KTH Teknikvetenskap

SF2729 GROUPS AND RINGS
LECTURE NOTES
2010-04-13

SANDRA DI ROCCO

CONTENTS

1. MORE ON RING-HOMOMORPHISMS

We have already seen the definition of ring homomorphism. Let us repeat it, but this time for rings with identity.

Definition 1.1. Let R_1, R_2 be rings with unity. A ring-homomorphism is a map $\phi : R_1 \to R_2$ such that

(1) $\phi(a+b) = \phi(a) + \phi(b)$.
(2) $\phi(ab) = \phi(a)\phi(b)$.
(3) $\phi(1_{R_1}) = 1_{R_2}$.

The last hypothesis is necessary in order for the image to be a subring of R_2 with a unity. Note that (prove it!) if ϕ is surjective or if R_2 has no zero-divisors this hypothesis is automatically satisfied.

The set

$$Ker(\phi) = \{x \in R_1, \phi(x) = 0_{R_2}\}$$

is called the *Kernel* of ϕ.

Example 1.2. Let R be a ring with unity. The map $\mathbb{Z} \to R$ that sends $m \mapsto m \cdot 1_R$ is a ring homomorphism. Check that this is in fact the only homomorphism preserving the unity from $\mathbb{Z}$ to R.

Example 1.3. Let $\phi : R_1 \to R_2$ be a ring homomorphism between rings with unity. Note that:

(1) the map $\phi^* : R_1^* \to R_2^*$ defined as $\phi^*(r) = \phi(r)$ is a group homomorphism.
(2) ϕ^* is injective if ϕ is injective.
(3) Is the same true for surjectivity?

2. IDEALS

Definition 2.1. Let R be a ring. An additive subgroup $I \subseteq R$ is said to be a *left ideal* if

$$ra \in I \text{ for all } r \in R, a \in I.$$

It is said to be a *right ideal* if

$$ar \in I \text{ for all } r \in R, a \in I.$$

It is called an *ideal* if it is a left and right ideal. Clearly for commutative rings every left (resp. right) ideal is an ideal.

Example 2.2.

(1) $\{0_R\}$ is called the trivial ideal.
(2) If $\phi : R_1 \to R_2$ is a ring homomorphism, then $Ker(\phi)$ is an ideal. Moreover one sees that a ring-homomorphism is injective if and only if $Ker(\phi) = \{0_{R_1}\}$.
(3) Let R be a ring and let $x \in R$. the set $Rx = \{rx, r \in R\}$ is an ideal and it is called the left ideal generated by x. Similarly xR is called the right ideal generated by x. When the ring is commutative $Rx = xR$ is denoted by $< x >$ and it is called the ideal generated by x. An ideal I for which there is an element x such that $I =< x >$ is called a *principal ideal*.
(4) Because ideals of the ring $\mathbb{Z}$ are additive subgroups they are of the form $m\mathbb{Z} =< m >$ and thus they are all principal.
(5) Let R be a commutative ring and let $r_1, \dots r_n \in R$. The subset:

$$(r_1, \dots r_n) = \{x_1 r_1 + \dots + x_n r_n, x_1, \dots, x_n \in R\}$$

is an ideal. It is the smallest ideal containing the elements $r_1, \dots r_n$ (EXERCISE) and it is called the ideal generated by $r_1, \dots r_n$.

Example 2.3. Consider $I = (2, x) \subset \mathbb{Z}[x]$. This ideal is not a principal ideal. In fact if it were $I = (p(x))$ for some $p(x) \in \mathbb{Z}[x]$, then $2 = f_1(x)p(x), x = f_2(x)p(x)$ for some $f_1(x), f_2(x) \in \mathbb{Z}[x]$. Recall that $\mathbb{Z}$ is an integral domain which implies that the degree function is additive. It follows that $\deg(p(x)) = 0$ and $\deg(f_2(x)) = 1$, which gives $p(x) = 1, -1$, and thus $1 \in I$. But clearly this is impossible since all the polynomials with constant term in I have even constant.

For polynomial with coefficients in a field the situation is quite different.

Proposition 2.4. *Let F be a filed, then all ideals in $F[x]$ are principal.*

Proof. Let $0 \neq I \subset F[x]$. If $I = 0$ then $I = (0)$. Let $g(x)$ be the element of minimal degree. If $\deg(g(x) = 0$ then $g(x)$ is a unit an thus $I = F[x] = (1)$. Let $g(x) \neq f(x) \in I$, then it is $f(x) = g(x)q(x) + r(x)$ because I is an ideal it is $r(x) \in I$ and $\deg(r(x)) < \deg(g(x))$, which implies $r(x) = 0$ and thus $I = (g(x))$. □

Definition 2.5. An integral domain is a *principal ideal domanin (PID)* is every ideal is principal.

