}}(x^{nm}-1) = \mathbb{Q}(\alpha,\cdots,\alpha^{nm}) = \mathbb{Q}(\alpha)$$

다음에 1의 원시 m-제곱근과 원시 n-제곱근을 각각 $\beta = e^{\frac{2\pi i}{m}}, \gamma = e^{\frac{2\pi i}{n}}$이라 하면 $(x^m-1)(x^n-1)$의 근은 $1, \beta, \cdots, \beta^{m-1}, \gamma, \cdots, \gamma^{n-1}$이다. 그러므로 $(x^m-1)(x^n-1)$의 분해체는

$$S_{\mathbb{Q}}\{(x^n-1)(x^m-1)\} = \mathbb{Q}(\beta,\gamma)$$

이다. 이 때 $\beta = \alpha^n$, $\gamma = \alpha^m$이므로

$$\mathbb{Q}(\beta,\gamma) \subset \mathbb{Q}(\alpha)$$

이다. 또한 $\gcd(m,n) = 1$이므로 $\exists\, x,y \in \mathbb{Z}, mx + ny = 1$이다. 그러면

$$\alpha = e^{\frac{2\pi i}{nm}} = e^{\frac{2\pi i}{nm}(mx+ny)} = e^{\frac{2\pi i}{n}x + \frac{2\pi i}{m}y} = e^{\frac{2\pi i}{n}x} e^{\frac{2\pi i}{m}y} = \gamma^x \beta^y \in \mathbb{Q}(\beta,\alpha)$$

가 성립한다. 따라서 $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta,\gamma)$이다. 그러므로 $S_{\mathbb{Q}}(x^{nm}-1) = S_{\mathbb{Q}}\{(x^n-1)(x^m-1)\}$이다.

9.5.9.

(1) 1의 원시 12-제곱근근을 $\alpha = e^{\frac{2\pi i}{12}} = \cos\frac{\pi}{6} + i\sin\frac{\pi}{6} = \frac{\sqrt{3}}{2} + i\frac{1}{2}$라 하면 $x^{12}-1$의 근은 $1, \alpha, \cdots, \alpha^{11}$이다.

한편 $2\alpha = \sqrt{3}+i$, $\alpha^{-1} = \sqrt{3}-i$이므로 $x^{12}-1$의 분해체는

$$K = S_{\mathbb{Q}}(x^{12}-1) = \mathbb{Q}(1, \alpha, \cdots, \alpha^{12}) = \mathbb{Q}(\alpha) = \mathbb{Q}\left(\frac{\sqrt{3}}{2} + i\frac{1}{2}\right) = \mathbb{Q}(\sqrt{3}, i)$$

이다. 그러므로

$$[K:\mathbb{Q}] = [\mathbb{Q}(\sqrt{3},i):\mathbb{Q}] = [\mathbb{Q}(\sqrt{3},i):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = \deg(x^2+1)\deg(x^2-3) = 4$$

이다.

(2) $\sigma \in G(\mathbb{Q}(\sqrt{3},i)/\mathbb{Q})$이라 하자.

$irr(\sqrt{3}, \mathbb{Q}) = x^2 - 3$
$irr(i, \mathbb{Q}) = x^2 + 1$

이므로 $\sqrt{3}$의 대수적 켤레원소는 $\pm\sqrt{3}$이고, i의 대수적 켤레원소는 $\pm i$이다. 그러므로 갈루아 군은

$$G(K/\mathbb{Q}) = \{\sigma_1 = id,\ \sigma_2 = \psi_{\sqrt{3},-\sqrt{3}},\ \sigma_3 = \psi_{i,-i},\ \sigma_4 = \sigma_2\sigma_3\}$$

이다. 임의의 $\sigma \in G(K/\mathbb{Q})$에 대하여 σ^2은 항등사상임을 보이자.

