Abstract Algebra – II Rings and Algebras (环理论与代数)

2.2 Homomorphisms, Subrings, and Ideals

2012 年 11 月 26 日

Outline

Homomorphisms, Subrings, and Ideals

Corresponding to groups, the next important notion is that of a ring homomorphism:

Definition

Given two rings R and S, a ring-homomorphism (环同态) *is a map $\phi\colon R \to S$ such that ϕ is a homomorphism of the additive groups, preserves multiplication and maps $1 \in R$ to $1 \in S$, i.e.*

$$\phi(a+b) = \phi(a) + \phi(b), \tag{1}$$

$$\phi(ab) = \phi(a)\phi(b), \tag{2}$$

$$\phi(1) = 1. \tag{3}$$

Homomorphisms, Subrings, and Ideals II

We say that the ring homomorphism ϕ is injective (monomorphism, embedding) *iff* $\ker\phi := \{r \in R : \phi(r) = 0\} = \{0\}$. *We say that ϕ is* surjective (epimorphism) *iff* $\operatorname{im}\phi := \phi(R) := \{\phi(r) : r \in R\} = S$. *We say that ϕ is an* isomorphism *iff it is injective and surjective. In the latter case we also say that R is* isomorphic *to S ($R \cong S$ via ϕ).*

Example

Consider the map $e\colon \mathbb{Z} \to \mathbb{Q} : z \mapsto z/1$. Clearly this is a ring homomorphism. Note that its kernel is $\ker e = \{0\}$, thus it is an embedding and so $\mathbb{Z}$ operates inside $\mathbb{Q}$.

Subrings, and Ideals I

Analogous to groups, we are also lead to the following two notions:

Definition

Given a (unital) ring R, then a subring (环子) *is a subset $S \subset R$ that forms a (unital) ring under the same operations.*
An ideal (理想) *$I \triangleleft R$ is an additive subgroup $I \subset (R, +)$ such that $RI \subset I$.*

Example

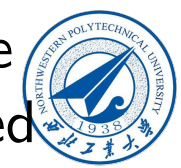
0. The trivial ideals are 0 and R. The latter also is the trivial subring. The smallest possible subring is $\langle 1 \rangle \subset R$, i.e. the image of the following ring homomorphism
$\phi_0 : \mathbb{Z} \to R : n \mapsto n \cdot 1$.

Examples of Subrings and Ideals I

1. It also follows that $\ker\phi \triangleleft R$ is an ideal and $\operatorname{im}\phi \subset S$ is a subring for every ring homomorphism $\phi\colon R \to S$.
2. Note further that $1 \in I$ implies $I \supset RI = R$, i.e. the ideal automatically is trivial.
3. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are subrings.
4. Starting from a field F, we see that for every nonzero ideal $(0) \neq I \triangleleft F$ there is a non-zero element $i \in I$ and thus $FI \supset Fi = F$, i.e. the ideal is already the whole field F. Thus fields only have trivial ideals. In particular the only homomorphisms between fields are embeddings (because $\phi(1) = 1 \neq 0$ implies $\ker\phi \neq F$).
5. Note that the $(n) := nR$ for $n \in R$ are the principal ideals (主理想) of R. In particular the Euclidean algorithm shows that all ideals of $\mathbb{Z}$ are of this form ($\{0\} = (0)$).

Examples of Subrings and Ideals II

6. Given a family of ideals $\{I_\alpha : \alpha \in A\}$ then their intersection $\bigcap_{\alpha\in A} I_\alpha$ is an ideal (analogously to normal subgroups). We call an ideal I irreducible (不可约理想) iff it cannot be written as the intersection of two different ideals.
7. Given a ring $(R, +, \cdot)$ we can construct further ideals in the following way. Let $\{a_j \in R : j \in J\}$ be ring elements and consider the smallest ideal that contains all elements a_j, i.e. $\bigcup_{\{a_j\}\subset I\lhd R} I \lhd R$. If there are only finitely many elements, we denote their generated ideal (生成理想) as $(a_1, \ldots, a_n)$.
8. Given two ideals $I, J \lhd R$, then their sum $I + J$ is another ideal, because $(I + J)R = IR + JR \subset I + J$. In this way the ideal generated by the elements a_j for $j \in J$ is $\sum_{j\in J}(a_j) \lhd R$, i.e. the sum of principal ideals. Endowed with these two operations the ideals of a ring form a *distributive lattice (分配格)* where we can also write $\vee$ for $+$, because $I + J$ is the ideal generated



Examples of Subrings and Ideals III

by $I \cup J$. You should show the distributive law ($I \cap (J + K) = I \cap J + I \cap K$ or equivalently $(I + J) \cap K = I \cap K + J \cap K$ for all ideals $I, J, K \triangleleft R$) as a homework.

9. Given two ideals $I, J \triangleleft R$, then their product is defined as $IJ := \langle ij : i \in I, j \in J \rangle_R$. Note that this also contains finite sums of products of elements. Clearly $RIJ \subset IJ$ and $IJ \subset I \cap J$, but in general it is not the same, e.g. $I = J = (x+1) \triangleleft \mathbb{R}[x]$, then $I^2 = (x+1)^2\mathbb{R}[x] \subsetneq (x+1)\mathbb{R}[x]$. Also this product is distributive over the addition, i.e. $I(J + K) = IJ + IK$ for ideals $I, J, K \triangleleft R$.
10. Given a ring R. Its nilradical (诣零根) is the set $\operatorname{nil\,rad} R := \sqrt{(0)} := \{z \in R : z^n = 0 \text{ for some } n \in \mathbb{N}\}$. In the homework you will show that this is an ideal.

