

MATH 601 HOMEWORK (DUE 9/18)

HIDENORI SHINOHARA

Exercise. (Problem 1) Let R be a commutative ring with one. Explain why there is a unique ring homomorphism, $\mathbb{Z} \rightarrow R$.

Proof. The existence of a ring homomorphism is clear since $\phi(n) = 1_R + \cdots + 1_R$ and $\phi(-n) = -\phi(n)$ define a homomorphism.

We will show the uniqueness of a ring homomorphism. Let $\phi_1, \phi_2 : \mathbb{Z} \rightarrow R$ be ring homomorphisms.

We claim that $\phi_1(n) = \phi_2(n)$ for each $n \in \mathbb{N}$.

- By definition, $\phi_1(1) = \phi_2(1) = 1_R$.
- Suppose $\phi_1(n) = \phi_2(n)$ for some $n \in \mathbb{N}$. Then $\phi_1(n+1) = \phi_1(n) + \phi_1(1) = \phi_2(n) + \phi_2(1) = \phi_2(n+1)$.

By mathematical induction, $\phi_1(n) = \phi_2(n)$ for each $n \in \mathbb{N}$.

For every $n \in \mathbb{N}$, $\phi_1(-n) = -\phi_1(n) = -\phi_2(n) = \phi_2(-n)$. Finally, $\phi_1(0) = \phi_1(0+0) = \phi_1(0) + \phi_1(0)$, so $\phi_1(0) = 0_R$. Similarly, $\phi_2(0) = 0_R$. Thus $\phi_1(0) = \phi_2(0)$.

Hence, we have shown that $\phi_1 = \phi_2$. □

Exercise. (Problem 2) Let $I \subset R$ be an ideal in a commutative ring. Describe a bijective correspondence between ideals in R/I and certain ideals in R .

Proof. The map $J \mapsto \{I + j \mid j \in J\}$ is a bijection between ideals in R that contain I and ideals in R/I . □

Exercise. (Problem 3) Let $I, J \subset R$ be ideals in a commutative ring. Let $I + J \subset R$ denote the smallest ideal containing I and J . Observe that $I + J = \{i + j \in R : i \in I, j \in J\}$. Let $\bar{J} \subset R/I$ denote the image of J under the canonical quotient map, $R \rightarrow R/I$. Observe that \bar{J} is an ideal in $S := R/I$. Use the universal mapping property of the quotient to show that $R/(I + J) \simeq S/\bar{J}$.

Proof. Let $\pi : R \rightarrow R/I$ be the canonical quotient homomorphism. Let $f : R \rightarrow R/(I + J)$ be the canonical quotient homomorphism. Then $\ker(f) = I + J$, so $I \subset \ker(f)$. By Proposition 6 (Universal mapping property of the quotient), there must exist a unique ring homomorphism $\bar{f} : R/I \rightarrow R/(I + J)$ such that $\bar{f} \circ \pi = f$. We claim that $\ker(\bar{f}) = \bar{J}$.

- $\ker(\bar{f}) \subset \bar{J}$? Let $r + I \in \ker(\bar{f})$. Then $r + I = \pi(r)$, so $0 = \bar{f}(r + I) = \bar{f}(\pi(r)) = (\bar{f} \circ \pi)(r) = f(r) = r + (I + J)$. Thus $r \in I + J$. This implies that $r = i + j$ for some $i \in I, j \in J$. Then $r + I = (i + j) + I = j + I \in \pi(J) = \bar{J}$.
- $\bar{J} \subset \ker(\bar{f})$? Let $j + I \in \bar{J}$. Then $\bar{f}(j + I) = \bar{f}(\pi(j)) = f(j) = j + (I + J) = 0$.

Therefore, $\ker(\bar{f}) = \bar{J}$. This implies that \bar{f} induces an isomorphism between $(R/I)/\bar{J}$ and $R/(I + J)$. □

Exercise. (Problem 4) Let R be a commutative ring and $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$ a non-zero polynomial of degree n . Suppose that $a_n \in R^\times$. Let $J = (f(x))$. Prove that every element of $R[x]/J$ may be written in exactly one way in the form $\sum_{i=0}^{n-1} r_i x^i + J$ with $r_0, r_1, \dots, r_{n-1} \in R$.

Proof. Let $g(x) + J \in R[x]/J$ be given. Since the leading coefficient of $f(x)$ is a unit, we will apply Theorem 9 in the handouts. Then there exists a unique polynomial $q(x), r(x) \in R[x]$ such that $g(x) = f(x)q(x) + r(x)$ with $\deg(r(x)) < \deg(f(x))$ or $r(x) = 0$. Then $g(x) + J = f(x)q(x) + r(x) + J = r(x) + J$ where $r(x)$ can be expressed as $\sum_{i=0}^{n-1} r_i x^i$ with $r_0, \dots, r_{n-1} \in R$.

Let $r'(x) = \sum_{i=0}^{n-1} r'_i x^i$ with $r'_0, \dots, r'_{n-1} \in R$. If $g(x) + J = r'(x) + J$, then $g(x) - r'(x) \in J$. Therefore, $g(x) - r'(x) = f(x)q'(x)$ for some $q'(x) \in R[x]$. This implies that $g(x) = f(x)q'(x) + r'(x)$. By the uniqueness of $q(x), r(x)$, we have $q(x) = q'(x)$ and $r(x) = r'(x)$.

