Course 9

2.4 Ideals

We study a notion which is the analogue for Ring Theory of normal subgroups for Group Theory.

Definition 2.4.1 Let $(R, +, \cdot)$ be a ring and let $U \subseteq R$. Then U is called a *left (right) ideal* of R if
(1) $U \neq \emptyset$ $(0 \in U)$;
(2) $x, y \in U \Longrightarrow x - y \in U$;
(3) $r \in R$, $x \in U \Longrightarrow rx \in U$ $(xr \in U)$.
If U is both a left and a right ideal, then U is called a *two-sided ideal* (or simply *ideal*) of R.
We denote by $U \trianglelefteq R$ the fact that U is a (two-sided) ideal of R.

Remark 2.4.2 (1) If R is a commutative ring, then left, right and (two-sided) ideals coincide.

(2) Every left (right, two-sided) ideal is a subring.

Example 2.4.3 (a) Let $(R, +, \cdot)$ be a ring. Then the trivial subrings $\{0\}$ and R are clearly two-sided ideals. A ring that has only trivial two-sided ideals is called *simple*.

(b) The set of ideals of $(\mathbb{Z}, +, \cdot)$ is

$$I(\mathbb{Z}, +, \cdot) = \{n\mathbb{Z} \mid n \in \mathbb{N}\}\,.$$

Indeed, since every ideal is a subring we have $I(\mathbb{Z}, +, \cdot) \subseteq S(\mathbb{Z}, +, \cdot) = \{n\mathbb{Z} \mid n \in \mathbb{N}\}$. On the other hand, for each n and for every $r \in \mathbb{Z}$ and $x \in n\mathbb{Z}$, there exists $k \in \mathbb{Z}$ such that $x = nk$, whence $rx = r(nk) = n(rk) \in n\mathbb{Z}$ and consequently each $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

(c) More generally, let $(R, +, \cdot)$ be a ring and $a \in R$. Then $Ra = \{ra \mid r \in R\}$ and $aR = \{ar \mid r \in R\}$ are a left ideal and a right ideal of R respectively.

(d) Let $f : R \to R'$ be a ring homomorphism. Then $\mathrm{Ker} f \trianglelefteq R$.

Indeed, $\mathrm{Ker}\, f \neq \emptyset$, because $f(0) = 0'$, and so $0 \in \mathrm{Ker}\, f$. Now let $r \in R$ and $x, y \in \mathrm{Ker} f$. Then $f(x) = f(y) = 0'$. It follows that

$$f(x - y) = f(x) - f(y) = 0' - 0' = 0'\,,$$

$$f(rx) = f(r) \cdot f(x) = f(r) \cdot 0' = 0'\,,$$

$$f(xr) = f(x) \cdot f(r) = 0' \cdot f(r) = 0'\,,$$

whence $x - y$, rx, $xr \in \mathrm{Ker} f$. Therefore, $\mathrm{Ker} f \trianglelefteq R$.

Theorem 2.4.4 *Let $(R, +, \cdot)$ be a unitary ring and U a left (right) ideal of R. If U contains an invertible element of R, then $U = R$.*

Proof. Assume that U contains an invertible element of R, say u. Since $u^{-1} \in R$, $u \in U$ and U is a left ideal of R, we deduce that $1 = u^{-1}u \in U$. But then $\forall r \in R$, we have $r = r \cdot 1 \in U$, so that $R \subseteq U$. Therefore, $U = R$. The proof for a right ideal U is similar. □

Corollary 2.4.5 *Let $(R, +, \cdot)$ be a unitary ring and U a left (right) ideal of R. If $1 \in U$, then $U = R$.*

Theorem 2.4.6 *Every division ring has only the trivial left or right ideals.*

Proof. Let $(K, +, \cdot)$ be a division ring and let U be a left ideal of K. Assume that $U \neq \{0\}$. Let $u \in U^*$. It follows that $1 = u^{-1} \cdot u \in U$. Now by Corollary 2.4.5, we get $U = K$. The proof for a right ideal is similar. □

Corollary 2.4.7 *Let K be a division ring, R a ring and $f : K \to R$ a ring homomorphism. Then f is either the trivial homomorphism or an injective homomorphism.*

Proof. We know that Ker$f$ is an ideal of K (see Example 2.4.3). Then by Theorem 2.4.6, we must have either Ker$f = \{0\}$ or Ker$f = K$. In the first case, f is injective, whereas in the second case $f(x) = 0$, $\forall x \in K$, that is, f is the trivial homomorphism. $\square$

As for subrings, the intersection is compatible with ideals, whereas the union is not in general.

