Ideals and factor rings

Abdennour Kitouni, Anatoliy Malyarenko and Sergei Silvestrov

December 8, 2015

Abstract

Contents of the lecture.

- ☞ Homomorphisms and factor rings.
- ☞ Prime and maximal ideals.

Ring homomorphisms

Definition 1. If R and R' are rings, a **ring homomorphism** is a function $\varphi\colon R \mapsto R'$ such that

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$.
2. $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

Example 1. Let R be an integral domain, and let F be its field of quotients. The function $\varphi\colon R \mapsto F$ given by $\varphi(a) = [a, 1]$ is easily seen to be a homomorphism.

Example 2. Let R be a ring, and let $R[x]$ be its ring of polynomials. The function $\varphi\colon R \mapsto R[x]$, given by $\varphi(a) = (a, 0, \dots)$ is a homomorphism.

Example 3. Complex conjugation $z = a + bi \mapsto \overline{z} = a - bi$ is a homomorphism $\mathbb{C} \mapsto \mathbb{C}$.

Example 4. Choose $m \geq 2$ and define the ring homomorphism $\varphi\colon \mathbb{Z} \mapsto \mathbb{Z}_m$ by $f(n) = n \mod m$.

Properties of homomorphisms

Theorem 1. *If $\varphi\colon R \mapsto R'$ is a ring homomorphism, then, for all $a \in R$,*

1. *If R has unity 1, then $\varphi(1)$ is unity for $\varphi[R]$.*
2. *$\varphi(a^n) = \varphi(a)^n$ for all $n \geq 0$.*
3. *If a is a unit, then $\varphi(a)$ is a unit and $\varphi(a^{-n}) = \varphi(a)^{-n}$ for all $n \geq 1$.*

Proof. 1. For all $a \in R$,

$$\varphi(a) = \varphi(1a) = \varphi(a1) = \varphi(1)\varphi(a) = \varphi(a)\varphi(1),$$

so $\varphi(1)$ is unity for $\varphi[R]$.

2. Induction on $n \geq 0$.
3. If $ab = 1$, then $1 = f(ab) = f(a)f(b)$, so $\varphi(a^{-1}) = \varphi(a)^{-1}$. Then use induction on $n \geq 1$.

□

Kernels and ideals

Definition 2. The **kernel** of a homomorphism of rings $\varphi\colon R \to R'$ is its kernel as a map of additive groups; that is, $\mathrm{Ker}(\varphi) = \varphi^{-1}(\{0\})$.

Theorem 2. *Let $\varphi\colon R \to R'$ be a ring homomorphism, then we have:*

- *φ is one-to-one if and only if $\mathrm{Ker}(\varphi) = \{0\}$.*
- *φ is onto R' if and only if $\varphi[R] = R'$.*

Definition 3. A subset N of a ring R is an **ideal** if

1. N is an additive subgroup of R;
2. if $r \in R$ and $a \in N$, then $ar \in N$ and $ra \in N$.

Example 5. Two ideals of a ring R are R itself (**improper ideal**) and $\{0\}$ (**trivial ideal**).

Example 6. For each integer n the cyclic subgroup $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

Ideals play approximately the same role in the theory of rings as normal subgroups do in the theory of groups. For instance, let R be a ring and N an ideal of R. Since the additive group of R is abelian, N is a normal subgroup. Consequently, there is a well-defined factor group R/N in which addition is given by $(a+N)+(b+N) = (a+b)+N$. R/N can in fact be made into a ring.

A parallel with group theory

As one might suspect from the analogy with groups, ideals and homomorphisms of rings are closely related. Various isomorphism theorems for groups carry over to rings with *normal subgroups* and *groups* replaced by *ideals* and *rings* respectively. In each case the desired isomorphism

is known to exist for additive abelian groups. If the groups involved are, in fact, rings and the normal subgroups ideals, then one need only verify that the known isomorphism of groups is also a homomorphism and hence an isomorphism of rings. In particular:

Theorem 3 (Analogue of Theorem 2 (Lecture 6)). *The kernel of a ring homomorphism is an ideal.*

Factor rings from homomorphisms

Theorem 4 (Analogue of Theorem 3 (Lecture 6)). *Let R be a ring and N an ideal of R. Then the additive factor group R/N is a ring (**factor ring**) with multiplication given by*

$$(a+N)(b+N) = ab+N.$$

If R is commutative or has a unity, then the same is true of R/N.