We will now discuss some operations with ideals. Let R be a commutative ring and let I, J be ideals in R.

- It is straight forward to see that the intersection $I \cap J$ is again an ideal.
- The union is not in general an ideal. We can instead define:

  $$I + J = \{x + y \text{ where } x \in I, y \in J\}.$$

  Verfy that it is indeed an ideal and that it is the smallest (w.r.t inclusion) ideal containing I and J.
- The product is defined as:

  $$IJ = \{\sum_{k=1}^{m} x_k y_k \text{ where } m \in \mathbb{Z}, x_k \in I, y_k \in J\}.$$

  Notice that in general $\{xy, x \in I, y \in J\}$ is not an ideal.

Example 2.6. If $I = n\mathbb{Z}, J = m\mathbb{Z}$ are two ideals of $\mathbb{Z}$, it is

$$I \cap J = lcm(m, n)\mathbb{Z},\ I + J = gcd(m, n)\mathbb{Z},\ IJ = mn\mathbb{Z}.$$

Observe that if an ideal $I \subseteq R$ contains a unit then it is $I = R$ (easy to see). It follows that a field F has only (0) and F for ideals, i.e. it has no non trivial proper ideals.

3. Quotient rings

Let R be a commutative ring and let I be an ideal of R. Because R is an abelian group, I is a normal subgroup of the group $(R, +)$, and thus there is a well defined quotient group R/I. We will denote an element in R/I as $x + I$. Recall that

$$x + I = y + I \text{ if and only if } x - y \in I.$$

We define a multiplication as:

$$(x + I) \cdot (y + I) = xy + I.$$

It is indeed a well defined binary operation, let $x' \in x + I, y' \in y + I$, i.e $x' = x + h, y' = y + g$. Then $x'y' = xy + (x'g + y'h + gh)$ and thus $x'y' + I = xy + I$. It is easy to see that R/I is a ring with unity $1 = 1_R + I$. It also follows easily that

Proposition 3.1. *The map*

$$\pi : R \to R/I, \pi(x) = x + I$$

is a well defined surjective ring homomorphism with $Ker(\pi) = I$.

Example 3.2 (Fundamental homomorphism theorem)**.** Let $\phi : R_1 \to R_2$ be a ring homomorphism (of commutative rings with unity). The following diagram is commutative:

$$\begin{array}{ccc} R_1 & \longrightarrow & \phi(R_1) \subseteq R_2 \\ \downarrow & \nearrow & \\ R/Ker(\phi) & & \end{array}$$

where the map $f : R/Ker(\phi) \to \phi(R_1)$ is defined as $r + Ker(\phi) \mapsto \phi(r)$ and it is an isomorphism.

Observe that the map f is a well defined ring-homomorphism. If $x + Ker(\phi) = y + Ker(\phi)$ for $x - y \in Ker(\phi)$, then $\phi(x + y) = \phi(x) - \phi(y) = 0_{R_2}$. Moreover f is clearly surgective and $Ker(f) = Ker(\phi) = \{0_{R/Ker(\phi)}\}$ whichi implies that f is injective and thus an isomorphism.

For example $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ as commuative rings with unity.

4. Prime and maximal idelas

Let R be a commutative ring.

Definition 4.1. We say that an element $a \in R$ divides $b \in R$, $a|b$, if there is $x \in R$ such that $b = ax$. An element $0_R \neq x \in R$ which is not a unit is said to be *prime* if for all $a, b \in R$ it is:

$$x|ab \Rightarrow x|a \text{ or } x|b.$$

We say that an element $0 \neq x$, which is not a unit, is irreducible if for all $a, b \in R$, then

$$x = ab \Rightarrow a \text{ is invertible or } b \text{ is invertible.}$$

This definition can be extended to ideals.