$\sigma_1{}^2 = id,$
$\sigma_2{}^2(\sqrt{3}) = \sigma_2(-\sqrt{3}) = \sqrt{3},\ \sigma_2(i) = i,$
$\sigma_3(\sqrt{3}) = \sqrt{3},\ \sigma_3^2(i) = \sigma_3(-i) = i$
$\sigma_4{}^2(\sqrt{3}) = \sigma_4(-\sqrt{3}) = \sqrt{3},\ \sigma_4{}^2(i) = \sigma_4(-i) = i$

이므로 σ^2은 항상 항등사상이다.

(3) 위 (1), (2)에 의해서 $\forall\, \sigma \in G(K/\mathbb{Q}), |\sigma| \leqq 2$이므로 $G(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$이다.

9.5.10. (1) 1의 원시 20-제곱근을 $\alpha = e^{\frac{2\pi i}{20}}$라 하면 $x^{20}-1$의 근은 $1, \alpha, \cdots, \alpha^{19}$이므로, $x^{20}-1$의분해체는

$$S_{\mathbb{Q}}(x^{20}-1) = \mathbb{Q}(1, \alpha, \cdots, \alpha^{19}) = \mathbb{Q}(\alpha)$$

이다. α의 위수가 20이다. 정리 8.4.11에 의하여 1의 원시 20-제곱근은 $\phi(20)=8$개 존재하고 다음과 같다.

$$\{\alpha^i | \gcd(n,i)=1, 1 \le i \le 19\} = \{\alpha^1, \alpha^3, \alpha^7, \alpha^9, \alpha^{11}, \alpha^{13}, \alpha^{17}, \alpha^{19}\}$$

$G(K/\mathbb{Q})$의 모든 원소는 α의 켤레근이므로 원시 20-제곱근이다. 따라서

$$G(K/\mathbb{Q}) = \{\psi_{\alpha,\alpha^i} | \gcd(n,i)=1, 1 \le i \le 19\}$$

이다.

(2) 1의 원시 4-제곱근을 $\beta = e^{\frac{2\pi i}{4}} = i$라 하면 x^4-5의 근은 $\sqrt[4]{5}, \sqrt[4]{5}\,\beta, \cdots, \sqrt[4]{5}\,\beta^3$가 된다. 그러면 x^4-5의 분해체는 다음과 같다.

$$S_{\mathbb{Q}}(x^4-5) = \mathbb{Q}(\sqrt[4]{5}\,\beta, \cdots, \sqrt[4]{5}\,\beta^4) = \mathbb{Q}(\sqrt[4]{5}, \beta) = \mathbb{Q}(i, \sqrt[4]{5})$$

이 때 $\alpha = \sqrt[4]{5}$라 하면 $irr(\sqrt[4]{5}, \mathbb{Q}) = x^4-5$이므로 α의 대수적 켤레근은 $\pm\alpha$, $\pm\alpha i$이고, $irr(i, \mathbb{Q}) = x^2+1$이므로 i의 대수적 켤레근은 $\pm i$이므로 x^4-5의 갈루아 군 $G(K/\mathbb{Q}) = \{\sigma_1, \cdots, \sigma_8\}$의 원소는 다음과 같다.

동형사상	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
α의 상	α	$-\alpha$	αi	$-\alpha i$	α	$-\alpha$	αi	$-\alpha i$
i의 상	i	i	i	i	$-i$	$-i$	$-i$	$-i$

(3) $irr(\sqrt[4]{5}, \mathbb{Q}(\sqrt{5})) = x^2 - \sqrt{5}$임을 보이자.

$$\begin{aligned} 4 = \deg(x^4-5) &= [\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}(\sqrt{2})]\deg(x^2-5) = [\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}(\sqrt{2})]2 \end{aligned}$$

이므로 $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}(\sqrt{2})] = 2$이다. 따라서 $irr(\sqrt[4]{5}, \mathbb{Q}(\sqrt{5})) \mid x^2 - \sqrt{5}$이어야 하므로 $irr(\sqrt[4]{5}, \mathbb{Q}(\sqrt{5})) = x^2 - \sqrt{5}$이다. 그러면 $\mathbb{Q}(\sqrt{5})$ 위에서 $\sqrt[4]{5}$의 켤레근은 $\pm\sqrt[4]{5}$이다. 또한 $irr(i, \mathbb{Q}(\sqrt{5})) = x^2+1$이므로 i의 켤레근은 $\pm i$이므로 x^4-5의 갈루아 군 $G(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$의 원소는 다음과 같다.