Theorem 2.4.8 *Let $(R, +, \cdot)$ be a ring and let $(U_i)_{i\in I}$ be a family of ideals of $(R, +, \cdot)$. Then $\bigcap_{i\in I} U_i$ is an ideal of $(R, +, \cdot)$.*

Proof. For each $i \in I$, U_i is an ideal of $(R, +, \cdot)$, hence $0 \in U_i$. Then $0 \in \bigcap_{i\in I} U_i \neq \emptyset$. Now let $x, y \in \bigcap_{i\in I} U_i$ and $r \in R$. Then $x, y \in U_i$, $\forall i \in I$. But U_i is an ideal of $(R, +, \cdot)$, $\forall i \in I$. It follows that $x - y, rx, xr \in U_i$, $\forall i \in I$, hence $x - y, rx, xr \in \bigcap_{i\in I} U_i$. Therefore, $\bigcap_{i\in I} U_i$ is an ideal of $(R, +, \cdot)$. $\square$

Example 2.4.9 In Example 2.4.3 (b), we have seen that $I(\mathbb{Z}, +, \cdot) = \{n\mathbb{Z} \mid n \in \mathbb{N}\}$. Take $U = 2\mathbb{Z}$, $V = 3\mathbb{Z} \in I(\mathbb{Z}, +, \cdot)$. Then $U \cap V = 2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ is an ideal of $(\mathbb{Z}, +)$. But $U \cup V = 2\mathbb{Z} \cup 3\mathbb{Z}$ is not an ideal of $(\mathbb{Z}, +)$, because, for instance, we have $2, -3 \in U \cup V$, but $2 - (-3) = 5 \notin U \cup V$. Therefore, in general the union of ideals is not an ideal.

This leads to the idea of ideal generated by a subset of a ring.

Definition 2.4.10 Let $(R, +, \cdot)$ be a ring and let $X \subseteq R$. Then we denote

$$(X) = \bigcap\{A \trianglelefteq R \mid X \subseteq A\} \trianglelefteq R$$

and we call it the *ideal generated by* X.

In fact, (X) is the "least" ideal of R containing X.

Here X is called the *generating set* of (X).

If $X = \{x\}$, then we denote $(x) = (\{x\})$.

Remark 2.4.11 Notice that $(\emptyset) = \{0\}$ by Definition 2.4.10.

Let us see how a generated ideal looks like, in the case of a *commutative ring with identity.*

Theorem 2.4.12 *Let $(R, +, \cdot)$ be a commutative ring with identity, and let $\emptyset \neq X \subseteq R$. Then*

$$(X) = \left\{ \sum_{i=1}^{n} a_i x_i \,\middle|\, a_i \in R, x_i \in X\,, i = 1, \ldots, n\,, n \in \mathbb{N}^* \right\},$$

that is, the set of all finite linear combinations of elements in X with coefficients in R.

Proof. Denote by U the right hand side of the above equality. We are going to prove that U is the least ideal of R containing X, that is, to show the following 3 properties:

(i) $X \subseteq U$;

(ii) $U \trianglelefteq R$;

(iii) If $V \trianglelefteq R$ and $X \subseteq V$, then $U \subseteq V$.

Let us discuss them one by one.

(i) Let $x \in X \neq \emptyset$. Then $x = 1 \cdot x \in U$. Hence $\emptyset \neq X \subseteq U$.

(ii) We have just seen that $U \neq \emptyset$. Let $x = \sum_{i=1}^{m} a_i x_i$, $y = \sum_{j=1}^{n} b_j y_j \in U$. Then we have $x - y, rx, xr \in U$, so that $U \trianglelefteq R$.

Clear.

(iii) If $V \trianglelefteq R$ and $X \subseteq V$, then $\sum_{i=1}^{n} a_i x_i \in V$ for every $a_1, \ldots, a_n \in R$, $x_1, \ldots, x_n \in X \subseteq V$ and $n \in \mathbb{N}^*$. It follows that $U \subseteq V$.