Proof. Once we have shown that multiplication in R/N is well defined, the proof that R/N is a ring is routine. Suppose $a+N = a'+N$ and $b+N = b'+N$. We must show that $ab+N = a'b'+N$. Since $a' \in a'+N = a+N$, $a' = a+i$ for some $i \in N$. Similarly, $b' = b+j$ with $j \in N$. Consequently $a'b' = (a+i)(b+j) = ab+ib+aj+ij$. Since N is an ideal,

$$a'b'-ab = ib+aj+ij \in N.$$

Therefore $a'b'+N = ab+N$, whence multiplication in R/N is well defined. □

Example: the residue classes

Example 7 (Example 7 (lecture 6) revisited). Let $R = \mathbb{Z}$, let $R' = \mathbb{Z}_n$ and let $\gamma\colon \mathbb{Z} \mapsto \mathbb{Z}_n$ maps an integer $m \in \mathbb{Z}$ to the remainder $\gamma(m)$ when m is divided by n. γ is a homomorphism of rings.

The kernel of γ is $n\mathbb{Z}$. By Theorem 4, the factor ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. The cosets of $n\mathbb{Z}$ are the *residue classes modulo n*. The isomorphism $\gamma\colon \mathbb{Z}/n\mathbb{Z} \mapsto \mathbb{Z}_n$ assigns to each residue class its smallest nonnegative element.

Factor rings from ideals

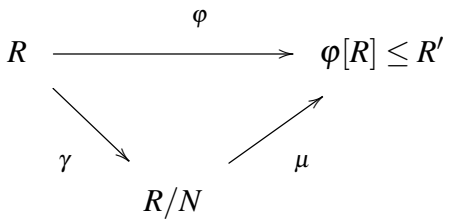
Theorem 5 (Analog of Theorem 4 (lecture 6))**.** *Let N be an additive subgroup of a ring R. The coset multiplication*

$$(a+N)(b+N) = (ab)+N$$

is well defined, independent of the choices a and b from the cosets, and makes the group R/N of left cosets into a ring if and only if N is an ideal of R.

The fundamental homomorphism theorem for rings

Theorem 6. *If $\varphi\colon R \mapsto R'$ is a homomorphism with kernel N, then $\varphi[R]$ is a ring, and $\mu\colon R/N \mapsto \mathrm{Im}(\varphi) \leq R'$ given by $\mu(a+N) = \varphi(a)$ is an isomorphism. If $\gamma\colon R \mapsto R/N$ is the homomorphism given by $\gamma(a) = a+N$, then $\varphi = \mu \circ \gamma$.*



Maximal ideals

Definition 4. An ideal M in a ring R is said to be **maximal** if $M \neq R$ and for every ideal N such that $M \subseteq N \subseteq R$, either $N = M$ or $N = R$.

Example 8. The ideal $3\mathbb{Z}$ is maximal in $\mathbb{Z}$, but the ideal $4\mathbb{Z}$ is not since $4\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$.

Maximal ideals may be characterised in terms of their factor rings.

Theorem 7 (Analogue of Theorem 8 (lecture 6))**.** *Let M be an ideal in a commutative ring R with unity $1 \neq 0$. M is maximal if and only if the factor ring R/M is a field.*

Corollary 1. *The following conditions on a commutative ring R with unity $1 \neq 0$ are equivalent.*

1. *R is a field.*
2. *R has no proper nontrivial ideals.*
3. *0 is a maximal ideal in R.*

Proof. R is isomorphic to $R/0$ and is a field if and only if 0 is maximal by Theorem 7. But clearly 0 is maximal if and only if R has no proper nontrivial ideals. □

Prime ideals

Definition 5. An ideal $P \neq R$ is said to be **prime** if for all $a, b \in R$ $ab \in P$ implies $a \in P$ or $b \in P$.

Example 9. The zero ideal in any integral domain is prime since $ab = 0$ if and only if $a = 0$ or $b = 0$.