동형사상	σ_1	σ_2	σ_3	σ_4
α의 상	$\sqrt[4]{5}$	$-\sqrt[4]{5}$	$\sqrt[4]{5}$	$-\sqrt[4]{5}$
i의 상	i	i	$-i$	$-i$

9.5.11.

(1) $f(x) = x^4+2$의 근은 $(x^4+2)(x^4-2) = x^8-4$의 그이다. 이 때 1의 원시 8-제곱근을

$$\alpha = e^{\frac{2\pi i}{8}} = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

이라고 하자. 그럼 x^8-4의 근은 $\sqrt[4]{2}, \cdots, \sqrt[4]{2}\,\alpha^7$이다. 그러면 이 중에서 x^4+2의 근은

$$\sqrt[4]{2}\,\alpha, \quad \sqrt[4]{2}\,\alpha^3, \quad \sqrt[4]{2}\,\alpha^5, \quad \sqrt[4]{2}\,\alpha^7$$

이 된다. 그러므로 x^4+2의 분해체는 $K = \mathbb{Q}(\sqrt[4]{2}, i)$이다. 이 때 $\alpha = \sqrt[4]{2}$라 하면 $irr(\sqrt[4]{2}, \mathbb{Q}) = x^4-2$이므로 α의 대수적 켤레근은 $\pm\alpha$, $\pm\alpha i$이다. 또한 $irr(i, \mathbb{Q}) = x^2+1$이므로 i의 대수적 켤레근은 $\pm i$이므로 x^4+2의 갈루아 군 $G(K/\mathbb{Q}) = \{\sigma_1, \cdots, \sigma_8\}$의 원소는 다음과 같다.

동형사상	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
α의 상	α	$-\alpha$	αi	$-\alpha i$	α	$-\alpha$	αi	$-\alpha i$
i의 상	i	i	i	i	$-i$	$-i$	$-i$	$-i$

(2) 예 9.4.16(2)와 (1)에 의해 x^4+2와 x^8-4의 분해체는 같으므로 x^8-4의 갈루아 군은 (1)의 결과와 같다.

9.5.12. (1) 1의 원시 5-제곱근을 $\alpha = e^{\frac{2\pi i}{5}}$라 하면 $x^5-7 \in \mathbb{Q}(\alpha)[x]$의 근은 $\sqrt[5]{7}$, $\sqrt[5]{7}\alpha$, $\cdots$, $\sqrt[5]{7}\alpha^4$이다(정리 9.4.14). 그러므로 x^5-7의 $\mathbb{Q}(\alpha)$ 위에서 분해체는 $K = \mathbb{Q}(\alpha)(\sqrt[5]{7})$이다.

(2) $irr(\sqrt[5]{7}, \mathbb{Q}(\alpha)) = x^5-7$임을 보이자.

$$irr(\sqrt[5]{7}, \mathbb{Q}) = x^5-7, \quad [\mathbb{Q}(\sqrt[5]{7}), \mathbb{Q}] = 5$$

이다. 한편

$$[K:\mathbb{Q}] = [\mathbb{Q}(\alpha)(\sqrt[5]{7}):\mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\sqrt[5]{7})][\mathbb{Q}(\sqrt[5]{7}):\mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\sqrt[5]{7})]5 \ \cdots \ (*)$$

이므로

$$5 \mid [K:\mathbb{Q}]$$

이다. 또한 $irr(\alpha, \mathbb{Q}) = x^4+x^3+x^2+x+1$이므로

$$\begin{aligned}
&[K:\mathbb{Q}] \\
&= [\mathbb{Q}(\alpha)(\sqrt[5]{7}):\mathbb{Q}] \\
&= [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}] \\
&= [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] \\
&= [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\sqrt[5]{7})]\deg(\alpha, \mathbb{Q}) \\
&= [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\sqrt[5]{7})]\deg(x^4+x^3+x^2+x+1) \\
&= [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\sqrt[5]{7})]4
\end{aligned}$$

이므로

$$4 \mid [K:\mathbb{Q}] \ \cdots \ (**)$$

이다. 따라서 $4 \cdot 5 \mid [K:\mathbb{Q}]$, 즉, $20 \mid [K:\mathbb{Q}]$이다.

