These are some notes from my Algebra I class. We use the textbook *Abstract Algebra* by Dummit and Foote, and will cover rings, groups, and modules.

PIDs, UFDs and All That

We always assume here that R is commutative and unital.

Preliminaries

Definition: If $a_1, \dots, a_n \in R$, then the *ideal generated by* $a_1, \dots, a_n$ is given by

$$(a_1, \dots, a_n) := \bigcap \{I \mid a_1, \dots, a_n \in I, I \text{ is an ideal in } R\}.$$

An ideal is called *principal* if $I = (a)$ for some $a \in I$. We may write $I = a \cdot R$ in this case. A ring where every ideal is principal is called a *principal ideal domain*.

Definition: If I and J are ideals in R, then IJ is given by

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \,\middle|\, x_i \in I, y_i \in J, n \in \mathbb{N} \right\}.$$

Theorem (Isomorphism Theorems)**:**

First Isomorphism Theorem: Let $\varphi \colon R \to S$ be a ring homomorphism. Then, $\overline{\varphi} \colon R/\ker(\varphi) \to \operatorname{im}(\varphi)$ is an isomorphism given by $\overline{\varphi}(a + \ker(\varphi)) = \varphi(a)$.

Second Isomorphism Theorem: Let R be a ring, $S \subseteq R$ a subring, and let $I \subseteq R$ be an ideal. Then,

(i) $I + S$ is a subring of R;

(ii) I is an ideal of $I + S$;

(iii) $I \cap S$ is an ideal of S;

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

Third Isomorphism Theorem: Let R be a ring, I, J ideals of R with $I \subseteq J$. Then, J/I is an ideal of R/I, and we have $(R/I)/(J/I) \cong R/J$.

Fourth Isomorphism Theorem: If R is a ring and I is an ideal, then there is a one-to-one correspondence between subrings of R/I and subrings of R containing I.

Definition: Let M be an ideal in R.

(i) We say M is prime if $M \neq R$ and, for any $ab \in M$, we have either $a \in M$ or $b \in M$.

(ii) We say M is maximal if $M \neq R$ and if $M \subseteq I \subseteq R$ where I is an ideal, then either $I = M$ or $I = R$.

Theorem: Let M be an ideal in R.

(i) M is prime if and only if R/M is an integral domain.

(ii) M is maximal if and only if R/M is a field.

Proof.

(i) Let M be maximal, with $a + M \in R/M$, $a + M \neq 0 + M$. Then, $a \notin M$, so that the ideal $(a) + M$ strictly contains M. Therefore, $1 + M \in (a) + M$, meaning there is some $r + M$ such that $(r + M)(a + M) = 1 + M$. Thus, an inverse exists.

Now, if R/M is a field, and $M \subsetneq I \subseteq R$, then I/M is an ideal of R/M, and since $I \supsetneq M$, we have

$I/M \neq 0 + M$. Since R/M is a field, its only ideals are either $0 + M$ and R/M, so $I/M = R/M$, meaning $I = R$.

(ii) We have $P \subseteq R$ is prime if and only if $ab \in P$ implies $a \in P$ or $b \in P$. Yet, means that $ab + P = 0 + P$ if and only if $a = 0 + P$ or $b = 0 + P$.

□

Chinese Remainder Theorem

Definition: We say two ideals I and J are *coprime* if $I + J = R$, or that there exist $x \in I$ and $y \in J$ such that $x + y = 1$.

Theorem (Chinese Remainder Theorem)**:** Let $I_1, \dots, I_n$ be pairwise coprime ideals of R. Then, for any $a_1, \dots, a_n \in R$, there exists $x \in R$ with $x \equiv a_i$ modulo I_i for all i. In other words, there a solution to the system of congruences given by

$$\begin{aligned} x + I_1 &= a_1 + I_1 \\ x + I_2 &= a_2 + I_2 \\ &\vdots \\ x + I_n &= a_n + I_n. \end{aligned}$$

Proof. It suffices to construct elements $y_1, \dots, y_n$ such that $y_i \equiv 1$ modulo I_i and 0 otherwise. Then, we will be able to set $x = \sum_i a_i y_i$ as our desired solution.

We construct y_1 as follows. From our assumption, $I_1 + I_j = R$ for all $j \geqslant 2$, so for each $j \geqslant 2$, there exists $u_j \in I_1$ and $v_j \in I_j$ such that $u_j + v_j = 1$. Taking the product, we find that

$$\begin{aligned} \prod_{j=2}^{n} (u_j + v_j) &= 1 \\ &= \underbrace{v_2 \cdots v_n}_{=:y_1} + \underbrace{\cdots + u_2 \cdots u_n}_{=:x_1}. \end{aligned}$$

We verify that y_1 does the job, which we can see by the fact that $y_1 \equiv 0$ modulo I_j for $j \neq 1$, as $v_2 \cdots v_j \in I_2 \cdots I_j \subseteq I_j$ for each $j \geqslant 2$. Similarly, each summand in x_1 contains at least one u_j, so $x_1 \equiv 0$ modulo I_1.

