1 Lecture 1 (March 4th)

Chapter 2 Modular Arithmetic

Remark. In abstract algebra, we learn algebraic structures such as rings (eg. $(\boldsymbol{Z}, +, \times)$) and groups (eg. $(\boldsymbol{Z}, +)$).

Remark. By convention we are going to denote the set of integers equipped with addition and multiplication by the triple $(\boldsymbol{Z}, +, \times)$.

Chapter 2.2 Congruence modulo n

Recall. Fix an integer $n > 0$, for example, $n = 5$. We can group integers (create a partition) that have the same remainder when divided by $n = 5$. This creates a congruence relation, denotable as "$7 = 12$" (In number theory, we would say that 7 and 12 are congruent mod 5). We let $\bar{a}$ denote the equivalence class of a with respect to the congruence modulo n.

Remark. Giving a partition on $\boldsymbol{Z}$ is equivalent to giving an equivalence relation on $\boldsymbol{Z}$. For example, we declare $6 \equiv_5 -4$. To summarize, $\bar{a} = \{b \mid b \equiv_n a\}$ or $[a]$. There is a mathematical reason why we prefer the former.

2 Lecture 2 (March 6th)

Last class, we have learnt $\boldsymbol{Z}/n\boldsymbol{Z}$ as a set. In this lecture, we will learn algebraic structures on $\boldsymbol{Z}/n\boldsymbol{Z}$.

Definition. (2.1) Let a and b be integers. We say that a is congruent to b modulo n if $a - b = nk$ for some $k \in \boldsymbol{Z}$. In this case, we write $a \equiv_n b$ (or $a \equiv b \pmod{n}$).

Remark. (2.2) $a \equiv_n b$ if and only if a and b have the same remainder after division by n.

Remark. $\equiv_n$ is an equivalence relation on $\boldsymbol{Z}$. Accordingly, $\bar{a} = \{b \in \boldsymbol{Z} \mid b \equiv_n a\}$.

Proof. (i) $a \equiv_n a$

(ii) $a \equiv_n b \implies b \equiv_n a$

(iii) $a \equiv_n b$, $b \equiv_n c \implies a \equiv_n c$

□

Definition. (2.5) We denote by $\boldsymbol{Z}/n\boldsymbol{Z}$ the set of congruence classes modulo n.

Remark. (i) $\bar{a} = \bar{b} \in \boldsymbol{Z}/n\boldsymbol{Z}$ if and only if $a \equiv_n b$

(ii) If $\bar{a} \cap \bar{b} \neq \emptyset$, then $\bar{a} = \bar{b}$

(iii) $\boldsymbol{Z} = \bar{0} \coprod \bar{1} \coprod \ldots \coprod \overline{n-1}$

Lastly, we also use $\boldsymbol{Z}/n\boldsymbol{Z}$ instead of $\boldsymbol{Z}_n$.

Remark. (2.9)

(i) $\boldsymbol{Z}/n\boldsymbol{Z}$ is a finite set having exactly n elements (how about $n = 0$?)

(ii) $\boldsymbol{Z}/0\boldsymbol{Z} = \boldsymbol{Z}$

Chapter 2.3 Algebra in $\boldsymbol{Z}/n\boldsymbol{Z}$

We want to define $+$ and $\cdot$ on $\boldsymbol{Z}/n\boldsymbol{Z}$. For example, $n = 5$ and we have $\boldsymbol{Z}/5\boldsymbol{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. Can we simply define $\bar{2} + \bar{3} = \bar{5}$? However, in process of formulating addition, we bump into the problem that we can add different representatives every time. In other words, we don't know whether "+" is well-defined! Let's phrase this differently. Let $\bar{a} = \bar{b}$ and $\bar{c} = \bar{d}$. Then we want $\overline{a+c} = \overline{b+d}$.

Lemma. (2.9) Let a, b, c, d be in $\boldsymbol{Z}$. If $a \equiv_n b$ and $c \equiv_n d$ then $a + c \equiv_n b + d$ and $ac \equiv_n bd$.

3 Lecture 3 (March 11th)

Last time, we dealt with the well-definedness of $+$ and $\cdot$ on $\boldsymbol{Z} \ / \ n\boldsymbol{Z}$.
Lemma. (2.9) Let $n > 0$ be an integer and let a, b, c, and d be integers. If $a \equiv_n c$ and $b \equiv_n d$, then $a + b \equiv_n c + d$ and $a \cdot b \equiv_n c \cdot d$. A start of a proof would be by considering $(a + b) - (c + d) = (a - c) + (b - d)$.

