Homework 4

18.40.

귀류법. $2\mathbb{Z}$와 $3\mathbb{Z}$가 환으로서 동형이라고 하자. 그러면 동형사상

$$\phi : 2\mathbb{Z} \to 3\mathbb{Z}$$

가 존재한다. 이 함수는 일대일이고 전사이다.

$\phi(2) = a$라 하면, $\phi(a+b) = \phi(a) + \phi(b)$이므로,

$$\phi(2n) = an$$

이다. 이 함수는 전사이므로,

$$3 \Big| |a|$$

이고, 이는 $a = -3, 3$임을 의미한다.

$a = -3$인 경우

$$-6 = \phi(2) + \phi(2) = \phi(4) = \phi(2)\phi(2) = 9$$

이므로 모순이다.

$a = 3$인 경우

$$6 = \phi(2) + \phi(2) = \phi(4) = \phi(2)\phi(2) = 9$$

이므로 모순이다.

따라서, $2\mathbb{Z}$와 $3\mathbb{Z}$가 환으로서 동형이 아니다. □

18.52.

예 18.15.에 의해서, $\mathbb{Z}_{rs}$, $\mathbb{Z}_r \times \mathbb{Z}_s$사이에 동형을 주는 사상

$$\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$$

가 존재한다. 여기서 ϕ는

$$\phi(x) = (x) \cdot (1, 1)$$

이다.

나눗셈 알고리즘을 이용하여

$$m = m_0 r + m_1 \quad (0 \le m_1 < r)$$

$$n = n_0 s + n_1 \quad (0 \le n_1 < s)$$

라 하자. 그러면 $(m_1, n_1) \in \mathbb{Z}_r \times \mathbb{Z}_s$이다.

ϕ가 동형사상이므로 전사이면서 단사이다. 따라서,

$$\exists x \in \mathbb{Z}_{rs} \Big| \phi(x) = (m_1, n_1)$$

이고, 이는

$$x \equiv m_1 \equiv m \mod r$$

$$x \equiv n_1 \equiv n \mod s$$

을 의미한다.

따라서, $\forall m, n \in \mathbb{Z}$에 대해 $x \equiv m \mod r$와 $x \equiv n \mod s$을 만족하는 정수 x가 존재한다. □

18.55.

$$2a = (a+a) = (a+a)^2 = 4a^2 = 4a$$

이므로,

$$a = -a$$

이다. 또한

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

이므로 $a = -a$을 이용하면,

$$ab = -ba = (-b)a = ba$$

이다.

따라서, 모든 부울환은 가환환이다.

19.23.

나눗셈환이므로 $0, 1 \in R$이다. (단, $0 \neq 1$) 또한,

$$0^2 = 0$$

$$1^2 = 1$$

이므로, $0, 1$은 멱등원이다.

$(a \neq 0) \wedge (a \neq 1)$이면 a가 멱등원이 아님을 보이자.

pf. 나눗셈환이므로 a는 가역원이고,

$$\exists b \in R \Big| ab = ba = 1$$

이다. 만약

$$a^2 = a$$

라 하면, 이 식에 b를 오른쪽에 곱하게 되면

$$aab = ab \iff a = 1$$

이므로, 모순이다.

따라서 $(a \neq 0) \wedge (a \neq 1)$이면 a는 멱등원이 아니고, R의 멱등원은 $0, 1$ 두개 뿐이다. □

19.29.

정역 D의 표수가 0이 아니라면 소수임을 보이면 충분하다.

정리 19.15.에 의해 표수가 0이 아니면, 표수는 $n \cdot 1 = 0$을 만족하는 가장 작은 자연수 n이다.

이 자연수 n이 소수가 아니라고 하자. 즉, $n = pq \quad (2 \leq p, q \in \mathbb{Z}^+)$라 하자. 그러면

$$0 = n \cdot 1 = (p \cdot 1)(q \cdot 1)$$

이고, D는 정역이므로 0의 약수가 존재하지 않는다. 따라서,

$$(p \cdot 1 = 0) \vee (q \cdot 1 = 0)$$

라 할 수 있다. $p, q < n$이므로, 이는 n이 $n \cdot 1 = 0$을 만족하는 가장 작은 자연수임에 모순이다.

