추상대수학 2차과제 20181288 윤성호

4.1.16 Let $b_0+b_1x+\cdots+b_kx^k \in R[x]$ be the inverse of 1_R+ax.

Then, we can say that the multiple of those two is $1_R \in R[x]$.

$(b_0+b_1x+\cdots+b_kx^k)(1+ax) = b_0+(b_1+ab_0)x+\cdots+(b_k+ab_{k-1})x^k+ab_kx^{k+1}$

Thus, the coefficients are all zero except b_0. ($\because$ equality of polynomials)

$b_0=1_R$, $b_i=(-1)^ia^i$ for $1\le i\le k$.

Last term, ab_kx^{k+1}, should also be zero.

Thus, $ab_k=(-1)^ka^{k+1}=0 \Rightarrow a^{k+1}=0$ ∎

4.1.22. Let $f(x)=\sum_{i=0}^{n}a_ix^i$, $a_i\in R$ and define $\varphi(f(x))=\sum_{i=0}^{n}a_i(k(x))^i$.

If we define φ as above, $\varphi(r)=r\ \forall r\in R$ and $\varphi(x)=k(x)$.

Let $f(x)=a_0+a_1x+\cdots+a_nx^n$, $g(x)=b_0+b_1x+\cdots+b_mx^m$. w.l.o.g $n\ge m$.

(i) $\varphi((f+g)(x))=\varphi((a_0+b_0)+(a_1+b_1)x+\cdots+(a_m+b_m)x^m+a_{m+1}x^{m+1}+\cdots+a_nx^n)$

$=\varphi(a_0+a_1x+\cdots+a_nx^n+b_0+b_1x+\cdots+b_mx^m)$

$=a_0+a_1k(x)+\cdots+a_n(k(x))^n+b_0+b_1(k(x))+\cdots+b_m(k(x))^m$

$=\varphi(f(x))+\varphi(g(x))$

(ii) $\varphi(fg(x)) = \varphi\left(a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m}\right)$

$$= a_0b_0 + (a_0b_1 + a_1b_0)k(x) + \cdots + a_nb_m(k(x))^{n+m}$$

$$= \left(a_0 + a_1k(x) + \cdots + a_n(k(x))^n\right)\cdot\left(b_0 + b_1k(x) + \cdots + b_m(k(x))^m\right)$$

$$= \varphi(f(x))\cdot\varphi(g(x))$$

By (i) and (ii) φ is a homomorphism.

(iii) Consider $\theta: R[x] \to R[x]$ which is another homomorphism

and $\theta(r) = r$ for any $r \in R$ and $\theta(x) = k(x)$. $\cdots (*)$

Then $\theta(f(x)) = \theta(a_0 + a_1x + \cdots + a_nx^n)$

$$= \theta(a_0) + \theta(a_1)\theta(x) + \cdots + \theta(a_n)(\theta(x))^n$$

$$= a_0 + a_1k(x) + \cdots + a_n(k(x))^n \quad (\because \text{by } (*))$$

$$= \varphi(f(x))$$

Therefore φ is a unique homomorphism $\blacksquare$

4.2.10. Let $d(x)$ be the gcd of two polynomials.

The $\deg(d(x))$ should be 1 or 0, since $\mathbb{Q}[x]$ is an integral domain.

$$\deg(d(x)) \le \deg(x+a+b) = 1$$

$$\deg(d(x)) \le \deg(x^3 - 3abx + a^3 + b^3) = 3$$

$$\Rightarrow 0 \le \deg(d(x)) \le 1$$

Meanwhile, $x^3 - 3abx + a^3 + b^3 = (x+a+b)(x^2 - (a+b)x + a^2 - ab + b^2)$

This means that $x+a+b \mid x+a+b$ and $x+a+b \mid x^3 - 3abx + a^3 + b^3$

$x+a+b$ is the monic polynomial with the highest degree,

which means $d(x) = x+a+b$ ∎

4.3.12. $(x^2+2)(x^2-2)$ in $\mathbb{Q}[x]$.

If x^2-2 is reducible in $\mathbb{Q}[x]$, then it should be factorized with two polynomials with degree 1 since $\mathbb{Q}[x]$ is a field.

But this doesn't happen because it doesn't have any roots in $\mathbb{Q}$ thus does not have linear factor by factor thm. Same situation happens for x^2+2.

$(x^2+2)(x+\sqrt{2})(x-\sqrt{2})$ in $\mathbb{R}[x]$.

By factor thm, x^2+2 does not have linear factors. Thus, x^2+2 is irreducible in $\mathbb{R}[x]$.

$(x+\sqrt{2}i)(x-\sqrt{2}i)(x+\sqrt{2})(x-\sqrt{2})$ in $\mathbb{C}[x]$.

These 4 factors are irreducible since $\mathbb{C}[x]$ is a field and every polynomial of degree 1 is irreducible. ■

4.3.22. (a) Let $f(x) = x^3 + a$ then

$$f(0) = 0 + a = a$$
$$f(1) = 1 + a = a + 1$$
$$f(2) = 8 + a = a + 2$$

The number of elements in $\mathbb{Z}_3$ is 3 and $a, a+1, a+2 \in \mathbb{Z}_3$ which are distinct.

Therefore, one of a, $a+1$, $a+2$ must be zero and by factor thm, x^3+a has a linear factor, which means x^3+a is reducible.