Lemma. (2.13) Let a, b, and c in $\boldsymbol{Z}$. Then,

1. $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$
2. $\bar{a} + \bar{0} = \bar{a} = \bar{0} + \bar{a}$
3. For each $\bar{a} \in \boldsymbol{Z}/n\boldsymbol{Z}$, there exists $\bar{b} \in \boldsymbol{Z}/n\boldsymbol{Z}$ such that $\bar{a} + \bar{b} = \bar{0} = \bar{b} + \bar{a}$
4. $\bar{a} + \bar{b} = \bar{b} + \bar{a}$
5. $\bar{a}(\bar{b}\bar{c}) = (\bar{a}\bar{b})\bar{c}$
6. $\bar{a}\bar{1} = \bar{a} = \bar{1}\bar{a}$
7. $\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}$
8. $(\bar{a} + \bar{b})\bar{c} = \bar{a}\bar{c} + \bar{b}\bar{c}$
9. $\bar{a}\bar{b} = \bar{b}\bar{a}$

The first three imply that $\boldsymbol{Z}$ is a group and four implies that it is abelian also. From five to eight, the properties tells us that group is a ring and the ninth tells us that it is a commutative one.

Proof. For the first property, we have

$$\begin{aligned}(\bar{a}+\bar{b})+\bar{c} =& \overline{a+b}+\bar{c} \\ =& \overline{(a+b)+c} \\ =& \overline{a+(b+c)} \\ =& \bar{a}+\overline{b+c} \\ =& \bar{a}+(\bar{b}+\bar{c})\end{aligned}$$

□

Remark. Unlike in $\boldsymbol{Z}$, $\bar{2}\cdot\bar{3}=\bar{6}=\bar{0}$ in $\boldsymbol{Z}/6\boldsymbol{Z}$. Note that $\bar{2}\neq\bar{0}$ in $\boldsymbol{Z}/6\boldsymbol{Z}$. Like so, two non-zero numbers can multiply to become zero in $\boldsymbol{Z}/n\boldsymbol{Z}$.

Theorem. (2.15) Let n be an integer greater than 1. Then the following are equivalent.

1. The integer n is a prime number.
2. Let a and b be in $\boldsymbol{Z}$. If $\bar{a}\bar{b}=\bar{0}$, then $\bar{a}=\bar{0}$ or $\bar{b}=\bar{0}$.
3. For all $\bar{a}\neq\bar{0}$ in $\boldsymbol{Z}/n\boldsymbol{Z}$, $\bar{a}$ has a multiplicative inverse.

Proof. We will prove that $2 \implies 3$. Let $\bar{a}\neq\bar{0}$ be an element of $\boldsymbol{Z}/n\boldsymbol{Z}$. Consider the subset of $\boldsymbol{Z}/n\boldsymbol{Z}$ consisting $\{\bar{a}\bar{0},\bar{a}\bar{1},\ldots,\bar{a}\overline{n-1}\}$. We claim that if $\bar{a}\bar{i}=\bar{a}\bar{j}$ for $0\leq i,j\leq n-1$, then $i=j$. Consequently, $\{\bar{a}\bar{0},\ldots,\bar{a}\overline{n-1}\}=\boldsymbol{Z}/n\boldsymbol{Z}$. In particular, $\bar{1}=\bar{a}\bar{b}$ for some $\bar{b}\in\boldsymbol{Z}/n\boldsymbol{Z}$. □

4 Lecture 4 (March 13th)

Last class, we have learned some properties of $\boldsymbol{Z}/n\boldsymbol{Z}$. Today, we will learn about rings.

Proposition. (2.16) Let n be an integer greater than 1. Then $\bar{a}\in\boldsymbol{Z}/n\boldsymbol{Z}$ has a multiplicative inverse if and only if $(a,n)=1$.

Proof. We know the following

$$1=(a,n)=ax+ny$$

for some $x,y\in\boldsymbol{Z}$. □

Theorem. (2.18) (Fermat's little theorem) Let p be a prime number and let a be an integer. Then $\bar{a}^p = \bar{a}$. In fact, $\bar{a}^{p-1} = \bar{1}$ for $\bar{a} \neq \bar{0}$. The proof is up to you.

Chapter 3 Rings

Chapter 3.1 Definition & Examples

Definition. (3.1) A ring is a set R equipped with two binary operations (a function $R \times R \to R$), an addition $+$ and a multiplication $\cdot$ which satisfies the following.

(i) $(a+b)+c = a+(b+c)$

(ii) There exists an element $0 \in R$ such that for every $a \in R$, $a+0 = a = 0+a$

(iii) For each a, there exists an a' such that $a+a' = 0 = a'+a$

(iv) $a+b = b+a$

(v) $(ab)c = a(bc)$

(vi) There exists an element $1 \in R$ such that for all $a \in R$, $a \cdot 1 = a = 1 \cdot a$

(vii) $a(b+c) = a \cdot b + a \cdot c$

(viii) $(a+b)c = ac + bc$

Example. Some examples of groups are

(i) $\boldsymbol{Z}, \boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ are rings

(ii) $\boldsymbol{Z}/n\boldsymbol{Z}$ is a ring

(iii) $5\boldsymbol{Z}$ is not a ring as it has no multiplicative identity

(iv) $\boldsymbol{Z}^{\geq 0} = \{m \in \boldsymbol{Z} \mid m \geq 0\}$ is not a ring

(v) $(M_{n\times n}(\boldsymbol{R}), +, \cdot)$

(vi) $\boldsymbol{R}[x]$

Chapter 3.2 Basic Properties

Proposition. (3.14) The additive and multiplicative identities are unique.