따라서, n은 소수일 수 밖에 없다. □

20.6.

$$2^{17} \equiv 0 \mod 2$$

$$2^{17} \equiv (2^6)^2(2^5) \equiv 5 \mod 9$$

이므로

$$2^{17} \equiv 14 \mod 18$$

이다. 이를 이용하면,

$$\begin{aligned} 2^{2^{17}} + 1 \equiv & 2^{14} + 1 \equiv (2^4)^3(2^2) + 1 \equiv (-3)^3(2^2) + 1 \\ \equiv & -108 + 1 \equiv -13 + 1 \equiv 7 \mod 19 \end{aligned}$$

이다.

20.14.

$$\begin{aligned} (45x \equiv 15 \mod 24) &\iff (-3x \equiv 15 \mod 24) \\ &\iff (3x \equiv -15 \mod 24) \\ &\iff (3x \equiv 9 \mod 24) \\ &\implies (x \equiv 3 \mod 8) \end{aligned}$$

이고, $8 \cdot 3 = 24$이므로, 따라서 주어진 합동식의 모든 해는

$$(3 + \mathbb{Z}_{24})$$

$$(11 + \mathbb{Z}_{24})$$

$$(19 + \mathbb{Z}_{24})$$

에 속하는 경우이다.

20.27.

자기 자신이 자신의 곱셉역원이 된다는 말은

$$x^2 = 1$$

라는 것이다.

$\mathbb{Z}_p$는 정역이므로,

$$x^2 = 1 \iff (x-1)(x+1) = 0$$

이면 0의 약수가 존재하지 않으므로,

$$(x - 1 = 0) \vee (x + 1 = 0)$$

이다.

즉, $\mathbb{Z}_p$의 원소중에서는 $x^2 = 1$을 만족하는 x는 $1, p-1$뿐이다.

20.28.

$p = 2$인 경우

$$(p-1)! \equiv (1)! \equiv 1 \equiv= -1 \mod p$$

이므로 성립한다.

$p \neq 2$인 경우

먼저, $1 \neq p - 1$이다. 1의 역원은 1이고, $p-1$의 역원은 $p-1$임을 문제 20.27.에서 보였다.

a와 b가 다르면, a의 역원과 b의 역원도 다르므로,

$$(x \neq 1) \vee (x \neq p-1) \vee (0 \neq x \in \mathbb{Z}_p)$$

이면 x의 역원은 1과 $p-1$이 아니다.

또, 문제 20.27.에 의해 $2, 3, \cdots, p-2$은 자기자신이 자신의 역원이 아니므로, $2, 3, \cdots, p-2$에서 서로 역원이 되게 하는 $\frac{p-3}{2}$개의 쌍을 만들어 줄 수 있다.

이를 이용하여 $(p-1)!$을 생각하면,

$$\begin{aligned} (p-1)! \equiv & (1)\,((2)(3)\cdots(p-2))\,(p-1) \\ \equiv & (1)\,((1)(1)\cdots(1))\,(p-1) \\ & \text{(단, 가운데 중괄호 안의 1의 개수는 } \frac{p-3}{2}\text{개이다.)} \\ \equiv & (p-1) \equiv -1 \mod p \end{aligned}$$

임을 알 수 있다.

따라서, 모든 소수 p에 대해 $(p-1)! \equiv -1 \mod p$이다. □

20.29.

Lemma. 1

a가 정수, b가 양의 정수, p가 소수이고, $p-1 \mid b-1$이면

$$a^b - a \equiv 0 \mod p$$

임을 보이자. **pf.**

모든 $b = n(p-1)+1$에 대해 보이면 충분하자. 이를 수학적 귀납법으로 보이자.

$n=1$인 경우는 페르마 소정리에 의해 $a^p - a \equiv 0 \mod p$이다.

$n=k$인 경우에 성립한다고 가정하자. 그러면, $b=(k+1)(p-1)+1$일 때를 생각하면

$$\begin{aligned} a^b - a \equiv & a^p a^{b-p} - a \equiv (a)(a^{b-p}) - a \equiv a^{b-(p-1)} - a \\ \equiv & a^{(k)(p-1)+1} - a \equiv 0 \mod p \end{aligned}$$

이다. 따라서, $n=k+1$인 경우에도 성립한다.

