Math 210A Lecture 23 Notes

Daniel Raban

November 26, 2018

1 Principal Ideal Domains, Maximal Ideals, and Prime Ideals

1.1 Group extensions

Definition 1.1. A **(short) exact sequence** of groups is a sequence

$$1 \longrightarrow N \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1$$

where ι is injective, π is surjective, and $\mathrm{im}(\iota) = \ker(\pi)$.

Definition 1.2. A **group extension** of G by N is a group E, where

$$1 \longrightarrow N \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1$$

is exact. If $E = N \rtimes_\varphi G$, we call it a **split extension**.

1.2 Simple rings and ideals

Proposition 1.1. *A ring is a division ring iff it has no nonzero proper left ideals.*

Proof. ($\implies$): Let $I \neq 0$ be a left ideal of R¿ If $r \in I \setminus \{0\}$, then $r \in R^\times$, so $1 \in I$. So $I = R$.

($\impliedby$): Let $r \in R \setminus \{0\}$. $Rr = R$, so there exists some $u \in R$ such that $ur = 1$. $Ru = R$, so there exists some $s \in R$ such that $su = 1$. Then $s = sur = r$. Then r has a left and a right inverse, so $r \in R^\times$. $\square$

Definition 1.3. A ring with no nonzero proper (two-sided) ideals is called **simple**.

Example 1.1. Let D be a division ring, and let $M_n(D)$ be the ring of $n \times n$ matrices with entries in D. Let $e_{i,j}$ be the matrix with 0 in every entry but (i, j) and a 1 in the (i, j) coordinate. Then $M_n(D)e_{i,j}$ is the set of matrices which are 0 outside of the j-th column.

Similarly, $e_{i,j}M_n(D)$ is the set of matrices which are 0 outside of the i-th row. So the two sided ideal $(e_{i,j}) = M_n(D)$.

To show that $M_n(D)$ is simple, let $A \in M_n(D) \setminus \{0\}$, and suppose that $a_{i,j} \neq 0$ for some i, j. Then $e_{i,i}Ae_{j,j} = a_{i,j}e_{i,j}$. Since $a_{i,j} \neq 0$, $a_{i,j} \in D^\times$,which means that $e_{i,j} \in (A)$. So $(A) = M_n(D)$.

Let I, J be ideals in a ring. Then IJ is the span of ab, with $a \in I$ and $b \in J$. In general, $IJ \subseteq I \cap J$.

Let (I_α) be a system of ideals, totally ordered under containment. Then $\bigcup_\alpha I_\alpha$ is an ideal (this is also true for left or right ideals).

Theorem 1.1 (Chinese remainder theorem). *Let $I_1, \dots, I_k$ be "pairwise coprime," i.e. $I_j + I_i = R$ for $j \neq i$. Then*

$$R/\bigcap_{i=1}^k \cong \prod_{i=1}^k R/I_i.$$

Proof. The proof is basically the same as the proof that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}.m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$, where $n = m_1 \cdots m_k$ and the m_i are coprime. □

1.3 Principal ideal domains

Definition 1.4. A **(left) zero divisor** $r \in R \setminus \{0\}$ is an element such that there exists some $s \in \mathbb{R} \setminus \{0\}$ with $rs = 0$. A **zero divisor** is a left and right zero divisor.

Definition 1.5. A **domain** is a commutative ring without zero divisors.

Definition 1.6. A **principal ideal domain (PID)** is a domain in which every ideal is principal (generated by 1 element).

Example 1.2. $\mathbb{Z}$ is a PID.

Example 1.3. If F is a field, then $F[x]$ is a PID. How do we divide polynomials? There is a map $\deg : F[x] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}$ such that $\deg(f) \geq 0$ if $f \neq 0$ and $\deg(f) = 0$ iff f is constant and nonzero. If $f, g \in F[x]$ with $g \neq 0$, then $= qg + r$, where $q, r \in F[x]$ and $\deg(r) < \deg(f)$.

Proposition 1.2. *If F is a field, then $F[x]$ is a PID.*

Proof. Let I be a nonzero ideal. Choose $g\ inI \setminus \{0\}$ for minimal degree. If $f \in I$, write $f = qg + r$ with $r \in I$ and $\deg(r) < \deg(g)$. Then $r = 0$, so $f \in (g)$. Hence, $I = (g)$. □

Definition 1.7. An element π of a commutative ring R is **irreducible** if whenever $\pi = ab$ with $a, b \in R$, either $a \in \mathbb{R}^\times$ or $b \in R^\times$.

Definition 1.8. Two elements $a, b \in R$ are **associate** if there exists $u \in R^\times$ such that $a = ub$.

Example 1.4. The irreducible elements in $\mathbb{Z}$ are $\pm$ primes.

Example 1.5. The irreducible elements in $F[x]$ are the (nonconstant) irreducible polynomials.

If $f \in F[x]$, we get a function $f : F \to F$. But this does not necessarily go both ways. Let $f = x^p - x = x(x^{p-1} - 1)$, where $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then $f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_p$, but $f \neq 0$ since $\deg(f) = p$.

1.4 Maximal and prime ideals

Definition 1.9. An ideal of a ring is **maximal** if it is proper and not properly contained in any proper ideal.

Definition 1.10. An ideal p of a commutative ring is **prime** if it is proper, and whenever $ab \in p$ for $a, b \in R$, then $a \in p$ or $b \in p$.

Proposition 1.3. *Principal prime ideals in a domain are generated by irreducible elements.*

Proof. If $p = (\pi)$ is prime and $ab = \pi \in (p)$, then either $a \in p$ or $b \in p$. So $a = s\pi$ or $b = t\pi$. Without loss of generality, $a = s\pi$. So $(bs - 1)\pi = 0$, which means that $b = s^{-1} \in R^\times$. $\square$

Example 1.6. In $\mathbb{Z}$ and $F[x]$, nonzero prime and maximal ideals are the same. However, in $F[x, y]$, the ideal (x) is prime but not maximal. The ideal (x, y) is prime and maximal. In the ring $\mathbb{Z}[x]$, (p, x) is maximal if p is prime. But (p) and (x) are prime but no maximal.

Lemma 1.1. *An element $m \subsetneq R$ is maximal iff R/m is a division ring. If R is commutative, then $p \subsetneq R$ is prime iff R/p is an integral domain.*

Proof. The key is that ideals in R/I are in correspondence with ideals of R containing I. When $I = m$, if R/m is a division ring, then the ideals in R/m are $0, R/m$. Then the only ideals in R containing m are m and R.

If p is prime, then $ab \in p$ implies that $a \in p$ or $b \in p$. So $a + p = p$ or $b + p = p$. This is equivalent to $\overline{a}\overline{b} = (a+p)(b+p) = p$. If R/p is an integral domain, then $ab \in p \iff \overline{a}\overline{b} = 0$, so $\overline{a} = 0$ or $\overline{b} = 0$. This is equivalent to $a \in p$ or $b \in p$. $\square$

Lemma 1.2 (Zorn's lemma)**.** *Let X be a partially ordered set. Suppose that every chain (totally ordered subset) in X has an upper bound (an upper bound $x \in X$ of a set $S \subseteq X$ is such that $s \leq x$ for all $s \in S$. Then X has a maximal element ($x \in X$ such that if $y \in X$ and $x \leq y$, then $y = x$).*

This is equivalent to the axiom of choice.

Theorem 1.2. *Every ring has a maximal ideal.*

Proof. Let X be the set of proper ideals in R. If $C \subseteq X$ is a chain, then $\bigcup_{N \in C} N$ is an upper bound for C. So X has a maximal element which is a maximal ideal. $\square$