Graduate Algebra, Fall 2014
Lecture 26

Andrei Jorza

2014-10-31

2 Rings

2.2 Ideals (continued)

2.2.3 Isomorphism theorems (continued)

Theorem 1. *Let R be a ring and $I \subset J \subset R$ ideals. Then*

1. *The abelian group quotient J/I is an ideal of R/I.*
2. *$(R/I)/(J/I) \cong R/I$.*

Proof. (1): $(R/I)(J/I) = RJ/I = J/I$ so J/I is an ideal of R/I.

(2): Again, this is an isomorphism of additive groups. The map is $(r + I) + J/I \mapsto r + I$. This respects multiplication so the bijection is in fact a ring isomorphism. □

2.2.4 The Chinese Remainder Theorem

Definition 2. We say that I and J are coprime if $I + J = R$.

Proposition 3. *Let R be a ring and $I_1, \dots, I_n$ be pairwise coprime ideals. Then*

$$R/I_1 \cdots I_n \cong R/I_1 \oplus \cdots \oplus R/I_n$$

via the map sending $r + I_1 \cdots I_n$ to $(r + I_1, \dots, r + I_n)$.

Proof. By induction. It suffice to show that if $I + J = R$ then $R/IJ \cong R/I \oplus R/J$ and if I, J, K are pairwise coprime then I and JK are coprime.

First, if $I + J = R$ and $I + K = R$ then $a + b = 1$ and $c + d = 1$ for $a, c \in I$, $b \in J$ and $d \in K$. Then $bd = (1 - a)(1 - c) = 1 - a - c + ac \in 1 + I$ and so $bd \in JK \cap (1 + I)$ showing that $I + JK = (1) = R$.

Next, suppose $I + J = R$ so $a + b = 1$ with $a \in I$ and $b \in J$. The map $R/IJ \to R/I \oplus R/J$ sending $r + IJ \to (r + I, r + J)$ is a homomorphism. Suppose $r + I = I, r + J = J$ so $r \in I \cap J$. Then $r = r(a + b) = ra + rb$. But $ra \in (I \cap J)I \subset IJ$ and $rb \in (I \cap J)J \subset IJ$ and so $r \in IJ$. Thus the map is injective. For surjectivity, note that if $x + I \in R/I$ and $y + J \in R/J$ then $r = xb + ya$ has the property that $r + I = xb + I = x(1 - a) + I = x + I$ (as $a \in I$) and similarly $r + J = y + J$. Thus $r + IJ$ maps to $(x + I, y + J)$ yielding surjectivity. □

2.3 Special types of ideals

2.3.1 Prime and maximal ideals

Definition 4. An ideal $\mathfrak{p} \subset R$ is **prime** if $R/\mathfrak{p}$ is an integral domain. An ideal $\mathfrak{m} \subset R$ is maximal if $R/\mathfrak{m}$ is a field.

Lemma 5. *An ideal $\mathfrak{p}$ is prime if and only if for every $x, y \in R$ such that $xy \in \mathfrak{p}$ it follows that $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.*

Example 6.

1. $p\mathbb{Z} \subset \mathbb{Z}$ is prime and maximal if p is a prime.
2. If $P(X)$ is an irreducible polynomial in $F[X]$ for a field F then $(P(X))$ is a prime and maximal ideal.
3. The ideal $(p) \subset \mathbb{Z}[X]$ is prime but not maximal. The ideal $(p, X) \subset \mathbb{Z}[X]$ is maximal. Indeed, by the isomorphism theorem, $\mathbb{Z}[X]/(p, X) \cong (\mathbb{Z}[X]/(X))/((p, X)/(X)) \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ which is a field.
4. From the homework: if $\mathfrak{p} \subset R$ is a prime ideal then $\mathfrak{p}[X] \subset R[X]$ is a prime ideal.
5. If $\mathfrak{m} = (x_1, \ldots, x_n) \subset F[x_1, \ldots, x_n]$ then $\mathfrak{m}^k$ consists of polynomials with each monomial of degree at least k.

Lemma 7 (Zorn's lemma)**.** *Suppose S is a partially ordered set. An ascending chain T in S is a totally ordered subset of S. If every such T has a supremum $\max(T) \in S$ then S contains a supremum $\max(S)$ in S.*

Proof. This is equivalent to the axiom of choice. □

Proposition 8. *Let R be a commutative ring and $I \neq R$ an ideal. Then $I \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset R$.*

Proof. Consider S the set of proper ideals of R containing I. Since $I \in S$, the set S is nonempty. Order S partially with respect to inclusion. Suppose $T \subset S$ is an ascending chain of ideals. Then $I_T = \cup_{I \in T} I$ is also an ideal. Indeed, if $x \in I_T$ and $r \in R$ then $x \in I$ for some $I \in T$ and so $xr \in I \subset I_T$. Moreover, $I_T \neq R$ because otherwise $1 \in I \in T$ for some I and this would imply $I = R$. By Zorn's lemma this implies that S has a maximal element $\mathfrak{m}$ which is clearly a proper ideal of R containing I.

Let's show that $\mathfrak{m}$ is a maximal ideal. Suppose $r \in R/\mathfrak{m}$ is nonzero, we'd like to show that it has an inverse. Since $r \notin \mathfrak{m}$, the ideal $\mathfrak{n} = \mathfrak{m} + (r)$ contains $\mathfrak{m}$ properly. By maximality of $\mathfrak{m}$, it follows that $\mathfrak{n}$ (which is an ideal containing I) cannot be proper so $\mathfrak{n} = R$ so $1 \in R = \mathfrak{m} + (r)$ can be written as $1 = u + rs$ for $u \in \mathfrak{m}$ and $s \in S$. But then $rs = 1$ in $R/\mathfrak{m}$ as desired. □

2.3.2 Radicals

Definition 9. A **nilpotent** element of a ring R is $x \in R$ such that $x^n \in R$. The set of nilpotent elements of a ring R is called the nilradical $\mathrm{Nil}(R)$.

Definition 10. Let $I \subset R$ be an ideal. The **radical** of I is the set $\sqrt{I} = \{x \in R | x^n \in I \text{ for some } n \geq 1\}$.

Example 11.

1. $\mathrm{Nil}(R) = \sqrt{(0)}$.
2. Let $R = \mathbb{Z}[x, y]$ and $I = (x, y^3)$. What is $\sqrt{I}$? We seek polynomials $P(x, y) \in \mathbb{Z}[x, y]$ such that $P(x, y)^n \in (x, y^3)$ for some $n \geq 1$. Write $P(x, y) = a + yF(y) + xG(x, y)$. We need $P(x, y)^n = (a + yF(y) + xG(x, y))^n$ to be in $(x, y^3) = x\mathbb{Z}[x, y] + y^3\mathbb{Z}[x, y]$. But $P(x, y)^n = (a + yF(y))^n + x \cdot \text{polynomial}$ is in (x, y^3) iff $(a + yF(y))^n \in (x, y^3)$ iff $(a + yF(y))^n \in (y^3)$. This is equivalent to $a^n + na^{n-1}yF(y) + \binom{n}{2}a^{n-2}y^2F(y)^2 \in (y^3)$. Thus we need $a^n = 0$ so $a = 0$ and this is sufficient. Therefore $P(x, y) = yF(y) + xG(x, y) \in (x, y)$ so $\sqrt{(x, y^3)} = (x, y)$.