Lecture 25 - Ring Theory

(25.0) Definitions

A ring R is a non-empty set together with two operations $+, \cdot : R \times R \to R$ [addition and multiplication] and two distinct elements $0, 1 \in R$ such that

(i) $(R, +, 0)$ is an abelian group

(ii) $(R, \cdot, 1)$ is a (multiplicative) monoid with identity element 1

(iii) Multiplication is distributive over addition:

$$a \cdot (b+c) = a \cdot b + a \cdot c$$
$$(b+c) \cdot a = b \cdot a + c \cdot a \qquad \forall\, a, b, c \in R$$

$R^\times := \{ a \in R$ such that a has a multiplicative inverse $\}$

(other notations for $R^\times$: $U(R)$ - group of units)

for $a \in R^\times$, a^{-1} denotes its (unique) multiplicative inverse.

(25.1) Examples. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$

If R_1, R_2 are two rings, $R_1 \times R_2$ with component-wise addition and multiplication is again a ring.

If R is a ring, $R[x] = \left\{ \sum_{j=0}^{N} a_j x^j : a_0, \ldots, a_N \in R, N \geq 0 \right\}$

is again a ring: addition (component-wise) $\sum_{j=0}^{M} a_j x^j + \sum_{k=0}^{N} b_k x^k = \sum_{k=0}^{\max(M,N)} (a_k + b_k) x^k$

mult.: $\left(\sum_{j=0}^{M} a_j x^j \right) \cdot \left(\sum_{k=0}^{N} b_k x^k \right) = \sum_{\ell=0}^{MN} (a_\ell b_0 + a_{\ell-1} b_1 + \ldots + a_0 b_\ell) x^\ell$

[with the understanding that $a_\ell = 0 \ \forall \ \ell > M$ and $b_k = 0 \ \forall \ k > N$]

$M_{n \times n}(R)$ = set of $n \times n$ matrices with coefficients from R is again a ring (usual addition and multiplication of matrices)

(25.2) Some important subtypes of rings.

Let R be a ring.

- R is said to be <u>commutative</u> if $ab = ba \ \forall a, b \in R$.
- R is said to be a <u>division ring</u> (or skew-field) if $R^\times = R \setminus \{0\}$.
- Field = commutative division ring.
- R is an <u>integral domain</u> if R is commutative and $\forall\, a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$

[In general if, for $a \in R$, there is $b \neq 0$, $b \in R$ such that $ab = 0$, we say 'a' is a zero divisor.
Integral domain = no (non-zero) zero divisors.]

e.g. $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring. If n is not a prime number, say $n = n_1 \cdot n_2$, the residue classes of n_1, n_2 in $\mathbb{Z}/n\mathbb{Z}$ are zero divisors.

If n is prime, $\mathbb{Z}/n\mathbb{Z}$ is a field.

(25.3) Subring. Let R be a ring. A subring R' of R is a subset $R' \subset R$ containing $0, 1$ which is closed under addition and multiplication

i.e. $\forall\ a, b \in R'$, $a+b \in R'$ & $ab \in R'$

Ideal Let $\mathfrak{a} \subset R$ be a subgroup of the abelian group $(R, +, 0)$. We say $\mathfrak{a}$ is

- a left ideal of R if $\forall\ \begin{matrix} r \in R \\ a \in \mathfrak{a} \end{matrix}$, $r \cdot a \in \mathfrak{a}$
- a right ideal of R if $\forall\ \begin{matrix} r \in R \\ a \in \mathfrak{a} \end{matrix}$, $a \cdot r \in \mathfrak{a}$
- an ideal of R if it's both left and right ideal.

Homomorphisms of rings. Let R_1 and R_2 be two rings.

A homomorphism of rings $f : R_1 \to R_2$ is a

- group homomorphism (i.e. $f(a_1 + b_1) = f(a_1) + f(b_1)$ $\forall\ a_1, b_1 \in R_1$)
- hom. of monoids (i.e. $f(1_{R_1}) = 1_{R_2}$ and $f(a_1 b_1) = f(a_1) \cdot f(b_1)$)

(25.4) Quotient ring. Let R be a ring and $\mathfrak{a} \subset R$ be an ideal (both left and right). Consider $R/\mathfrak{a}$ together with the structure of the quotient (abelian) group. Consider the multiplication on $R/\mathfrak{a}$ defined as

$$(a + \mathfrak{a}) \cdot (b + \mathfrak{a}) = a \cdot b + \mathfrak{a}$$

$R/\mathfrak{a}$ is called the <u>quotient ring</u> (or residue ring) of R modulo $\mathfrak{a}$. It naturally comes equipped with a ring hom. $\pi : R \longrightarrow R/\mathfrak{a}$.