한편 (*)와 (**)에서

$$4 \mid [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\sqrt[5]{7})]5$$

이므로

$$4 \mid [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\sqrt[5]{7})], \quad \text{즉,} \quad 4 \mid [K:\mathbb{Q}(\sqrt[5]{7})] = \deg(\alpha, \mathbb{Q}(\sqrt[5]{7}))$$

이다. α는 $x^4+x^3+x^2+x+1$의 근이고 $\deg(\alpha, \mathbb{Q}(\sqrt[5]{7}) \geqq 4$이므로

$$irr(\alpha, \mathbb{Q}(\sqrt[5]{7})) = x^4+x^3+x^2+x+1$$

이다. 그러므로

$$[K:\mathbb{Q}(\sqrt[5]{7})] = \deg(\alpha, \mathbb{Q}(\sqrt[5]{7})) = 4$$

이고 (*)에서

$$[K:\mathbb{Q}] = 20$$

이다. 따라서

$$20 = [K:\mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\alpha)]4$$

이므로 $[\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\alpha)] = 5$이다. 그러므로

$$5 = [\mathbb{Q}(\alpha, \sqrt[5]{7}):\mathbb{Q}(\alpha)] = \deg(\sqrt[5]{7}, \mathbb{Q}(\alpha))$$

이고 $\sqrt[5]{7}$이 x^5-7은 근이므로 $irr(\sqrt[5]{7}, \mathbb{Q}(\alpha)) = x^5-7$이다. 또한 $\mathbb{Q}(\alpha)$ 위에서 $\sqrt[5]{7}$의 대수적 켤레근은 $\sqrt[5]{7}$, $\sqrt[5]{7}\alpha$, $\cdots$, $\sqrt[5]{7}\alpha^4$이므로 x^5-7의 갈루아 군 $G(K/\mathbb{Q}) = \{\sigma_1, \cdots, \sigma_5\}$의 원소는 다음과 같다.

동형사상	σ_1	σ_2	σ_3	σ_4	σ_5
$\sqrt[5]{7}$의 상	$\sqrt[5]{7}$	$\sqrt[5]{7}\alpha$	$\sqrt[5]{7}\alpha^2$	$\sqrt[5]{7}\alpha^3$	$\sqrt[5]{7}\alpha^4$

따라서 갈루아군의 위수가 5이므로 $\mathbb{Z}_5$와 동형이다.

9.5.13. (1) 1의 원시 n-제곱근을 $w = e^{\frac{2\pi i}{n}}$라 하면 $x^n-a \in \mathbb{Q}[x]$의 근은 $\sqrt[n]{a}$, $\sqrt[n]{a}w$, $\cdots$, $\sqrt[n]{a}w^{n-1}$이다(정리 9.4.14). 그러므로 $a \neq 0$이므로 x^n-a의 $\mathbb{Q}$ 위에서 분해체는 $K = \mathbb{Q}(\sqrt[n]{a}, w)$이다.

(2) n이 소수이므로 $irr(w, \mathbb{Q}) = x^{n-1}+x^{n-2}+\cdots+x+1$이다(정리 9.5.4). 따라서 $\mathbb{Q}$ 위에서 w의 대수적 켤레근은 $w, w^2, \cdots, w^{n-1}$($n-1$개)이다. 한편 $\sqrt[n]{a}$의 켤레근은 $\deg(\sqrt[n]{a}, \mathbb{Q})$개이다. 그러므로

$$|G(\mathbb{Q}(\omega, \sqrt[n]{a})/\mathbb{Q})| = (n-1)\deg(\sqrt[n]{a}, \mathbb{Q})$$

이다.