따라서, 수학적 귀납법에 의해 모든 자연수 n에 대해 $b=n(p-1)+1$이면

$$a^b - a \equiv 0 \mod p$$

이다. □

위 Lemma를 이용하면,

$$\begin{aligned} 37-1 \mid 37-1 &\implies n^{37} - n \equiv 0 \mod 37 \\ 19-1 \mid 37-1 &\implies n^{37} - n \equiv 0 \mod 19 \\ 13-1 \mid 37-1 &\implies n^{37} - n \equiv 0 \mod 13 \\ 7-1 \mid 37-1 &\implies n^{37} - n \equiv 0 \mod 7 \\ 3-1 \mid 37-1 &\implies n^{37} - n \equiv 0 \mod 3 \\ 2-1 \mid 37-1 &\implies n^{37} - n \equiv 0 \mod 2 \end{aligned}$$

이다. 따라서,

$$n^{37} - n \equiv 0 \mod 383838$$

임을 알 수 있다.

22.11.

문제 20.29.의 Lemma를 이용하면,

$$3x^{106} + 5x^{99} + 2x^{53} \equiv 3x^4 + 5x^3 + 2x^5 \mod 7$$

이므로,

$$\begin{aligned} \phi_4(3x^{106} + 5x^{99} + 2x^{53}) \equiv & (3)4^4 + (5)4^3 + (2)4^5 \\ \equiv & (3)(2)^2 + (5)(2)(4) + (2)(2)^2(4) \\ \equiv & 12 + 40 + 32 \equiv 84 \equiv 0 \mod 7 \end{aligned}$$

이다. 따라서 0이다.

22.17.

문제 20.29.의 Lemma를 이용하면,

$$\begin{aligned} 2x^{219} + 3x^{74} + 2x^{57} + 3x^{44} \equiv & 2x^3 + 3x^2 + 2x + 3x^4 \mod 5 \\ \equiv & 2x + 3x^2 + 2x^3 + 3x^4 \mod 5 \end{aligned}$$

이다.

$$2x + 3x^2 + 2x^3 + 3x^4 = (x)(3x+2)(x^2+1)$$

모든 $x \in \mathbb{Z}_5$에 대해 대입해보면,

$$\begin{aligned} \phi_0(x) = 0 &\implies \phi_0(2x + 3x^2 + 2x^3 + 3x^4) = 0 \\ \phi_1(3x+2) = 0 &\implies \phi_1(2x + 3x^2 + 2x^3 + 3x^4) = 0 \\ \phi_2(x^2+1) = 0 &\implies \phi_2(2x + 3x^2 + 2x^3 + 3x^4) = 0 \\ \phi_3(x^2+1) = 0 &\implies \phi_3(2x + 3x^2 + 2x^3 + 3x^4) = 0 \end{aligned}$$

$$(4)(12+2)(16+1) \equiv 2 \mod 5 \implies \phi_4(2x+3x^2+2x^3+3x^4) = 2$$

이다. 따라서, 해는

$$\{0, 1, 2, 3\}$$

이다.

22.22.

$x^4 = x^2 \mod 4$이다. 따라서, 3차 이하 다항식만 생각해도 충분하다. 프로그래밍을 통해 구한 결과는 다음과 같다. (상수항이 둘다 1인 경우만 생각하였다. 둘다 3인 경우는 각각에 3을 곱해주면 된다.)

$$\begin{aligned} &(0x^3 + 0x^2 + 2x + 1)(0x^3 + 0x^2 + 2x + 1) \equiv 1 \mod 4 \\ &(3x^3 + 0x^2 + 1x + 1)(1x^3 + 0x^2 + 3x + 1) \equiv 1 \mod 4 \\ &(3x^3 + 0x^2 + 3x + 1)(1x^3 + 0x^2 + 1x + 1) \equiv 1 \mod 4 \\ &(2x^3 + 0x^2 + 0x + 1)(2x^3 + 0x^2 + 0x + 1) \equiv 1 \mod 4 \\ &(2x^3 + 0x^2 + 2x + 1)(2x^3 + 0x^2 + 2x + 1) \equiv 1 \mod 4 \\ &(1x^3 + 0x^2 + 1x + 1)(3x^3 + 0x^2 + 3x + 1) \equiv 1 \mod 4 \\ &(1x^3 + 0x^2 + 3x + 1)(3x^3 + 0x^2 + 1x + 1) \equiv 1 \mod 4 \\ &(2x^3 + 1x^2 + 1x + 1)(0x^3 + 1x^2 + 3x + 1) \equiv 1 \mod 4 \\ &(2x^3 + 1x^2 + 3x + 1)(0x^3 + 1x^2 + 1x + 1) \equiv 1 \mod 4 \\ &(1x^3 + 1x^2 + 0x + 1)(1x^3 + 1x^2 + 0x + 1) \equiv 1 \mod 4 \\ &(1x^3 + 1x^2 + 2x + 1)(1x^3 + 1x^2 + 2x + 1) \equiv 1 \mod 4 \\ &(0x^3 + 1x^2 + 1x + 1)(2x^3 + 1x^2 + 3x + 1) \equiv 1 \mod 4 \\ &(0x^3 + 1x^2 + 3x + 1)(2x^3 + 1x^2 + 1x + 1) \equiv 1 \mod 4 \\ &(3x^3 + 1x^2 + 0x + 1)(3x^3 + 1x^2 + 0x + 1) \equiv 1 \mod 4 \end{aligned}$$