(25.5) Lemma. (1) If $\{\mathfrak{a}_j\}_{j \in J}$ is a set of ideals of a ring R, then so is $\bigcap_{j \in J} \mathfrak{a}_j$. [Similarly, left or right ideals].

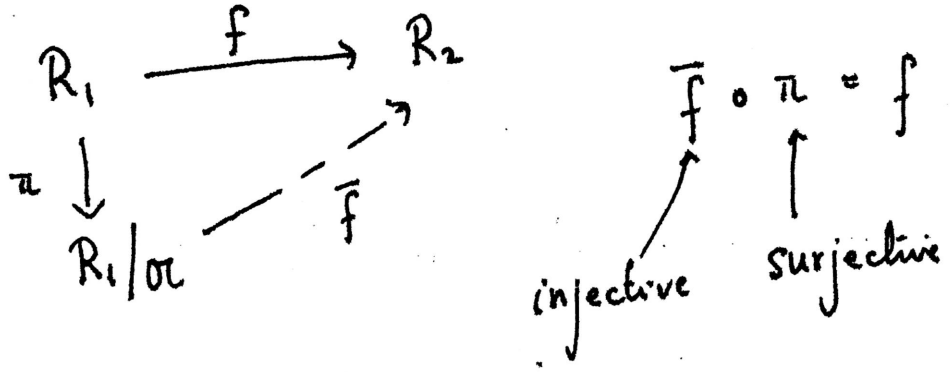
(2) Let $f : R_1 \longrightarrow R_2$ be a ring hom. Then $\mathfrak{a} = \operatorname{Ker}(f) \subset R_1$ is an ideal. $\operatorname{Im}(f) \subset R_2$ is a subring

The proof of this lemma is straightforward and hence omitted.

Fundamental Theorem for homomorphisms.

Let $f \in \mathrm{Hom}_{\text{Rings}}(R_1, R_2)$ and $\mathfrak{a} := \ker(f) \subset R_1$.

Then there is unique $\overline{f} : R_1/\mathfrak{a} \to R_2$ such that



First iso. Thm. Let R be a ring and $\mathfrak{a} \subset R$ an ideal.

$\overline{R} := R/\mathfrak{a}$. Then there is a 1-1 correspondence

$$\left\{ \begin{array}{l} \text{Subgroups of } (R,+,0) \\ \text{containing } \mathfrak{a} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{Subgroups of} \\ (\overline{R},+,0) \end{array} \right\}$$

$$\begin{array}{ccc} \Psi & & \Psi \\ A & \longmapsto & \overline{A} = A \bmod \mathfrak{a} \\ & & = \pi(A) \text{ under } \pi : R \to \overline{R}. \end{array}$$

- A is a subring $\iff$ $\overline{A}$ is a subring
- A is an ideal $\iff$ $\overline{A}$ is an ideal. in which case

$R/A \xrightarrow{\sim} \overline{R}/\overline{A}$ is an isomorphism of rings.

Second Iso. Thm. Let R be a ring, $S \subset R$ a subring and $\mathfrak{a} \subset R$ an ideal. Then $S \cap \mathfrak{a}$ is an ideal in S; and $S + \mathfrak{a}$ is a subring of R containing $\mathfrak{a}$.

$$(S+\mathfrak{a})/\mathfrak{a} \xrightarrow{\sim} S/(S \cap \mathfrak{a})$$

(25.7) Remark: for a ring homomorphism $f: R_1 \to R_2$.

(a) $f^{-1}(\mathfrak{a}_2) \subset R_1$ is an ideal for every $\mathfrak{a}_2 \subset R_2$ ideal.

(b) $f(R_1^\times) \subset R_2^\times$

(c) Image of an ideal need not be an ideal.

eg. $f: \mathbb{Z} \to \mathbb{Z}[x]$ is a ring hom.

$\cup$

(n) = all multiples of n

$f((n))$ is not an ideal (not closed under multiplication by x).