Hence U is the least ideal of R containing X, which shows the conclusion of the theorem. $\square$

Corollary 2.4.13 *Let $(R, +, \cdot)$ be a commutative ring with identity, and $a \in R$. Then*

$$(a) = aR = Ra.$$

Theorem 2.4.14 *Let $(R, +, \cdot)$ be a ring. Then the partially ordered set $(I(R, +, \cdot), \subseteq)$ of ideals of R is a complete lattice, where*

$$\inf(U_i)_{i\in I} = \bigcap_{i\in I} U_i, \quad \sup(U_i)_{i\in I} = \left(\bigcup_{i\in I} U_i\right)$$

for every family $(U_i)_{i\in I}$ of ideals of R.

2.5 Factor ring. Isomorphism theorems for rings

Definition 2.5.1 Let $(R,+,\cdot)$ be a ring and let $U \trianglelefteq R$.

(1) Define on R the equivalence relation r_U by:

$$x\, r_U\, y \Longleftrightarrow x - y \in U\,.$$

(2) Denote $R/r_U = \{x+U \mid x \in R\}$ by R/U and define on R/U the operations " $+$ " and " $\cdot$ " by

$$(x+U)+(y+U) = (x+y)+U\,,$$

$$(x+U)\cdot(y+U) = (x\cdot y)+U\,,$$

for every $x, y \in R$.

Theorem 2.5.2 *In the context of the previous definition, r_U is an equivalence relation on R and $(R/U,+,\cdot)$ is a ring, called the quotient (factor) ring of R modulo U. If R has the identity 1, then R/U has identity, namely $1+U$.*

Proof. Since U is a (normal) subgroup of the abelian group $(R,+)$, r_U is an equivalence relation on R from Group Theory. Also, $(R/U,+)$ is an abelian group.

Let us show that $(R/U,\cdot)$ is a semigroup (monoid). Let $x, y, z \in R$. Then:

$$\begin{aligned}(x+U)\cdot[(y+U)\cdot(z+U)] &= (x+U)\cdot(yz+U) = x(yz)+U = (xy)z+U\\ &= (xy+U)\cdot(z+U) = [(x+U)\cdot(y+U)]\cdot(z+U).\end{aligned}$$

If R has the identity 1, then R/U has identity, namely $1+U$.

Also, one easily shows the distributive laws. Hence $(R/U,+,\cdot)$ is a ring (with identity). □

Example 2.5.3 For $R = \mathbb{Z}$ and $U = n\mathbb{Z}$ ($n \in \mathbb{N}$) the above construction gives the ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ of residue classes modulo n. Note that $\mathbb{Z}_0 = \{\{x\} \mid x \in \mathbb{Z}\}$, $\mathbb{Z}_1 = \{\mathbb{Z}\}$ and $\mathbb{Z}_n = \{\widehat{0}, \dots, \widehat{n-1}\}$ for $n \geq 2$.

Recall that the ring $\mathbb{Z}_n$ is a field if and only if n is a prime (see seminar).

Theorem 2.5.4 (The First Isomorphism Theorem) *Let $f : R \to R'$ be a ring homomorphism. Then:*

(i) $\mathrm{Ker} f \trianglelefteq R$*;*

(ii) $R/\mathrm{Ker} f \simeq \mathrm{Im} f$*.*

Proof. The first part was already shown. Let $\overline{f} : R/\mathrm{Ker} f \to \mathrm{Im} f$ be defined by

$$\overline{f}(x + \mathrm{Ker} f) = f(x), \quad \forall x \in R.$$

From the First Isomorphism Theorem for groups, we already know that $\overline{f}$ is a well-defined group isomorphism between the abelian groups $(R,+)$ and $(R',+)$.

We denote $K = \mathrm{Ker} f$ and $\widehat{x} = x + \mathrm{Ker} f$, hence $\overline{f}(\widehat{x}) = f(x)$. For every $x, y \in R$, we have

$$\overline{f}(\widehat{x}\cdot\widehat{y}) = \overline{f}(\widehat{x\cdot y}) = f(x\cdot y) = f(x)\cdot f(y) = \overline{f}(\widehat{x})\cdot\overline{f}(\widehat{y}),$$