We can use factor thm since $\mathbb{Z}_3$ is a commutative ring with 1_R. ■

(a) Let $f(x) = x^5 + a$ then

$f(0) = 0 + a = a$ $\quad$ $f(3) = 243 + a = a+3$

$f(1) = 1 + a = a+1$ $\quad$ $f(4) = 1024 + a = a+4$

$f(2) = 32 + a = a+2$

The number of elements in $\mathbb{Z}_5$ is 5 and $a, a+1, a+2, a+3, a+4 \in \mathbb{Z}_5$ which are distinct. Therefore, one of $a, a+1, a+2, a+3, a+4$ must be zero and by factor thm, x^5+a has a linear factor, which means x^5+a is reducible

We can use factor thm since $\mathbb{Z}_5$ is a commutative ring with 1_R ∎

4.4.8. (b) Let a be root of x^2-7. We know that $a = \pm\sqrt{7}$ but $\pm\sqrt{7} \notin \mathbb{Q}$, thus by factor thm, x^2-7 is irreducible in $\mathbb{Q}[x]$ ∎

(d) Let $f(x) = 2x^3 + x^2 + 2x + 2$ then $f(0) = 2$ $\quad f(2) = 1$ $\quad f(4) = 4$

$f(1) = 2$ $\quad f(3) = 1$

$\forall a \in \mathbb{Z}_5$, $f(a) \neq 0$, which means there is no linear factor by factor thm, thus irreducible in $\mathbb{Z}_5$ ∎

(f) Let $g(x) = x^4 + x^2 + 1$ then $g(1) = 0$. Thus $x-1 = x+2 \mid x^4+x^2+1$.

This means that x^4+x^2+1 is reducible in $\mathbb{Z}_3$ ∎

4.4.10. We need to find $a \in \mathbb{Z}$, $0 \le a < p$ such that $a^2+1=0 \pmod p$.

Thus $a^2+1=np$ for $n \in \mathbb{Z}$. We need to find only one p, let's think of a situation that $n=1$. Then $p=a^2+1$. We can consider that if $a=4$, $p=17$, the equation holds.

In this case, $x^2+1=(x+4)(x+13)$ ▨

4.4.26. (a) Note that $\mathbb{Q}[\sqrt{2}] \neq \emptyset$ since $0 \in \mathbb{Q}[\sqrt{2}]$ ($\because$ for the case that $r_i=0\ \forall i$)

Let $a, b \in \mathbb{Q}[\sqrt{2}]$

Let $a=a_0+a_1\sqrt{2}+\cdots+a_n(\sqrt{2})^n$ for some $n \in \mathbb{N}$.

$b=b_0+b_1\sqrt{2}+\cdots+b_m(\sqrt{2})^m$ for some $m \in \mathbb{N}$.

w.l.o.g $n \ge m$.

Claim 1: $a-b \in \mathbb{Q}[\sqrt{2}]$

$$a-b=(a_0-b_0)+(a_1-b_1)\sqrt{2}+\cdots+(a_m-b_m)(\sqrt{2})^m+a_{m+1}(\sqrt{2})^{m+1}+\cdots+a_n(\sqrt{2})^n \in \mathbb{Q}[\sqrt{2}].$$

Claim 2: $ab \in \mathbb{Q}[\sqrt{2}]$

$$ab=a_0b_0+(a_1b_0+a_0b_1)\sqrt{2}+\cdots+a_nb_m(\sqrt{2})^{n+m} \in \mathbb{Q}[\sqrt{2}]$$

By Claim 1, 2, $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$ ▨

(b) Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ $(\forall i,\ a_i \in \mathbb{Q},\ n \in \mathbb{N})$
$g(x) = b_0 + b_1 x + \cdots + b_m x^m$ $(\forall i,\ b_i \in \mathbb{Q},\ m \in \mathbb{N})$

w.l.o.g $n \geq m$.

(i) $\theta((f+g)(x)) = \theta((a_0+b_0) + (a_1+b_1)x + \cdots + (a_m+b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_n x^n)$

$= (a_0+b_0) + (a_1+b_1)\sqrt{2} + \cdots + (a_m+b_m)(\sqrt{2})^m + a_{m+1}(\sqrt{2})^{m+1} + \cdots + a_n(\sqrt{2})^n)$

$= a_0 + a_1\sqrt{2} + \cdots + a_n(\sqrt{2})^n + b_0 + b_1 + \cdots + b_m(\sqrt{2})^m$

$= f(\sqrt{2}) + g(\sqrt{2})$

$= \theta(f(x)) + \theta(g(x))$

(ii) $\theta((f \cdot g)(x)) = \theta(a_0 b_0 + (a_1 b_0 + a_0 b_1)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + a_n b_m x^{n+m})$

$= a_0 b_0 + (a_1 b_0 + a_0 b_1)\sqrt{2} + (a_0 b_2 + a_1 b_1 + a_2 b_0)(\sqrt{2})^2 + \cdots + a_n b_m (\sqrt{2})^{n+m})$

$= (a_0 + a_1\sqrt{2} + \cdots + a_n(\sqrt{2})^n) \cdot (b_0 + b_1\sqrt{2} + \cdots + b_m(\sqrt{2})^m)$

$= f(\sqrt{2}) \cdot g(\sqrt{2})$

$= \theta(f(x)) \cdot \theta(g(x))$

(iii) Let $c \in \mathbb{Q}[\sqrt{2}]$ then we can say that $c = \sum_{i=0}^{n} c_i (\sqrt{2})^i$ $(\forall i,\ c_i \in \mathbb{Q})$

Then we always have $f(x) = \sum_{i=0}^{n} c_i x^i$ s.t $\varphi(f(x)) = c$.

This means θ is surjective.

(iv) Consider $f(x) = x^2$, $g(x) = \frac{1}{2}x^4$.

$$\theta(f(x)) = f(\sqrt{2}) = 2 = g(\sqrt{2}) = \theta(g(x))$$ but

$f(x) \neq g(x)$. Thus, θ is not injective.

By (i), (ii), (iii), and (iv), θ is a surjective homomorphism but not an isomorphism. $\blacksquare$