The rest of the y_i follow analogously. □

We can restate the Chinese Remainder Theorem in a variety of ways.

Theorem (Chinese Remainder Theorem, Alternative Versions)**:** Let $I_1, \dots, I_n$ be pairwise coprime ideals.

(i) There exists a surjective homomorphism

$$\begin{aligned} \varphi \colon R &\rightarrow R/I_1 \times \cdots \times R/I_n \\ r &\mapsto (r + I_1, \dots, r + I_n). \end{aligned}$$

This homomorphism induces an isomorphism

$$\overline{\varphi} \colon R/(I_1 \cap \cdots \cap I_n) \rightarrow R/I_1 \times \cdots \times R/I_n.$$

(ii) If $I_1, \dots, I_n$ are pairwise coprime, then

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

are isomorphic.

Example: We observe that if $R = \mathbb{Z}$, and $p_1, \dots, p_r$ are distinct primes with $\ell_1, \dots, \ell_r$ positive integers, then

$$\mathbb{Z}/p_1^{\ell_1} \cdots p_r^{\ell_r}\mathbb{Z} \cong \mathbb{Z}/p_1^{\ell_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\ell_r}\mathbb{Z}.$$

Example (Polynomial Interpolation)**:** If we let

$$p_i(x) = x - \alpha_i,$$

where $\alpha_i \in \mathbb{F}$, we observe that there is a surjective evaluation homomorphism

$$\mathrm{ev}\colon \frac{\mathbb{F}[x]}{(p_i(x))} \to \mathbb{F},$$

given by $f(x) \mapsto f(\alpha_i)$. In particular, if $\alpha_1, \dots, \alpha_r$ are distinct, then

$$\frac{\mathbb{F}[x]}{(p_1(x), \dots, p_r(x))} \cong \mathbb{F} \times \cdots \times \mathbb{F},$$

so that, for all $\beta_1, \dots, \beta_r \in \mathbb{F}$, there is some $f(x) \in \mathbb{F}[x]$ such that $f(\alpha_i) = \beta_i$ for $i = 1, \dots, r$.

Field of Fractions and Localization

Given a ring R, how can we find maximal ideals in R? More specifically, given a commutative ring R with 1, and prime ideal $P \subseteq R$, we want to construct a new ring R_p with unique maximal ideal P.

Toward this end, we start by reviewing a useful construction known as the field of fractions.

Definition: Let R be an integral domain. We define the field $K = \mathrm{frac}(R)$ to be the unique field with an injection

$$\begin{aligned} \iota\colon R &\hookrightarrow K \\ 1_R &\mapsto 1_K, \end{aligned}$$

satisfying the following universal property.

Given any embedding into a field, $\sigma\colon R \hookrightarrow L$, such that $1_R \mapsto 1_L$, there is a unique extension $\widetilde{\sigma}\colon K \to L$ such that the following diagram commutes.

$$\begin{tikzcd} R \arrow[r, hook, "\iota"] \arrow[dr, "\sigma"'] & K \arrow[d, "\widetilde{\sigma}"] \\ & L \end{tikzcd}$$

In order to construct K, we let $S \subseteq R \times R$ be defined by

$$S = \{(a, b) \mid b \neq 0\}.$$

We impose an equivalence relation on S by saying $(a, b) \sim (c, d)$ if and only if $ad - bc = 0$. Clearly, this relation is reflexive and symmetric. To see that it is transitive, we let $(a, b) \sim (c, d)$, and $(c, d) \sim (e, f)$, meaning $ad - bc = 0$ and $cf - de = 0$. Multiplying the first equation by f and the second equation by b, then subtracting, we get $adf - bde = 0$, meaning $d(af - be) = 0$. Since R admits no zero divisors, this means that $af - be = 0$, so the relation is transitive.

We write $[(a, b)] = \frac{a}{b}$ for K, with operations

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

These operations are well-defined and do satisfy the universal property. Verifying this is a pain, but it can be done.

Now, we may extend this to all unital commutative rings, not just integral domains.

Definition: Let R be a unital commutative ring, and let $S \subseteq R$. We say S is *multiplicative* if

- $1 \in S$;
- $0 \notin S$;
- for any $x, y \in S$, $xy \in S$.

Example:

(i) If R is an integral domain, then $R \setminus \{0\}$ is multiplicative.

(ii) If $z \in R$ is such that z is not nilpotent, then $S = \{z^n \mid n \geqslant 0\}$ is multiplicative.