Example 10. If p is a prime integer, then the ideal $p\mathbb{Z}$ is prime since $ab \in p\mathbb{Z}$ means that p divides ab, then p divides a or p divides b, which means that $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

Theorem 8. *In a commutative ring R with unity $1 \neq 0$ an ideal P is prime if and only if the factor ring R/P is an integral domain.*

Proof. R/P is a commutative ring with unity $1+P$ and zero element $0+P=P$ by Theorem 4.

If P is prime, then $1+P \neq P$ since $P \neq R$. Furthermore, R/P has no zero divisors since

$$\begin{aligned}(a+P)(b+P) = P &\Rightarrow ab+P = P \\ &\Rightarrow ab \in P \\ &\Rightarrow a \in P \quad \text{or} \quad b \in P \\ &\Rightarrow a+P = P \quad \text{or} \quad b+P = P.\end{aligned}$$

Therefore, R/P is an integral domain.

Conversely, if R/P is an integral domain, then $1+P \neq 0+P$, whence $1 \notin P$. Therefore, $P \neq R$. Since R/P has no zero divisors,

$$\begin{aligned}ab \in P &\Rightarrow ab+P = P \\ &\Rightarrow (a+P)(b+P) = P \\ &\Rightarrow a+P = P \quad \text{or} \quad b+P = P \\ &\Rightarrow a \in P \quad \text{or} \quad b \in P.\end{aligned}$$

Therefore, P is prime. □

Corollary 2. *If R is a commutative ring with unity $1 \neq 0$, then every maximal ideal M in R is prime.*

Proof. By Theorem 7, R/M is a field, hence an integral domain. By Theorem 8, M is prime. □

Prime fields

Theorem 9. *If F is a field, then either it is of prime characteristic p and contains a subfield isomorphic to $\mathbb{Z}_p$ or it is of characteristic 0 and contains a subfield isomorphic to $\mathbb{Q}$.*

Proof. Consider the ring homomorphism $\varphi\colon \mathbb{Z} \mapsto F$ defined by $\varphi(n) = n \cdot 1$. The kernel $\mathrm{Ker}(\varphi)$ must be an ideal in $\mathbb{Z}$. All ideals in $\mathbb{Z}$ are of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$.

If $m = 0$, then φ is one-to-one, and so there is an isomorphic copy of $\mathbb{Z}$ that is a subring of F. Its field of quotients is $\mathbb{Q}$ and is a minimal field containing the above mentioned subring. So F must contain a subfield isomorphic to $\mathbb{Q}$ and has characteristic 0.

If $m \neq 0$, the Fundamental Homomorphism Theorem gives $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ is isomorphic to $\varphi[\mathbb{Z}] \subseteq F$. Since F is a field, $\varphi[\mathbb{Z}]$ is a domain, and so m is a prime p. Now $\varphi[\mathbb{Z}] = \{0, 1, 2 \cdot 1, \ldots, (p-1) \cdot 1\}$ is a subfield of F isomorphic to $\mathbb{Z}_p$, and the characteristic of F is p. □

Definition 6. The fields $\mathbb{Q}$ and $\mathbb{Z}_p$ are **prime fields**.

Principal ideals

Definition 7. Let R be a commutative ring with unity $1 \neq 0$. The ideal $\{ra\colon r \in R\}$ is called the **principal ideal generated by** $a \in R$ and is denoted by $\langle a \rangle$. An ideal N is called **principal** if there exist $a \in R$ such that $N = \langle a \rangle$.

Theorem 10. *If F is a field, then every ideal in $F[x]$ is principal.*

Theorem 11. *The maximal ideals in $F[x]$ are the ideals $\langle f(x) \rangle$ generated by irreducible polynomials $f(x)$.*

Our basic goal and outline of its achieving

We would like to prove the following: let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. There exist a field E containing both F and a zero α of $f(x)$.

Sketch of proof.

1. Choose an irreducible factor $p(x)$ of $f(x)$ in $F[x]$ (nothing to do if $p(x)$ does not exist).
2. By Theorem 11, the ideal $\langle p(x)\rangle$ is maximal. By Theorem 7, the factor ring $E = F[x]/\langle p(x)\rangle$ is a field.
3. Find an isomorphism between F and a subfield in E.
4. Put $\alpha = x + \langle p(x)\rangle \in E$. Prove that $\varphi_\alpha(f(x)) = 0$. That is, α is a zero of $f(x)$ in E.

□