Definition 4.2. A proper ideal $I \subset R$ is said to be prime if for all $a, b \in R$ it is

$$ab \in I \Rightarrow a \in I \text{ or } b \in I.$$

Corollary 4.3. *It follows that for principal ideals (x) is prime if and only if x is prime.*

Proof. Let (x) be prime and let $x|ab$ then $ab = xy$ for an element $y \in R$ which implies that $ab \in (x)$. Then it is $a \in (x)$, i.e $x|a$ or $b \in (x)$, i.e $x|b$. □

Proposition 4.4. *I is prime if and only if R/I is an integral domain.*

Proof. Let I be a prime ideal and let $(r_1 + I)(r_2 + I) = r_1r_2 + I = 0_R + I$. Then it is $r_1r_2 - 0 = r_1r_2 \in I$ and thus $r_1 \in I$ or $r_2 \in I$, i.e. $r_1 + I = 0$ or $r_2 + I = 0$. Viceversa assume that R/I is an integral domain and that $ab \in I$. This means that $ab + I = (a + I)(b + I) = 0$ and thus the conclusion. □

Example 4.5. Observe that $R/(0) \cong R$ which implies that a commutative ring R is an integral domain if and only if the ideal (0) is prime.

Example 4.6. The non trivial prime ideals of $\mathbb{Z}$ are all of the form (p) where p is prime.

Definition 4.7. An ideal $I \subseteq R$ is said to be *maximal* if it is not contained in any other proper ideal ideal of R.

Example 4.8. $2\mathbb{Z}$ is maximal, in fact if $2\mathbb{Z} \subseteq m\mathbb{Z}$ then $m|2$ and thus $m = 1, 2$, i.e. $m\mathbb{Z} = 2\mathbb{Z}$ or $m\mathbb{Z} = \mathbb{Z}$.

We leave as an exercise to prove that: There is a bijection of sets between the set of ideals of R containing I and the ideals of R/I, via the quotient map $\pi : R \to R/I$.

Proposition 4.9. *I is maximal if and only if R/I is a field.*

Proof. By the previous observation if R/I is a field then the only ideals are (0) and R/I which means exactly that that there is no proper ideal containing I and thus I is maximal. Now assume that I is maximal and assume that there is $0 \neq a + I$ which is not a unit. This means $a \notin I$ and there is no element b such that $ab - 1_R \in I$. Consider $J = (a + I)R/I$. it is a non trivial ideal of R/I which does not contain the unity, and thus it is proper. By the observation above $\pi^{-1}(J)$ is a proper ideal of R containing I, which is impossible. □

It follows that if $\{0\}$ is maximal then $R \cong R/\{0\}$ is a fileld. We can than conclude that: *a commutative ring with unity is a field if and only if $\{0\}$ and R are the only ideals.*

Example 4.10. Let K be a filed. The ideal (x) is maximal and $K[x]/(x) \cong K$. (use the evaluation at 0.).

Proposition 4.11. *Every maximal ideal is prime.*

Proof. I maximal implies that R/I is a field which implies that R/I is an integral domain and thus I is prime. □

Note that the converse is not true:

Example 4.12. The ideal $(0) \in \mathbb{Z}$ is prime but not maximal, $(0) \subset 2\mathbb{Z} \neq \mathbb{Z}$. The ideal $(x) \subset \mathbb{Z}[x]$ is also prime but not maximal.

Example 4.13. Notice that if R is an PID then for every non invertible element $0 \neq x$ it is:

$$x \text{ irreducible then } (x) \text{ is maximal.}$$

In fact if x is irreducible and $(x) \subset J = (a) \neq R$ the it is $x = ab$ for some $b \in R$ which then implies that b is a unit and thus $J = (x)$.

More generally

Proposition 4.14. *If R is an integral domain and $0 \neq x \in R$ is not invertible then*

$$x \textit{ prime} \Rightarrow \textit{ irreducible}.$$

Proof. Let x be prime and let $x = ab$. this means that $x|ab$ and thus $x|a$ or $x|b$. If $x|a$ then $xc = a$ and thus $xcb = x$ which means that because R is an integral domain $cb = 1$. It follows that b is invertible. Similar if $x|b$. □

Proposition 4.15. *If R is a PID and $x \in R$ is a non invertible element then*

$$x \textit{ irreducible} \Rightarrow x \textit{ prime}\ .$$

Proof.

$$x \text{ irreducible} \Rightarrow (x) \text{ maximal} \Rightarrow (x) \text{ prime } \Rightarrow x \text{ prime}$$

□

As a corollary we see that:

Proposition 4.16. *If R is a PID and $x \in R$ is a non invertible element then*

$$x \textit{ irreducible} \Leftrightarrow (x) \textit{ maximal} \Leftrightarrow (x) \textit{ prime } \Leftrightarrow x \textit{ prime}$$

Example 4.17. Apply the above to $F[x]$.

RECOMMENDED EXCERCISES

IV-26 Ideals and Factor Rings. 3,18,20,22,24,26,27,30,31,38.

IV-27 Prime and maximal ideals. 24,28,30,31,32,34,35