Therefore, $g(x) + J$ can be written in exactly one way in the form $\sum_{i=0}^{n-1} r_i x^i + J$ with $r_0, \dots, r_{n-1} \in R$. \square

Exercise. (Problem 5)

- (1) Consider the subring $S := \mathbb{Z}[(1 + \sqrt{5})/2] \subset \mathbb{R}$. Find a generating set for the abelian group $(S, +)$ with the minimal possible cardinality and justify your answer.
- (2) Find an explicit principal ideal, $I \subset \mathbb{Z}[x]$, and an explicit ring isomorphism, $\mathbb{Z}[x]/I \simeq S$. In the course of justifying your answer make explicit use of the mapping property of polynomials, the universal mapping property of the quotient, and division with remainder.
- (3) To what familiar ring is $\mathbb{Z}[(1 + \sqrt{5})/2]/((3 - \sqrt{5})/2)$ isomorphic?
- (4) To what familiar ring is $\mathbb{Z}[(1 + \sqrt{5})/2]/(2 + \sqrt{5})$ isomorphic?

Proof.

- (1) Suppose a generating set is a singleton. Let $x \in S$ be such an element. Then $kx = 1$ for some $k \in \mathbb{Z}$ because we must be able to obtain 1 by adding or subtracting x finitely many times. $k \neq 0$, so this implies that $x = 1/k$. Then $x \in \mathbb{Q}$. However, $(1 + \sqrt{5})/2 \notin \mathbb{Q}$. $(\mathbb{Q}, +)$ is an abelian group, so it is closed under addition and subtraction. Therefore, a generating set cannot be a singleton.

We claim that $\{1, (1 + \sqrt{5})/2\}$ is a generating set. Let $s \in S$ be given. Then s is a real number such that $s = \sum_{i=0}^{\infty} r_i ((1 + \sqrt{5})/2)^i$. Since this is \mathbb{R} , the \sum means limits. Since $|((1 + \sqrt{5})/2)^i| > 1$ for each $i > 0$, there must exist an $N \in \mathbb{N}$ such that $\forall i \geq N, r_i = 0$. Then $s = \sum_{i=0}^N r_i ((1 + \sqrt{5})/2)^i$.

Since $(1 + \sqrt{5})/2$ is a root to the equation $x^2 - x - 1 = 0$, we know that it satisfies $x^2 = x + 1$. By applying this repeatedly, $((1 + \sqrt{5})/2)^n$ can be expressed as a linear combination of $(1 + \sqrt{5})/2$ and 1 over \mathbb{Z} . Therefore, s can be expressed as a linear combination of $(1 + \sqrt{5})/2$ and 1 over \mathbb{Z} . A linear combination of two numbers over \mathbb{Z} can be expressed as a finite sequence of addition and subtraction of the two numbers, so $\{1, (1 + \sqrt{5})/2\}$ is indeed a generator of $(S, +)$.

- (2) By the mapping property of the polynomial ring, there is a unique ring homomorphism $\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[(1 + \sqrt{5})/2]$ with $x \mapsto (1 + \sqrt{5})/2$. We showed in part (1), that every element in $\mathbb{Z}[(1 + \sqrt{5})/2]$ is a linear combination of 1 and $(1 + \sqrt{5})/2$ over \mathbb{Z} . For any $a + b(1 + \sqrt{5})/2 \in \mathbb{Z}[(1 + \sqrt{5})/2]$, $\phi(a + bx) = a + b(1 + \sqrt{5})/2$. Therefore, ϕ is surjective. We clearly have $x^2 - x - 1 \in \ker(\phi)$. Consequently, there is an inclusion of

ideals $(x^2 - x - 1) \subset \ker(\phi)$. To show that this inclusion is an equality, we will apply division with remainder: For $g(x) \in \ker(\phi)$, write $g(x) = (x^2 - x - 1)q(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(x^2 - x - 1) = 2$. If $r(x) \neq 0$, then we may write $r(x) = ax + b$. Since $g(x)$ is in the kernel, $0 = \phi(g(x)) = \phi(r(x)) = a(1 + \sqrt{5})/2 + b$. This implies $a(1 + \sqrt{5})/2 = -b \in \mathbb{Z}$. Since a is an integer and $(1 + \sqrt{5})/2$ is irrational, this is possible if and only if $a = b = 0$. Thus in fact $r(x)$ must be zero, which implies $g(x) \in (x^2 - x - 1)$. Thus $(x^2 - x - 1) = \ker(\phi)$.

By the part 3 of the universal mapping property of the quotient, we have a ring isomorphism $\bar{\phi} : \mathbb{Z}[x]/\ker(\phi) \rightarrow \phi(\mathbb{Z}[x])$. In other words, $\bar{\phi}$ is an isomorphism between $\mathbb{Z}[x]/(x^2 - x - 1)$ and $\mathbb{Z}[(1 + \sqrt{5})/2]$.

- (3) We showed above that $\mathbb{Z}[(1 + \sqrt{5})/2]$ is isomorphic to $\mathbb{Z}[x]/(x^2 - x - 1)$. The ϕ in part (ii) maps x to $(1 + \sqrt{5})/2$. The ideal $(3 - \sqrt{5})/2$ gets identified with the ideal in $\mathbb{Z}[x]/(x^2 - x - 1)$ generated by $2 - x + (x^2 - x - 1)$. Lemma 11 allows us to identify $\mathbb{Z}[(1 + \sqrt{5})/2]/((3 - \sqrt{5})/2)$ with

$$\mathbb{Z}[x]/(x^2 - x - 1, 2 - x) \simeq \mathbb{Z}/(2^2 - 2 - 1) \simeq \mathbb{Z}/(1)$$

where the first isomorphism comes from the isomorphism $\mathbb{Z}[x]/(2 - x) \rightarrow \mathbb{Z}$, which maps x to 2. Thus the ideal generated by $(x^2 - x - 1)$ in $\mathbb{Z}[x]/(2 - x)$ gets identified with (1) .

Thus $\mathbb{Z}[(1 + \sqrt{5})/2]/((3 - \sqrt{5})/2) \simeq (0)$.

□