Proof. Suppose there O and O' are two additive identities. Then,

$$O = O + O' = O'$$

□

Proposition. (3.15) The additive inverse is unique.

Proof. Let a be an element of R. Assume that both b and c are additive inverses of a.

$$c = O + c = (b + a) + c = b + O = b$$

□

Remark. (Notation)

(i) $a \cdot b = ab$

(ii) $a + a + \ldots + a = na$ and $a \cdot a \cdot \ldots \cdot a = a^n$

(iii) $a^0 = 1$ by convention

(iv) For $n > 0$, $(-n)a = (-a) + \ldots + (-a)$

Proposition. (3.17) Let R be a ring. If $a + c = b + c$, then $a = b$.

5 Lecture 5 (March 18th)

Last class, we have dealt with the basic properties of rings. Today, we learn more about rings.

Recall. Notation-wise, we have noted that

(i) $a \cdot b = ab$

(ii) a^n for $n > 0$ and a^0 is defined as 1.

(iii) na for $n \in \boldsymbol{Z}$

Proposition. (3.14, 15, 16) The uniqueness of 0, 1, and $-a$.

Proposition. (3.17) Let R be a ring. If $a + c = b + c$ then $a = b$.

Corollary. (3.18) For every a in a ring R,

$$0a = 0 = a0$$

Proof.

$$0 + 0a = (0 + 0)a = 0a + 0a$$

□

Remark. There is no cancellation law for multiplication ($ac = dc$ does not imply that $a = d$).

Chapter 3.3 Special Types of Rings

Example. (3.19) Not every ring is commutative. For instance, consider $M_{2\times 2}(\boldsymbol{R})$.

Definition. (3.20) A ring is commutative if $ab = ba$ for all $a, b \in R$.

Definition. (3.22) Let a be an element of R. We say that a is a zero divisor if there exists a non-zero $b \in R$ such that $ab = 0$ or $ba = 0$.

Example. In $M_{2\times 2}(\boldsymbol{R})$,

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = 0$$

Observe that both matrices are zero-divisors.

Definition. (3.23) Let R be a commutative ring. We will say that R is an integral domain if $1 \neq 0$ and $ab = 0$ implies that $a = 0$ or $b = 0$.

Example. $\boldsymbol{Z}$ or equivalently $\boldsymbol{Z}/0\boldsymbol{Z}$ are integral domains whereas $\boldsymbol{Z}/1\boldsymbol{Z}$ is not as its multiplicative and additive identities are equal to each other.

Example. (3.26) Let $n > 1$ be an integer. Then $\boldsymbol{Z}/n\boldsymbol{Z}$ is an integral domain if and only if n is a prime.

Proposition. Let $a \in R$ be an element. If a is not a zero-divisor, then the multiplicative cancellation holds for a. That is, if $ab = ac$ or $ba = ca$, then $b = c$.

Proof. (3.26) If $ab = ac$, then $0 = a(b - c) = a(b + (-c))$. □

Definition. (3.27) If a has a multiplicative inverse (that is, there exists $b \in R$ such that $ab = 1 = ba$), then we say that a is invertible or a unit.

Remark. We denote the set of units in R by $R^{\times}$.

Proposition. (3.28) Let $n > 0$ be an integer.

$$(\boldsymbol{Z}/n\boldsymbol{Z})^{\times} = \{\bar{a} \mid (a, n) = 1\}$$

Definition. (3.27) We say that R is a field if

(i) R is commutative

(ii) $1 \neq 0$ in R

(iii) Every nonzero element is invertible

Remark. If R is a field, then $R^\times = R - \{0\}$.

Example. (3.30)

(i) $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$

(ii) $\boldsymbol{Z}/p\boldsymbol{Z}$ where p is a prime

Proposition. (3.31) Every field is an integral domain.

Proof. Yours! □

Remark. The conserve doesn't hold.

6 Lecture 6 (March 20th)

Last time, we have learned integral domains & fields. Today, we will learn Cartesian products and subrings.

Recall. (i) (3.22) $a \in R$ is a zero-divisor if there exists a $b \neq 0$ such that $ab = 0$ or $ba = 0$

(ii) (3.23) R is an integral domain if (1) R is commutative, (2) $1 \neq 0$, and (3) R has no nonzero zero-divisors

(iii) R has no nonzero zero-divisors

(iv) $a \in R$ is a unit for $ab = ba = 1$ for some $b \in R$

(v) R is a field if (1), (2), and every nonzero element is a unit

Remark. The fact that $1 = 0$ in R is equivalent to saying that R is the trivial ring $\{0\}$

Proposition. (3.28) When $n > 0$,

$$(\boldsymbol{Z}/n\boldsymbol{Z})^\times = \{\bar{a} \in \boldsymbol{Z}/n\boldsymbol{Z} \mid (a, n) = 1\}$$

The problem with this definition is that we don't know whether the condition $(a, n) = 1$ works for the entirety of $\bar{a}$. However, we know from number theory that if $a \equiv_n b$, then $(a, n) = (b, n)$.