$$(3x^3+1x^2+2x+1)(3x^3+1x^2+2x+1)\equiv 1 \mod 4$$
$$(0x^3+2x^2+0x+1)(0x^3+2x^2+0x+1)\equiv 1 \mod 4$$
$$(0x^3+2x^2+2x+1)(0x^3+2x^2+2x+1)\equiv 1 \mod 4$$
$$(3x^3+2x^2+1x+1)(1x^3+2x^2+3x+1)\equiv 1 \mod 4$$
$$(3x^3+2x^2+3x+1)(1x^3+2x^2+1x+1)\equiv 1 \mod 4$$
$$(2x^3+2x^2+0x+1)(2x^3+2x^2+0x+1)\equiv 1 \mod 4$$
$$(2x^3+2x^2+2x+1)(2x^3+2x^2+2x+1)\equiv 1 \mod 4$$
$$(1x^3+2x^2+1x+1)(3x^3+2x^2+3x+1)\equiv 1 \mod 4$$
$$(1x^3+2x^2+3x+1)(3x^3+2x^2+1x+1)\equiv 1 \mod 4$$
$$(2x^3+3x^2+1x+1)(0x^3+3x^2+3x+1)\equiv 1 \mod 4$$
$$(2x^3+3x^2+3x+1)(0x^3+3x^2+1x+1)\equiv 1 \mod 4$$
$$(1x^3+3x^2+0x+1)(1x^3+3x^2+0x+1)\equiv 1 \mod 4$$
$$(1x^3+3x^2+2x+1)(1x^3+3x^2+2x+1)\equiv 1 \mod 4$$
$$(0x^3+3x^2+1x+1)(2x^3+3x^2+3x+1)\equiv 1 \mod 4$$
$$(0x^3+3x^2+3x+1)(2x^3+3x^2+1x+1)\equiv 1 \mod 4$$
$$(3x^3+3x^2+0x+1)(3x^3+3x^2+0x+1)\equiv 1 \mod 4$$
$$(3x^3+3x^2+2x+1)(3x^3+3x^2+2x+1)\equiv 1 \mod 4$$

$$(2x+1)^2\equiv 1 \mod 4$$

가 가장 간단한 다항식인 것 같다.

22.25.

a.

$f(x), g(x)\in D[x]$이고, $f(x)\neq 0, g(x)\neq 0$라 하자.

$\deg f(x)=n$라 하고, $\deg g(x)=m$라 하면,

$$\deg(f(x)g(x))=n+m$$

이다.

가역원이기 위해서는 $n+m=0$이므로, $n=m=0$이다.

차수가 0일때에는, D의 가역원이 $D[x]$에서 가역원이며 D의 가역원이 아닌 원소는 $D[x]$에서도 가역원이 아니다.

따라서, $D[x]$의 가역원은 D의 가역원이다.

b.

a.에 의해 $1, -1$뿐이다.

c.

a.에 의해 $1,2,3,4,5,6$뿐이다.

23.7.

가역원은

$$\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$$

이고, 여기서 3이 가역원들의 곱셈순환군을 생성한다.

6.16.의 정리를 이용하면, 생성원은

$$\{3^1,3^3,3^5,3^7,3^9,3^11,3^13,3^15\}$$

$$\{3,10,5,11,14,7,12,6\}$$

임을 알 수 있다.