hence $\overline{f}$ is a ring isomorphism. □

Example 2.5.5 Let us show the ring isomorphism $\mathbb{R}[X]/(X+1) \cong \mathbb{R}$ by using the first isomorphism theorem. Let $\varphi : \mathbb{R}[X] \to \mathbb{R}$ be defined by $\varphi(f) = f(-1)$ for every $f \in \mathbb{R}[X]$. Then φ is a ring homomorphism (homework!). Recall that if R is a commutative unitary ring and $a \in R$, then the ideal generated by a is $(a) = aR$. Also, according to the Bézout Theorem, for $a \in \mathbb{R}$, we have $f(a) = 0 \Leftrightarrow (X-a)|f$. Hence $(X+1) = (X+1)\mathbb{R}[X]$. It follows that:

$$\mathrm{Ker}\,\varphi = \{f \in \mathbb{R}[X] \mid f(-1) = 0\} = \{f \in \mathbb{R}[X] \mid (X+1)|f\} = (X+1)\mathbb{R}[X] = (X+1).$$

We also have $\mathrm{Im}\,\varphi = \mathbb{R}$, because for every $a \in \mathbb{R}$, there exists $f = a \in \mathbb{R}[X]$ such that $\varphi(f) = f(-1) = a$. By the First Isomorphism Theorem for rings we have $\mathbb{R}[X]/(X+1) \cong \mathbb{R}$.

Theorem 2.5.6 (The Second Isomorphism Theorem) *Let R be a ring and A, U subrings of R such that $U \trianglelefteq (A \cup U)$. Then:*
(i) $(A \cup U) = A + U$.
(ii) $A \cap U \trianglelefteq A$.
(iii) $A/(A \cap U) \simeq (A + U)/U$.

Proof. (i) Note that every subring is a subgroup, and the group $(R, +)$ is abelian. Then $A + U = U + A$, hence from Group Theory we have $< A \cup U >= \sup(A, U) = A + U$ in the subgroup lattice of $(R, +)$. But this also holds in the subring lattice of R.

(ii), (iii) Let $i : A \to A + U$ be the homomorphism defined by $i(a) = a + U$ for every $a \in A$, and let $p : A + U \to (A + U)/U$ be the homomorphism defined by $p(x) = x + U$ for every $x \in A + U$. Denote $p' = p \circ i : A \to (A + U)/U$, and use the First Isomorphism Theorem for the ring homomorphism p'. We have

$$\operatorname{Ker} p' = \{a \in A \mid p'(a) = U\} = \{a \in A \mid a + U = U\} = A \cap U,$$

hence $A \cap U \trianglelefteq A$. Also, p' is surjective, because for every class $(a + u) + U$ ($a \in A$, $u \in U$), we have $(a + u) + U = a + U = p'(a)$. It follows that $(A + U)/U \simeq A/(A \cap U)$. $\square$

Theorem 2.5.7 (The Third Isomorphism Theorem) *Let R be a ring, and U, V ideals of R such that $U \subseteq V$. Then:*
(i) $V/U \trianglelefteq R/U$.
(ii) $(R/U)/(V/U) \simeq R/V$.

Proof. (i) We know that $\emptyset \neq V/U$ is a subgroup of R/U. For every $r \in R$ and $v + U \in V/U$, we have $r(v + U) = rv + U \in V/U$ and $(v + U)r = vr + U \in V/U$. Hence $V/U \trianglelefteq R/U$.

(ii) From the Third Isomorphism Theorem for groups,

$$g : (R/U)/(V/U) \to R/V, \quad g((x + U) + (V/U)) = x + V$$

is a well-defined isomorphism between the corresponding additive groups. For every $x_1, x_2 \in R$, we have

$$\begin{aligned} g(((x_1 + U) + (V/U)) \cdot ((x_2 + U) + (V/U))) &= g((x_1 + U) \cdot (x_2 + U) + (V/U)) \\ &= g((x_1x_2 + U) + (V/U)) \\ &= x_1x_2 + V \\ &= (x_1 + V) \cdot (x_2 + V) \\ &= g((x_1 + U) + (V/U)) \cdot g((x_2 + U) + (V/U)). \end{aligned}$$

Hence g is a ring isomorphism. $\square$

Example 2.5.8 Consider the ring $(\mathbb{Z}, +, \cdot)$. Let $m, n \in \mathbb{N}$ be such that $m|n$. Then we have $U = n\mathbb{Z} \subseteq m\mathbb{Z} = V$. By the third isomorphism theorem we have

$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m.$$

Hence the factor rings of $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$ are isomorphic to $\mathbb{Z}_m$ for $m \in \mathbb{N}$ with $m|n$.