Remark. We note that

$$\text{Fields} \subset M_{2\times 2}(\boldsymbol{R}), \boldsymbol{R}[x] \in \text{Integral Domains} \subset \boldsymbol{Z}/4\boldsymbol{Z} \in \text{Rings}$$

Proposition. (3.33) Let R be an integral domain having finitely many elements. Then R is a field.

Proof. The proof is similar to the proof of Fermat's little theorem. Set $R = \{a_1, a_2, \ldots, a_n\}$. It suffices to prove that We now prove that this is a field. Let's fix $a_i \neq 0$. If suffices to prove that $a_i \in R^\times$. Consider the subset of R $a_iR = \{a_i \cdot a_1, a_i \cdot a_2, \ldots, a_i \cdot a_n\}$. Since R is an integral domain, $a_iR = R$. Indeed, if $a_i \cdot a_j = a_i \cdot a_k$, $a_j = a_k$. Then, $1 = a_i \cdot a_j$ for some j. Consequently, every nonzero element in R has a multiplicative inverse. □

Chapter 4 The Category of Rings

Chapter 4.1 Cartesian Products

Definition. (4.1) Lets R and S be rings. The catesian product of R and S is the set $R \times S$ equipped with component-wise addition and multiplication.

Remark. In $R \times S$,

$$\begin{cases} (r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \\ (r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2) \end{cases}$$

forms a ring. If it exists, the inverse of an element would look like (r^{-1}, s^{-1}). We remind ourselves that there exists projection functions (pr_1, pr_2) from $X \times Y$ to X and Y.

Example. (4.2, 4.3)

(i) $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z} \neq \boldsymbol{Z}/4\boldsymbol{Z}$

(ii) $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/3\boldsymbol{Z} \cong \boldsymbol{Z}/6\boldsymbol{Z}$

7 Lecture 7 (March 25th)

Last class, we have learned the properties of rings and subrings. Today, we will learn about ring homomorphisms.

Proposition. (3.33) A finite integral domain is a field

Definition. (4.1) Let R and S be rings. The set

$$(R \times S, (r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2), (r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2))$$

is called the cartesian product of R and S.

Example. (4.2, 4.3)

(i) Comparing $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$ and $\boldsymbol{Z}/4\boldsymbol{Z}$ we find that these are very different sets. Adding identical elements in one results in the 0 whereas this isn't always the case for the other.

(ii) Comparing $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/3\boldsymbol{Z}$ and $\boldsymbol{Z}/6\boldsymbol{Z}$, we find that they are identical.

Definition. (4.5) Let S be a subset of a ring R. We say that S is a subring of R if

(i) $0, 1 \in S$

(ii) S is closed under $+$ and $\cdot$

(iii) $(S, +, \cdot)$ is a ring

Note that a subring is not only a ring of its own but also manifests the algebraic structure of the original ring.

Example. (4.6, 4.7, 4.8, 4.9, 4.11, 4.12, 4.13)

(i) $\boldsymbol{Z} \subset \boldsymbol{Q} \subset \boldsymbol{R} \subset \boldsymbol{C}$

(ii) $\boldsymbol{Z}/n\boldsymbol{Z} \subset \boldsymbol{Z}$

(iii) $\Delta_R = \{(r, r) \mid r \in R\} \subset R \times R$

(iv) $R \subset R[x]$

(v) $\boldsymbol{Z}[i] = \{m + in \mid m, n \in \boldsymbol{Z}\} \subset \boldsymbol{C}$

(vi)

$$\left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \middle| \, a, b \in R \right\} \subset M_{2\times 2}(\boldsymbol{R})$$

Proposition. (4.14) S is a subring of R if and only if ...

Chapter 4.3 Ring Homomorphisms

Chapter 4.4 Isomorphisms of Rings

Definition. (cf. definition (4.29)) Let R and S be rings, and let $\phi : R \to S$ be a function. We will say that ϕ is a ring isomorphism if it satisfies

(i) ϕ is bijective

(ii) ϕ preserves the ring operations, or $\phi(r_1+r_2) = \phi(r_1)+\phi(r_2)$ and $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$

Definition. (4.15) We will say that ϕ is a ring homomorphism if

(i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$

(ii) $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$

8 Lecture 7 (March 27th)

Last time, we have learned about isomorphisms. Today, we will learn about homomorphisms.

Definition. (4.29) Let R and S be rings. A function $\phi : R \to S$ is said to be a isomorphism if

(i) ϕ is a bijection

(ii) $\phi(r_1, +r_2) = \phi(r_1) + \phi(r_2)$

(iii) $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$

We don't need conditions such as $\phi(0) = 0$, $\phi(-r) = -\phi(r)$, and $\phi(1) = 1$ as they are implied by the conditions above.