Factor ring (商环)

Remark

Note that in the case of non-commutative (associative) algebras, we need to distinguish between left ideals ($RI \subset I$), right ideals ($IR \subset I$) and two-sided ideals (both). The kernel of an algebra homomorphism is both. Also for the following construction we need a two-sided ideal.

Another construction that follows immediately is that of a quotient ring by an ideal:

Factor ring (商环) II

Proposition (Factor ring)

Given a non-trivial ideal $I \triangleleft R$, then the space of cosets R/I has an induced ring structure via representatives $(a+I)+(b+I)=(a+b)+I$, $(a+I)(b+I)=ab+I$ *with* $0+I=I$ *and* $1+I$ *being the neutral elements. Moreover the projection* $\pi: R \to R/I$ *is a surjective ring homomorphism. This is denoted the* quotient ring (商环).

Proof.

Since $RI \subset I$ and for $1 \in R$, we see that the multiplication is indeed the operation on the sets and thus representative independent. Also for $1 \notin I$ it is clear that $1+I \neq I$, i.e. the quotient ring is indeed unital. □

Factor ring (商环) III

Example

Given any principal ideal $(n) \triangleleft R$, we obtain a quotient ring $R/(n)$. Particular examples are the integers modulo n where $n \in \mathbb{Z}$.

Lemma

Given a ring homomorphism $\phi\colon R \to S$ and an ideal $I \triangleleft R$, then ϕ factors through the projection $\pi\colon R \to R/I$,i.e. $\phi = \bar{\phi} \circ \pi$ for some homomorphism $\bar{\phi}\colon R/I \to S$, iff $\ker \phi \subset I$. In this case ϕ factors uniquely. □

Isomorphism theorems

Also analogous to groups we have the standard isomorphism theorems:

Theorem (First isomorphism theorem)

Given a ring homomorphism $\phi\colon R \to S$*, then* $R/\ker\phi \cong \operatorname{im}\phi$*.* □

Theorem (Second isomorphism theorem)

Given two ideals $I, J \triangleleft R$ *with* $I \subset J$*, then* ($I \triangleleft J$ *is an ideal in the non-unital ring* J)*,* $J/I \triangleleft R/I$ *is an ideal and*

$$(R/I)/(J/I) \cong R/J.$$

The proof is left as an exercise.

Isomorphism theorems II

Theorem (Third isomorphism theorem)

Given a subring $S \subset R$ and an ideal $I \triangleleft R$, then $S + I \subset R$ is a subring, $S \cap I \triangleleft S$ is an ideal, and

$$(S + I)/I \cong S/(S \cap I)$$

Also this proof is left as an exercise.

Proposition (Characteristic)

Given any (commutative unital) ring $(R, +, \cdot, 1)$ there is a canonical ring homomorphism $\phi_0 \colon \mathbb{Z} \to R : n \mapsto n \cdot 1$. Its kernel is an ideal in $\mathbb{Z}$ and thus generated by a unique non-negative element $n \in \mathbb{N}$. We call this $n = \operatorname{char} R$ the characteristic (特征) *of R. In particular ϕ_0 factors to $\bar{\phi} \colon \mathbb{Z}/(n) \hookrightarrow R$.*

Exercises

Exercise

a. Show that the union $\bigcup_{n\geq 0} S_n$ of an ascending chain of subrings $\langle 1\rangle \subset S_1 \subset S_2 \subset \cdots \subset R$ is a subring of R.

b. What happens for ascending chains of ideals?

c. Show that every intersection of subrings $S_\alpha \subset R$, $\alpha \in A$ is a subring $\bigcap_{\alpha\in A} S_\alpha \subset R$.

d. Show the corresponding fact for ideals.

Exercise

Let $I, J \lhd R$ be ideals. Show that $I \cup J$ is an ideal iff $I \subset J$ or $J \subset I$.

Exercises II

Exercise

Given any ring R. Show that the nil radical $\operatorname{nil\,rad} R := \{z \in R : z^n = 0 \text{ for some } n \in \mathbb{N}\}$ is an ideal. What is the nil radical of $\mathbb{Z}$?

Exercise

Prove the isomorphism theorems for rings (Theorem 2.2.9, 2.2.10, and 2.2.11, respectively).

Exercises III

Exercise

Given any ring homomorphism $\phi\colon R \to R'$. Show the following

a. a chain of subrings $S_1 \subset S_2 \subset R$ corresponds to a chain of subrings $S_1' \subset S_2' \subset R'$ where $S' := \phi(S) \subset R'$;

b. any chain of subrings $S_1' \subset S_2' \subset R'$ corresponds to a chain of subrings $\ker\phi \subset S_1 \subset S_2 \subset R$ where $S := \phi^{-1}(S') := \{r \in R : \phi(r) \in S'\}$;

c. any chain of ideals $I_1' \subset I_2'$ with $I_k' \lhd R'$ corresponds to a chain of ideals $\ker\phi \subset I_1 \subset I_2$ with $I_k := \phi^{-1}(I) \lhd R$;

d. ϕ and ϕ^{-1} also preserve intersections (of subrings or ideals) and sums and products of ideals.

Exercises IV

Exercise

Let $\phi\colon R \to R'$ be a ring homomorphism and $I \triangleleft R$ an ideal.

a. Assuming that ϕ is surjective, show that $\phi(I) \triangleleft R'$ is an ideal.

b. Given the results in Exercise 2.2.5 and a surjective ϕ, show that there is a 1:1 correspondence between ideals $\ker\phi \subset I_1 \subset I_2$ with $I_k \triangleleft R$ and $I'_1 \subset I'_2$ with $I'_k \triangleleft R'$.
Hint: You also have to show uniqueness of $\ker\phi \subset I \triangleleft R$ with $\phi(I) = I'$ for any fixed $I' \triangleleft R'$.

c. Give an example where $\phi(I)$ is not an ideal.