23.9.

$$\begin{aligned}x^4+4\equiv& x^4-1 \mod 5\\ \equiv&(x^2-1)(x^2+1) \mod 5\\ \equiv&(x^2-1)(x^2-4) \mod 5\\ \equiv&(x-1)(x+1)(x-2)(x+2) \mod 5\\ \equiv&(x+1)(x+2)(x+3)(x+4) \mod 5\end{aligned}$$

이다.

23.17.

$$f(x)=x^4-22x^2+1$$

라 하자. 만약 $f(x)$가 $\mathbb{Q}[x]$에서 일차인수를 가지면, $f(x)$는 유리수해를 가져야한다. 그러면 정리 23.12.에 의해 $f(x)$는 정수해 m을 가지고 m이 1의 약수가 되는데, $f(1)=f(-1)=-20$이므로 $f(x)$는 $\mathbb{Q}[x]$에서 일차인수를 가지지 않는다.

이제 만약 $f(x)$가 $\mathbb{Q}[x]$에서 인수분해가 된다면, 두 이차 다항식의 곱으로 될 수 밖에 없다. 여기서 정리 23.11.을 이용하면 $\mathbb{Z}[x]$에서 두 이차 다항식의 곱으로 인수분해가 되고, 그러면 $a,b,c,d\in\mathbb{Z}$에 대해,

$$f(x)=x^4-22x^2+1=(x^2+ax+b)(x^2+cx+d)$$

라 할 수 있다. 그러면,

$$a+c=0,\quad b+d+ac=-22,\quad ad+bc=0,\quad bd=1$$

을 만족해야하고,

$$(a+c=0)$$

이면서,

$$((b = d = 1) \vee (b = d - 1)$$

이므로,

$$(a^2 = 24) \vee (a^2 = 20)$$

인데 이는 불가능하다.

따라서, $f(x)$는 $\mathbb{Q}[x]$에서 기약이다. □

23.28.

정리 23.10.에 의해 차수가 3인 다항식이 기약이기 위한 필요충분조건은 $\mathbb{Z}_2$에서 해를 가지지 않는 것임을 안다. 즉, 3차 다항식 $f(x)$를

$$f(x) = x^3 + ax^2 + bx + c$$

라 하면,

$$f(0)! = 0, \quad f(1)! = 0$$

이므로,

$$c = 1, \quad 1 + a + b + c \equiv 1 \mod 2$$

이다.

즉, $c = 1, \quad a + 1 \equiv b \mod 2$이다.

따라서, 가능한 모든 $\mathbb{Z}_2[x]$의 3차 기약 다항식은

$$\left\{x^3 + x^2 + 1, x^3 + x + 1\right\}$$

이다.

23.34.

$$f(x) = x^p + a$$

라 하면,

$$f(-a) \equiv (-a)^p + a \equiv -a + a \equiv 0 \mod p$$

이므로, $f(x)$는 $\mathbb{Z}_p[x]$에서 기약이 아니다.

23.35.

$a \neq 0$이 $f(x)$의 해이므로,

$$0 = f(a) = a_0 + a_1 a + a_2 a^2 + \cdots + a_n a^n$$

이다. 이 식의 양변을 a^n으로 나누면,

$$0 = a_n + a_{n-1}(\frac{1}{a}) + a_{n-2}(\frac{1}{a})^2 + \cdots + a_0(\frac{1}{a})^n$$

이므로, $\frac{1}{a}$는 $a_n + a_{n-1}x + \cdots a_0 x^n$의 해이다.

26.2.

$\mathbb{Z}_n$의 $\mathbb{Z}_2$와 동형인 부분환이 있다고 가정하고 H라 하자.

덧셈연산에 대해서는 군이므로, 항등원 $0 \in H$이다. 이제 0이 아닌 원소 $a \in H$라 하자.

$$a + a = 0, \quad a^2 \equiv a \mod n$$

을 만족해야하므로,

$$2 \mid n, \quad a = \frac{n}{2}$$

이어야 한다. $n = 2a$라 하고, $a = 2k + r \quad (r = 0 \text{ or } 1, k \in \mathbb{Z})$라 하면

$$4k^2 + 4rk + r^2 \equiv 2k + r \mod 4k + 2r$$

$$2rk \equiv 2k \mod 4k + 2r$$

이므로 $r = 1$일 수 밖에 없다. 즉,

$$n = 2a = 4k + 2$$

인 경우에만 $\mathbb{Z}_2$와 동형인 부분환이 존재한다.