Definition. (4.15) Let R and S be rings. A function $\phi : R \to S$ is called a (ring) homomorphism if

(i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$

(ii) $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$

(iii) $\phi(1) = 1$

As the function isn't bijective, there doesn't need to be a mapping of $\phi(1)$, and we require the third condition.

Example. The function $f : \boldsymbol{Z} \to \boldsymbol{Z} \times \boldsymbol{Z}$ defined by $n \mapsto (n, 0)$ is not a ring homomorphism.

Definition. (4.32) We will say that two rings R and S are isomorphic if there exists an isomorphism $\phi : R \to S$.

Remark. (4.33) The isomorphic relation is an equivalence relation.

Example. (4.38 - 4.43)

(i) $\boldsymbol{Z}/4\boldsymbol{Z}$ is not isomorphic to $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$

(ii) $\boldsymbol{Z}/6\boldsymbol{Z}$ is isomorphic to $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/3\boldsymbol{Z}$

(iii) The complex conjugation $\boldsymbol{C} \to \boldsymbol{C} : z \mapsto \bar{z}$ is an isomorphism

(iv) The function

$$\boldsymbol{C} \to \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \boldsymbol{R} \right\}$$

defined as

$$a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

is an isomorphism.

(v) $R \to \Delta_R = \{(r,r) \mid r \in R\}$ defined as $r \mapsto (r,r)$ is an isomorphism

(vi) $R[x,y]$ and $(R[x])[y]$ is isomorphic

9 Lecture 9 (April 1st)

Last class, we have learned about isomorphisms and homomorphisms. This class, we learn about some properties of homomorphisms.

Definition. (4.29) A function $\phi : R \to S$ is called an isomorphism if it is a homomorphism and bijective.

Proposition. (4.16) Let $\phi : R \to S$ be a ring homomorphism. Then $\phi(0) = 0$

Proof. $\phi(0+0) = \phi(0) + \phi(0) = \phi(0) = \phi(0) + 0$ □

Example. (4.17 – 26)

(i) The unique function $0 : R \to 0$ is a homomorphism

(ii) $0 \to R : 0 \mapsto 0$ is not a ring homomorphism if R is nontrivial

(iii) $pr_1 : R \times S \to R$ and $pr_2 : R \times S \to S$ are ring homomorphisms

(iv) $\boldsymbol{Z} \to \boldsymbol{Z}/n\boldsymbol{Z} : m \mapsto \bar{m}$ is a ring homomorphism

(v) $\boldsymbol{Z} \to R : n \mapsto n \cdot 1$ is a ring homomorphism

(vi) $\boldsymbol{Z}/12\boldsymbol{Z} \to \boldsymbol{Z}/4\boldsymbol{Z} : \bar{n} \mapsto \bar{n}$ is a ring homomorphsim

(vii) Fix $r \in R$. $R[x] \to R : f(x) \mapsto f(r)$ is a ring homomorphism

(viii) $\boldsymbol{C} \to \boldsymbol{C} : a + bi \mapsto a - bi$ is a homomorphism

(ix) $\boldsymbol{Z} \to \boldsymbol{Z} : n \mapsto 2n$ is not a ring homomorphism

(x) $\boldsymbol{Z}/2\boldsymbol{Z} \to \boldsymbol{Z}$ there is no such ring homomorphism

(xi) $\det : M_{2\times 2}(R) \to R$ is not a ring homomorphism

We MUST check whether the function in (vi) is well defined.

Corollary. (4.31) Let $\phi : R \to S$ be a ring homomorphism. Then ϕ is an isomorphism if and only if there exists a ring homomorphism $\psi : S \to R$ such that $\psi \circ \phi = \mathrm{id}_R$ and $\phi \circ \psi = \mathrm{id}_S$.

Chapter 5 Canonical Decomposition, Quotients, and Isomorphism Theorems

Chapter 5.1 Rings: Canonical Decomposition I

Remark. Any function can be written as a composition of a surjection and an injection.

Proposition. (5.1) Let $\phi : R \to S$ be a homomorphism. Then the image of ϕ (denoted as Im ϕ) is a subring of S.

Remark. (5.2) If R' is a subring of R, then $f(R')$ is a subring of S.

Chapter 5.2 Kernels and Ideals

Definition. (5.3) Let $\phi : R \to S$ be a homomorphism. The kernal of ϕ is the subset $\{r \in R \mid \phi(r) = 0\} \subset R$ and will be denoted by Ker ϕ. Note that Ker $\phi = \phi^{-1}(\{0\})$.

Example. (5.4, 5.5)

(i) Let n be a nonnegative integer. Then the kernel of the homomorphism $\boldsymbol{Z} \to \boldsymbol{Z}/n\boldsymbol{Z}$ (given by $m \mapsto \bar{m}$) is $n\boldsymbol{Z}$

(ii) Let $\mathrm{ev}_0 : R[x] \to R$ be the homomorphism defined by the evaluation at 0. Then, Ker ev_0 is the set of all polynomials with no constant terms.

Proposition. (5.6) The set (Ker $\phi, +$) satisfies the four ring axioms.