(iii) If P is a prime ideal, then $S = R \setminus P$ is multiplicative.

We will use (iii) to construct a ring with a unique maximal ideal. First, though, we construct a ring of fractions using multiplicative sets.

Definition: Let R be a unital commutative ring, and let $S \subseteq R$ be multiplicative. We construct a ring $S^{-1}R$ by taking an equivalence relation on $R \times S$ as follows:

$$(a, s) \sim (b, t) \Leftrightarrow \exists s' \in S \text{ such that } s'(at - bs) = 0.$$

We write

$$S^{-1}R = \{[(a, s)] \mid a \in R, s \in S\},$$

and denote

$$[(a, s)] = \frac{a}{s}.$$

This becomes a ring under the operations

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$
$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

We call $S^{-1}R$ the *localization of* R *with respect to* S.

We can see some basic properties of the localization.

Proposition: Let R be a unital commutative ring, $S \subseteq R$ multiplicative, and let $S^{-1}R$ be the corresponding localization.

- The additive identity in $S^{-1}R$ is $\frac{0}{1}$.
- The additive inverse of $\frac{a}{s}$ in $S^{-1}R$ is $\frac{-a}{s}$.
- For all $a \in R$ and all $s, s' \in S$, we have $\frac{as'}{ss'} = \frac{a}{s}$.
- Every element of the form $\frac{s}{t}$ where both $s, t \in S$ is invertible, with corresponding inverse $\frac{t}{s}$.
- The map $\iota_S \colon R \to S^{-1}R$ given by $r \mapsto \frac{r}{1}$ is an injective ring homomorphism such that $\iota_S(S) \subseteq (S^{-1}R)^{\times}$, where $(S^{-1}R)^{\times}$ denotes the group of invertible elements in $S^{-1}R$.

Unique Factorization Domains, Principal Ideal Domains, and Euclidean Domains

Definition: A ring R is called *Noetherian* if, for any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$, there is some index N such that for all $m \geqslant N$, $I_m = I_N$.

Proposition: The following are equivalent:

- R is Noetherian;
- every ideal in R is finitely generated.

Proof. Let R be Noetherian. Suppose toward contradiction that there exists I that is not finitely generated. Then, I is nonzero, so there is $\alpha_1 \in I$ such that $I_1 = (\alpha_1)$ is nonzero. Since I is not finitely generated, $I \neq I_1$, so there is $\alpha_2 \in I \setminus I_1$, so that $I_2 = (\alpha_1, \alpha_2)$ is such that $I_1 \subseteq I_2$. Inductively, we generate $I_n = (\alpha_1, \dots, \alpha_n)$ such that $I_{n-1} \subsetneq I_n$, implying that we have a strictly ascending chain of ideals, which is a contradiction.

Suppose every ideal in R is finitely generated. Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals, and set $I = \bigcup I_n$ be their union. By assumption, I is finitely generated, so we have $I = (\alpha_1, \dots, \alpha_N)$ for some $\alpha_1, \dots, \alpha_N \in R$. Yet, since I is the union of all these ideals, there is some M such that $\alpha_1, \dots, \alpha_N \in I_M$, meaning the chain stabilizes. □

Corollary: If R is a principal ideal domain, then R is Noetherian.

Definition: Let R be an integral domain.

(i) Two elements $a, b \in R$ are called *associated* if $a = bu$ for some unit (invertible) element $u \in R$. Equivalently, a and b are associated if $(a) = (b)$

(ii) An element $a \in R$ is called *irreducible* if

- a is not a unit element;
- whenever $a = bc$ for some $b, c \in R$, then one of b or c is a unit.

(iii) An element a is called *prime* if $a \neq 0$, $a \notin R^\times$, and (a) is prime. Equivalently, a is prime if, whenever $a|bc$, it follows that $a|b$ or $a|c$, where divisibility in R is defined traditionally (i.e., there exists $z \in R$ such that $az = b$).

Note: Prime elements are irreducible, but not necessarily vice versa.

The question then arises: when are irreducibles prime?

Definition: We say $a \in R$ with $a \neq 0$, $a \notin R^\times$ has a *unique factorization* into irreducibles if

(i) we may write $a = up_1 \cdots p_r$, where u is a unit and $p_1, \dots, p_r$ are irreducible;

(ii) for any other such factorization

$$\begin{aligned} a &= u\prod_{i=1}^{r} p_i \\ &= v\prod_{j=1}^{s} q_j, \end{aligned}$$

where p_i, q_j are irreducible and u, v are units, we have

- $r = s$;
- upon permutation of factors, p_i and q_i are associated.

We call R a *unique factorization domain* if, for any $a \in R$ with $a \neq 0$, $a \notin R^\times$, a has unique factorization into irreducibles.