26.18.

체 F에서 환 R로 가는 준동형사상

$$\phi : F \to R$$

의 Kernel $N = Ker(\phi)$를 생각하자. 일단 $0 \in N$이다.

$\{0\} = N$인 경우

정리 26.6.에 의해 ϕ는 일대일 사상이다.

$\{0\} \neq N$인 경우

0이 아닌 원소 $a \in F$가 $a \in N$이다.

$a \neq 0$이고, F의 원소이므로 곱셈에 대한 역원 a^{-1}가 존재하고

$$\phi(1) = \phi(a)\phi(a^{-1}) = 0$$

이므로, $1 \in N$이다.

따라서, 임의의 원소 $f \in F$에 대해

$$\phi(f) = \phi(f)\phi(1) = 0$$

이므로, $N = F$이고 이는 ϕ가 모든 원소를 0으로 보내는 사상임을 의미한다.

결론. 따라서 체에서 환으로의 모든 준동형사상은 일대일 사상이거나, 모든 원소를 0으로 보내느 사상이다. □

26.20.

$\phi_p(a+b) = \phi_p(a) + \phi_p(b)$**을 보이자.**

$$\begin{aligned}\phi_p(a+b) =& (a+b)^p \\ =& \sum_{i=0}^{p} \binom{p}{i} \cdot (a^i b^{p-i}) && (R\text{은 가환환}) \\ =& a^p + b^p && (1 \le i \le p-1 \implies p \Big| \binom{p}{i}) \\ =& \phi_p(a) + \phi_p(b)\end{aligned}$$

$\phi_p(ab) = \phi_p(a)\phi_p(b)$**을 보이자.**

$$\begin{aligned}\phi_p(ab) =& (ab)^p \\ =& a^p b^p && (R\text{은 가환환}) \\ =& \phi_p(a)\phi_p(b)\end{aligned}$$

따라서, $\phi_p(a) = a^p$로 정의하면 ϕ는 준동형사상이다.

26.37.

$\phi(a+bi+c+di) = \phi(a+bi) + \phi(c+di)$**을 보이자.**

$$\begin{aligned}\phi(a+bi+c+di) =& \begin{bmatrix} a+c & b+d \\ -b-d & a+c \end{bmatrix} \\ =& \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ =& \phi(a+bi) + \phi(c+di)\end{aligned}$$

$\phi((a+bi)(c+di)) = \phi(a+bi)\phi(c+di)$**을 보이자.**

$$\begin{aligned}\phi((a+bi)(c+di)) =& \phi(ac-bd+(ad+bc)i) \\ =& \begin{bmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{bmatrix} \\ =& \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ =& \phi(a+bi)\phi(c+di)\end{aligned}$$

ϕ는 준동형사상이다.

$Ker(\phi) = \{0\}$**임을 보이자.**

$$\phi(a+bi) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

이기 위한 조건은

$$a = b = 0$$

이므로, $Ker(\phi) = \{0\}$이다. 따라서, ϕ는 단사함수이다.

$$\phi : \mathbb{C} \to \phi[\mathbb{C}]$$

은 $\phi[\mathbb{C}]$의 정의에 의해 전사함수이다.

위 세가지 증명에 의해서, ϕ는 $\mathbb{C}$와 $\phi[\mathbb{C}]$는 동형사상을 유도한다.

27.2.

먼저 정리 19.11.에 의해 유한 정역은 체임을 안다.

또한, 곱셈항등원을 가진 가환환 R에서 M이 극대 아이디얼이기 위한 필요충분조건은 $R \setminus M$이 체이고, N이 소 아이디얼이기 위한 필요충분조건이 $R \setminus N$이 정역이므로, $\mathbb{Z}_{12}$의 소 아이디얼과 극대 아이디얼은 같음을 알 수 있다.

$\mathbb{Z}_{12}$의 진 아이디얼은

$$\{0,1,2,3,4,5,6,7,8,9,10,11\}$$

$$\{0,2,4,6,8,10\}$$

$$\{0,3,6,9\}$$

$$\{0,4,8\}$$

$$\{0,6\}$$

$$\{0\}$$

이고, 여기서 극대 아이디얼의 성질을 만족하는 것은

$$\{0,2,4,6,8,10\}$$

$$\{0,3,6,9\}$$

뿐이다.