10 Lecture 10 (April 3rd)

Last time, we learned homomorphisms and kernals. Today, we will learn ideals and quotient rings.

Recall. Let $\phi : R \to S$ be a ring homomorphism.

Proposition. (5.1) Im $\phi = \phi(R) \subset S$ is a subring.

Remark. (5.2) If $R' \subset R$ is a subring, then $\phi(R') \subset S$ is also a subring.

Definition. (5.3) Ker $\phi = \phi^{-1}(\{0\}) = \{r \in R \mid \phi(r) = 0\}$ is called the kernal of ϕ.

Proposition. (5.6) (Ker $\phi, +$), closed under addition, satisfies the ring properties (i) through (iv). That is, it is a abelian group.

Proposition. (5.17) For all $a \in$ Ker ϕ and all $r \in R$ both ra and ar belong to Ker ϕ.

Definition. (5.8) Let R be a ring and I be a subset of R. I is an ideal if it is:

(i) Closed under addition

(ii) The additive identity is in I $(0 \in I)$

(iii) (Absorption property) For all $a \in I$ and $r \in R$, ar and ra are in I

Remark. (i) If $a \in I$, then $(-1) \cdot a = -a \in I$

(ii) If I is nonempty, then the condition that $0 \in I$ is redundant for I to be an ideal

Example. (5.10 – 15)

(i) Ker ϕ is an ideal of R

(ii) 0 and R are ideals of R

(iii) $\boldsymbol{Z} \subset \boldsymbol{Q}$ is not an ideal

(iv) $m\boldsymbol{Z} \subset \boldsymbol{Z}$ is an ideal for all $m \in \boldsymbol{Z}$

(v) The set of all polynomials $f(x, y)$ in $\boldsymbol{C}[x, y]$ that have no constant term is an ideal.

Proposition. (5.16) Let R be a commutative ring and let $r \in R$ be an element. Then the subset

$$(a) = \{ra \mid r \in R\}$$

is an ideal of R.

Definition. (5.17) Let R be a commutative ring and let $a \in R$ be an element. We say that (a) is a principle ideal generated by a.

Remark. Let $a_1, a_2, \ldots, a_n$ be elements of a commutative ring R. Then the subset $(a_1, \ldots, a_r) = \{r_1 a_1 + r_2 a_2 + \ldots + r_n a_n \mid r_i \in R\}$ is an ideal and called the ideal generated by $a_1, \ldots, a_n$.

Chapter 5.3 Quotient Rings

The following diagram shows what we are trying to do.

$$\begin{array}{rcl} \boldsymbol{Z} & \longleftrightarrow & R \\ n\boldsymbol{Z} & \longleftrightarrow & I \\ \boldsymbol{Z}/n\boldsymbol{Z} & \longleftrightarrow & R/I \end{array}$$

Alike how we partitioned the integers using the relationship of multiples of integers, we are going to partition a ring using the relation that elements are in identical ideals.

Definition. (5.19) Let R be a ring and I be an ideal of R. We define a relation $\sim_I$ on R by declaring that $a \sim_I b$ if and only if $b - a \in I$. We say that a is congruent to b modulo the ideal I.

Proposition. (5.20) The relation $\sim_I$ is an equivalence relation.

Remark. Let $R = \boldsymbol{Z}$ and $I = n\boldsymbol{Z}$ then

$$a \sim_I b \qquad \Longleftrightarrow \qquad a \equiv_n b$$

Remark. For each $a \in R$, the equivalence class a can be described as follows:

$$[a] = \{r \in R \mid a \sim_I r\} = \{a + i \mid i \in I\} = a + I$$

For example,

$$\bar{2} = 2 + 5\boldsymbol{Z}$$

Definition. (5.22) We call $\bar{a}$ the coset of a modulo I. We will denote by R/I the set of all cosets and call it the quotient of R modulo I.

11 Lecture 11 (April 8th)

Last class, we have learned kernals and ideals. Today, we will learn quotient rings and isomorphism theorems.
Definition. (5.3) Let $\phi : R \to S$ be a ring homomorphism.

$$\ker \phi = \{r \in R \mid \phi(r) = 0\} = \phi^{-1}(\{0\})$$

Definition. (5.8) Let I be a subset of a ring R. Then I is said to be an ideal if

(i) It is closed under $+$ and additive inverses

(ii) $0 \in I$

(iii) (Absorbtion property) $ar = ra \in I$ for all $r \in R$ and all $a \in I$

Proposition. (5.16) If R is commutative, then $\ker \phi$ is an ideal of R.

Definition. (5.19) Let R be a commutative ring and I be an ideal of R. $a \sim_I b$ if and only if $b - a \in I$. Then, we say "a is congruent to b modulo I".

Remark. (i) Here, $\sim_I$ is an equivalence relation

(ii) The equivalence class of $a \in R$

$$[a] = \bar{a} + I = \{a + i \mid i \in I\} \subset R$$

is called the (left) coset of a modulo I.

