Graduate Algebra, Fall 2014
Lecture 25

Andrei Jorza

2014-10-29

2 Rings

2.1 Basics

2.1.2 Integral Domains (continued)

Proposition 1. *If R is a domain and $ab = ac$ then $a = 0$ or $b = c$. If R is finite then it is a field.*

Proof. $ab - ac = 0$ implies $a(b - c) = 0$ so either $a = 0$ or $b = c$. □

2.1.3 Subrings

Definition 2. A subring of a ring R is a ring $S \subset R$ inheriting $+$ and $\cdot$ from R.

Example 3.

1. $\mathbb{Z}$ is a subring of $\mathbb{Q}$.
2. R is a subring of $M_n(R)$.
3. $\mathbb{Z}[\sqrt{5}]$ is a subring of $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ which is a subring of $\mathbb{Q}(\sqrt{5})$.
4. $R[X]$ is a subring of $R[\![X]\!]$.

2.1.4 Homomorphisms

Definition 4. Let R, S be two rings. A **homomorphism** $f : R \to S$ is a map which is a homomorphism of abelian groups for $+$ and a homomorphism of monoids for $\cdot$.

Lemma 5. *Let $f : R \to S$ be a homomorphism.*

1. *Then the kernel $\ker f = \{x \in R | f(x) = 0\}$ is 0 iff f is injective.*
2. *If f is bijective then f^{-1} is also a homomorphism and f is said to be an isomorphism.*

Example 6.

1. Inclusion of a subring into a ring.
2. $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with kernel $n\mathbb{Z}$.
3. $R[X] \to R$ given by evaluation at $X = a \in R$ is a homomorphism.

2.2 Ideals

2.2.1 Basic examples

Definition 7. A **left ideal** of a ring R is a subset $I \subset R$ which is an abelian group wrt $+$ and $RI = I$. It is a **right ideal** if $IR = I$. It is a **two-sided ideal** if $RI = IR = I$.

Example 8.

1. $\langle n \rangle = n\mathbb{Z} \subset \mathbb{Z}$.
2. $\langle P(X) \rangle = P(X)R[X] \subset R[X]$.
3. $\langle r \rangle = rR \subset R$.
4. $\langle p, X \rangle = p\mathbb{Z}[X] + X\mathbb{Z}[X] \subset \mathbb{Z}[X]$ is an ideal.
5. If $r_1, \ldots, r_k \in R$ then $\langle r_1, \ldots, r_k \rangle_r = \sum r_i R$ is a right ideal. The set $\langle r_i \rangle_l = \sum R r_i$ is a left-ideal.

Definition 9. If I is a two-sided ideal of R then the abelian group quotient R/I is a ring. Indeed, it is an abelian group and we need to check that it is a monoid wrt multiplication. Let $r, s \in R$. Then $(r + I)(s + I) = rs + rI + Is + I^2 = rs + I$.

2.2.2 Operations on ideals

Lemma 10. *Let R be a ring and $I, J \subset R$ be two ideals. Then*

1. *$I \cap J$ is an ideal of R.*
2. *$I + J = \{i + j | i \in I, j \in J\}$ is an ideal of R.*
3. *$IJ = \{\sum i_k j_k | i_k \in I, j_k \in J\}$ is an ideal of R.*

Example 11.

1. $m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}$.
2. $m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$
3. $m\mathbb{Z}n\mathbb{Z} = mn\mathbb{Z}$.
4. If $I = \langle i_1, \ldots, i_m \rangle$ and $J = \langle j_1, \ldots, j_n \rangle$ then $IJ = \langle i_u j_v | 1 \leq u \leq m, 1 \leq v \leq n \rangle$.
5. In $\mathbb{Z}[X]$ have
$$I = (2, X)(3, X) = (6, 2X, 3X, X^2)$$
Since $3X, 2X \in I$, it follows that $X \in I$ and if $X \in I$ then automatically $2X, 3X, X^2 \in I$ so
$$I = (6, X)$$

2.2.3 Isomorphism theorems

Theorem 12. *Let $f : R \to S$ be a homomorphism of rings.*

1. *Then $\ker f$ is an ideal of R and $\operatorname{Im} f$ is a subring of S.*
2. *If I is an ideal of R then $f : R \to R/I$ is a surjective homomorphism with kernel I.*
3. *$R/\ker f \cong \operatorname{Im} f$.*

Proof. (1): If $f(x) = 0$ and $r \in R$ then $f(rx) = f(r)f(x) = 0$ so $rx \in \ker f$ which implies that $\ker f$ is an ideal. Also $f(x) + f(y)f(z) = f(x + yz)$ so $\operatorname{Im} f$ is a subring of S.

(2): The map $x \mapsto x + I$ is the homomorphism f and clearly has kernel I and is surjective.

(3): This is an isomorphism of groups the map begin $x + \ker f \mapsto f(x)$. Note that this map is also multiplicative and so the bijection of groups respects $+$ and $\cdot$ and so is a ring homomorphism.

□

Theorem 13. *Let R be a ring, $A \subset R$ a subring and $I \subset R$ an ideal.*

1. $A + I = \{a + i | a \in A, i \in I\}$ *is a subring of R.*
2. $A \cap I$ *is an ideal of A.*
3. $(A + I)/I \cong A/(A \cap I)$.

Proof. (1): $A + I$ contains $1 = 1 + 0$ and is closed under $+$ and $\cdot$ and so is a subring.

(2): $A(A \cap I) \subset A^2 \cap AI = A \cap I$ so is an ideal.

(3): This is an isomorphism of additive groups (from group theory) and the map is given by $a + i + I \mapsto a + I$. This bijection respects multiplication as well and so is a ring homomorphism. □