27.6.

$\mathbb{Z}_3[x] \setminus \langle x^3+x^2+c \rangle$가 체가 되는 것과 $\langle x^3+x^2+c \rangle$가 극대 아이디얼인 것과 동치이다. 또한, $\langle x^3+x^2+c \rangle$가 극대 아이디얼인 것은 x^3+x^2+c가 $\mathbb{Z}_3$위에서 기약인 것과 동치이다.

$f(x) = x^3+x^2+c$은 3차 다항식이므로 $\mathbb{Z}_3$에서 해를 가지지 않으면 기약이다.

$$f(0) \equiv c \mod 3$$

$$f(1) \equiv c+2 \mod 3$$

$$f(2) \equiv c \mod 3$$

이므로, $c = 2 \in \mathbb{Z}_3$이다.

27.26.

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

은 환이며, 부분환으로

$$\mathbb{Z}_2 \times \{0\} \simeq \mathbb{Z}_2$$

$$\{0\} \times \mathbb{Z}_3 \simeq \mathbb{Z}_3$$

을 가지고 있다.

따라서 가능하다.

27.30.

정리 27.24.에 의해 $F[x]$의 모든 아이디얼은 주 아이디얼임을 상기하자.

임의의 비자명 진 소 아이디얼 N을 생각하자. $N = \langle f(x) \rangle$이고, 비자명 아이디얼이므로 $N \neq \{0\}$이다.

$f(x)$는 F에서 기약이다.

만약 $f(x)$가 F에서 기약이 아니라고 하면, $f(x)$보다 차수가 낮은 두 다항식 $g(x), h(x) \in F[x]$가 존재하여

$$f(x) = g(x)h(x)$$

인데, $g(x)h(x) \in N$이고, $g(x) \notin N, h(x) \notin N$이므로 소 아이디얼임에 모순이다. □

또한 정리 27.25.에 의해 아이디얼 $\langle f(x) \rangle$가 극대 아이디얼이 될 필요충분조건이 $f(x)$가 F 위에서 기약임을 알고 있다.

따라서, F가 체이면 다항식환 $F[x]$의 모든 비자명 진 소 아이디얼은 극대 아이디얼이다.

27.38.

N이 $M_2(\mathbb{Z}_2)$의 비자명 아이디얼일때, $N = M_2(\mathbb{Z}_2)$임을 보이면 충분하다.

일단 $O \in N$이다. (덧셈군의 항등원)

N이 비자명 아이디얼이므로, $A \neq O$인 $A \in N$을 만족하는 행렬

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

을 생각하자.

아이디얼의 성질에 의해,

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} A = \begin{bmatrix} c & d \\ a & b \end{bmatrix} \quad A \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & a \\ d & c \end{bmatrix}$$

도 N에 속한다.

Case 1. A에 1이 한개

위 성질에 의해

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in N$$

이다.

N이 덧셈부분군이므로,

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix} = x \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + y \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + z \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + w \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in N$$

이다. 따라서, $N = M_2(\mathbb{Z}_2)$이다.

Case 2. A에 1이 두개

Case 2-1. 1이 가로나 세로로 붙어있는 경우

$$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \in N \implies \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in N$$

이므로, Case 1.에 의해 $N = M_2(\mathbb{Z}_2)$이다.

Case 2-2. 1이 대각선에 위치한 경우

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in N \implies \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in N$$

이므로, Case 1.에 의해 $N = M_2(\mathbb{Z}_2)$이다.

Case 3. A에 1이 세개

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in N \implies \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in N$$

이므로, Case 1.에 의해 $N = M_2(\mathbb{Z}_2)$이다.

Case 4. A에 1이 네개

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \in N \implies \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \in N$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \in N \implies \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in N$$

이므로, Case 1.에 의해 $N = M_2(\mathbb{Z}_2)$이다.

따라서, N이 비자명 아이디얼인 모든 경우에 대해

$$N = M_2(\mathbb{Z}_2)$$

임을 알 수 있다.

따라서 행렬환 $M_2(\mathbb{Z}_2)$은 단순환이다. □