Definition. (5.22) R/I (the set of all cosets $\{\bar{a} \mid a \in R\}$) is called the quotient of R modulo I.

Remark. We can give a ring structure to $R/I = \{\bar{a} \mid a \in R\}$by defining

$$\begin{cases} R/I \times R/I \to R/I : (\bar{a}, \bar{b}) \mapsto \overline{a+b} \\ R/I \times R/I \to R/I : (\bar{a}, \bar{b}) \mapsto \overline{ab} \end{cases}$$

Theorem. (5.26) Let R be a (commutative) ring and let $I \subset R$ be an ideal. Then $(R/I, +, \cdot)$ is a ring.

Proof. We first show well-definedness of $+$ and $\cdot$. Then, we can show the eight ring properties. □

Example. (5.27 - 34)

(i) $\boldsymbol{Z}/n\boldsymbol{Z}$

(ii) $R/R = \{\bar{a} \mid a \in R\} = \{R\} \neq R$ In this case, $\bar{a} = R$ for every $a \in R$.

(iii) If R is commutative, then R/I is also commutative ($\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$).

(iv) R/I is not necessarily an integral domain, even if R is an integral domain. For example, $\boldsymbol{Z}/4\boldsymbol{Z}$ is not an integral domain, since $\bar{2} \cdot \bar{2} = \bar{0}$.

(v) Consider $R[x] \;/\; (x)$. $\overline{f(x)} = \overline{1 + 2x + 3x^2} = \overline{1} + \overline{2} \cdot \overline{x} + \overline{3}(\overline{x})^2$.

(vi) For a commutative ring R, $R[x] \;/\; (x - r) \cong R$

(vii) $\boldsymbol{R}[x] \;/\; (x^2+1) \cong \boldsymbol{C}$. For $f(x) \in \boldsymbol{R}[x]$, $f(x) = (x^2+1)q(x)+ax+b$ and $\overline{f(x)} = \overline{ax+b}$. The function would be $\overline{f(x)} \to ai + b$.

12 Lecture 12 (April 10th)

Last time we have learned about quotient rings. Today, we learn about the first isomorphism theorems.

Chapter 5.3 Rings: Canonical Decomposition II

Proposition. (5.35) Let R be a ring and I be an indeal of R. Then the natural projection $\pi : R \to R/I$ given by $r \mapsto \overline{r}$ is a surjective ring homomorphism with $\ker \pi = I$.

Proof. Almost yours!

$$\begin{aligned} r \in \ker I &\iff \pi(r) = \overline{r} = \overline{0} \\ &\iff r = r - 0 \in I \end{aligned}$$

$\square$

Theorem. (5.37 5.38) (The 1st isomorphism theorem) Let $\phi : R \to S$ be a ring homomorphism. Then

(i) The function $\overline{\phi} : R \,/\, \ker\, \phi \to S$ given by the rule $\overline{\phi}(\overline{r}) = \phi(r)$ is a well-defined ring homomorphism

(ii) $\overline{\phi}$ is an injective ring homomorphism

(iii) $\mathrm{Im}\, \overline{\phi} = \mathrm{Im}\, \phi$

In particular, $\overline{\phi}$ induces an isomorphism $R \,/\, \ker\, \phi \to \mathrm{Im}\, \phi$.

Remark. (i) For the projection function $\pi : R \to R \,/\, I$, applying the above, we have $R \,/\, \ker\, \pi \cong \mathrm{Im}\, \pi$.

(ii) We recall that a function can be decomposed into a surjection and an injection. Likewise, a homomorphism can be decomposed into a projection, isomorphism, and surjection.

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"'] & S \\
R/\ker\varphi \arrow[r, "\sim"'] & \mathrm{Im}\,\varphi \arrow[u, hook]
\end{tikzcd}$$

(iii) In linear algebra

$$\begin{aligned}
L : V \to W &\implies V \,/\, \ker\, L \cong \mathrm{Im}\, L \\
&\implies \dim V - \dim \ker L = \dim V \,/\, \ker L = \dim \mathrm{Im}\, L = \mathrm{rank}\, L \\
&\implies \dim L = \dim \ker L + \mathrm{rank}\, L
\end{aligned}$$

Proof. The steps are as follows.

($*$) Well-definedness of $\overline{\phi} : R \,/\, \ker\, \phi \to S : \overline{r} \mapsto \phi(r)$. We claim that if $\overline{r_1} = \overline{r_2}$, then $\phi(r_1) = \phi(r_2)$. Note that $r_1 - r_2 \in \ker\, \phi$. Then,

$$0 = \phi(r_1 - r_2) = \phi(r_1) + \phi(-r_2) = \phi(r_1) - \phi(r_2)$$

(i) Let $\overline{\phi}$ be a ring homomorphism. Prove $+$ separately.

$$\overline{\phi}(\overline{a} \cdot \overline{b}) = \overline{\phi}(\overline{ab}) = \overline{\phi(ab)} = \overline{\phi(a)\phi(b)} = \overline{\phi(a)} \cdot \overline{\phi(b)} = \overline{\phi}(\overline{a}) \cdot \overline{\phi}(\overline{b})$$

(ii) We now prove that $\overline{\phi}$ is injective. Suppose that $\overline{r} \in \ker \overline{\phi}$. We want to prove that $\overline{r} = \overline{0}$. By the assumption,

$$0 = \overline{\phi}(\overline{r}) = \phi(r)$$

that is, $r \in \ker \phi$, which completes the proof.

(iii) $\operatorname{Im} \overline{\phi} = \operatorname{Im} \phi$

$\square$

Example. (5.40, 5.41)

(i) Let R be a ring and $r \in R$. Consider the evaluation homomorphism

$$\mathrm{ev}_r : R[x] \to R : f(x) \mapsto f(r)$$

Note that $\ker \mathrm{ev}_r = (x - r)$. Applying the 1st isomorphism theorem,

$$R[x] \;/\; (x - r) = R[x] \;/\; \ker \mathrm{ev}_r \to \operatorname{Im} \mathrm{ev}_r = R$$

13 Lecture 13 (April 15th)

Last time we have learned

Theorem. (5.37, 5.38) Let $\phi : R \to S$ be a ring homomorphism. Then:

(i) The induced map $\overline{\phi} : R \;/\; \ker \phi \to S$ is defined by $\overline{\phi}(\overline{r}) = \phi(r)$ is a well-defined ring homomorphism

(ii) $\overline{\phi}$ is injective

(iii) $\operatorname{Im} \overline{\phi} = \operatorname{Im} \phi$

In particular, there is an isomorphism of rings $\overline{\phi} : R \;/\; \ker \phi \to \operatorname{Im} \phi$.

Example. (i) For each $r \in R$ there is an isomorphism

$$R[x] \;/\; (x - r) \to R$$

(ii) There is an isomorphism of rings

$$\boldsymbol{R}[x] \;/\; (x^2 + 1) \to \boldsymbol{C}$$

Chapter 5.6 The Chinese Remainder Theorem

Example. Let's examine whether we can solve the following system of congruences.

$$\begin{cases} x \equiv_3 2 \\ x \equiv_7 2 \\ x \equiv_8 5 \end{cases}$$

We attempt to generalize this from $\boldsymbol{Z}$ to R.

Definition. (5.43) Let R be a ring and let I and J be ideals of R. The sum $(I+J)$ of I and J is defined to be

$$\{a+b \mid a \in I, b \in J\}$$

The product (IJ) of I and J is defined to be

$$\Big\{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J\Big\}$$

Remark. (i) $I+J$ and IJ are ideals of R

(ii) $I+J$ is the smallest ideal containing both I and J

(iii) $IJ \subset I \cap J \subset I$ or $J \subset I+J$

(iv) In $R[x]$, set $I = J = (x)$. Then $IJ = (x^2) \not\subset (x) = I \cap J$

(v) In $R[x]$, let $I = (x, 2)$. Then $x^2 + 4$ cannot be written as a product of two elements of I. Moreover, $I^2 \not\subset I$

Example. In $\boldsymbol{Z}$,

(i) $(a) + (b) = (\gcd(a, b))$

(ii) $(a) \cap (b) = (\mathrm{lcd}(a, b))$

(iii) $(a) \cdot (b) = (ab)$

Theorem. (5.52) (Chinese Remainder Theorem) Let R be a commutative ring, and let I and J be ideals of R. If $I + J = R$, then

$$R \,/\, IJ \cong R \,/\, I \times R \,/\, J$$

Corollary. (5.53) Let $n_1, \ldots, n_r$ be pairwise relatively prime positive integers. Let $N = n_1 n_2 \ldots n_r$. Then $\boldsymbol{Z}/n\boldsymbol{Z}$ is isomorphic to $\boldsymbol{Z}/n_1\boldsymbol{Z} \times \boldsymbol{Z}/n_2\boldsymbol{Z} \times \ldots \times \boldsymbol{Z}/n_r\boldsymbol{Z}$.

Remark. Going back to solving a system of congruences, $(3, 7) = (7, 8) = (3, 8) = 1$ implied that there existed a unique solution in modulo $3 \cdot 7 \cdot 8$.

$$\boldsymbol{Z}/3 \cdot 7 \cdot 8 \cong \boldsymbol{Z}/3\boldsymbol{Z} \times \boldsymbol{Z}/7\boldsymbol{Z} \times \boldsymbol{Z}/8\boldsymbol{Z}$$

Proposition. (5.48) Let R be a ring, let I and J be ideals of R. Assume that $I + J = R$. Then the homomorphism $\pi : R \to R/I \times R/J : r \mapsto (\bar{r}, \bar{r})$ is surjective.

Proof. For a given $(\bar{a}, \bar{b}) \in R/I \times R/J$, we can find a $x \in R$ such that $\pi(x) = (\bar{a}, \bar{b}) \in R/I \times R/J$. Let $x - a = i \in I$ and $x - b = j \in J$. □