NOVEMBER 14 NOTES

1. 7.4: Properties of Ideals

For this section, let R be a ring with identity $1 \neq 0$.

Proposition 1.1. *Let I be an ideal of R. Then:*

(1) $I = R$ if and only if I contains a unit.
(2) Assume R is commutative. Then, R is a field if and only if its only ideals are (0) and R.

One important class of ideal is the notion of 'maximal' ideal.

Definition 1.2. An ideal M in a ring R is **maximal** if $M \neq R$ and the only ideals containing M are M and R.

Example 1.3. If R is a field, the only ideal $M \neq R$ is the ideal $M = (0)$, so this is maximal.

Proposition 1.4. *If R is a ring with identity $1 \neq 0$, then every ideal $I \neq R$ is contained in a maximal ideal.*

Proof. Note: we skipped the proof of this in class because we've never talked about Zorn's Lemma. Please read or ignore as you wish. Let $I \subset R$ be an ideal of R, $I \neq R$. Let S be the set of all proper ideals of R which contain I. Because $I \in S$, $S \neq \emptyset$. Let C be a chain in S, i.e. C is a chain of ideals $J_1 \subset J_2 \subset J_3 \subset \dots$ such that each J_i is a proper ideal that contains I, and let $J = \cup_{i \geq 1} J_i$. Then, J is an ideal: J is non-empty because $0 \in I \subset J_i$, and if $a, b \in J$, there is some J_i and J_k such that $a \in J_i$ and $b \in J_k$, and either $J_i \subset J_k$ or $J_k \subset J_i$, so $a, b \in J_i$ or $a, b \in J_k$. Suppose without loss of generality $a, b \in J_i$. Because J_i is an ideal, $a - b \in J_i$ and $ra \in J_i$ for any $r \in R$, so J is a subring that is also an ideal. Also, J must be proper: if J is not proper, then $1 \in J$, which would mean $1 \in J_i$ for some i, contradicting that J_i is proper. Therefore, every chain C in S has an upper bound, so by Zorn's Lemma, S has a maximal element which is a proper ideal containing I. □

Proposition 1.5. *Assume R is commutative. An ideal M is maximal if and only if R/M is a field.*

Proof. Because the ideals of R/M are precisely the ideals of R containing M, M is maximal if and only if there are no proper ideals containing M if and only if there are no ideals of R/M other that (0) and R/M, which occurs if and only if R/M is a field. □

Example 1.6. The ideal $(n) \in \mathbb{Z}$ is maximal if and only if n is prime. If n is prime, then $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ is a field. If n is not prime, then $n = ab$ for some integers a, b with $a, b \neq 1$, so $(n) \subsetneq (a) \subsetneq \mathbb{Z}$ (so (n) is not maximal).

Example 1.7. The ideal $(x) \in \mathbb{Z}[x]$ is not maximal because $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, which is not a field. (For any ring R, $R[x]/(x) \cong R$ because (x) is the kernel of the surjective homomorphism $ev_0 : R[x] \to R$.)

There are several maximal ideals that do contain (x): for instance, $M = (x, 2)$. The quotient $\mathbb{Z}[x]/(x, 2) \cong \mathbb{Z}_2$ which is a field, so $(x, 2)$ is maximal.

Example 1.8. Let F be a field. The ideal (x) in $F[x]$ is maximal because $F[x]/(x) \cong F$.

Another type of ideal is a prime ideal.

Definition 1.9. Let R be a commutative ring. A **prime ideal** is a proper ideal P of R such that, for $a, b \in P$, $ab \in P$ implies a or $b \in P$.

This is actually just a generalization of prime number! Recall that if p is prime, and p divides ab, then either p divides a or p divides b. This translates into ideals as follows: suppose $ab \in (p) \subset \mathbb{Z}$. Then, this means $ab = pk$ for some p, so $p \mid ab$, so $p \mid a$ or $p \mid b$. If $p \mid a$, then $a \in (p)$, and if $p \mid b$, then $b \in (p)$. So, $ab \in (p)$ implies either $a \in (p)$ or $b \in (p)$. In other words, a nonzero number p is prime if and only if the ideal (p) is prime. As we saw above, these are also the maximal ideals of $\mathbb{Z}$.

Proposition 1.10. *Assume R is commutative. Then, P is a prime ideal in R if and only if R/P is an integral domain.*

Proof. P is prime if and only if for any $ab \in P$, either $a \in P$ or $b \in P$. Because $ab \in P$ if and only if $ab = 0 \in R/P$, this is true if and only if a or b is zero in R/P, i.e. R/P has no zero divisors. □

Example 1.11. If R is an integral domain, then (x) is a prime ideal in $R[x]$ because $R[x]/(x) \cong R$.

Finally, because fields are integral domains, we see that:

Corollary 1.12. Every maximal ideal of a commutative ring R is a prime ideal.

2. 7.5: Rings of Fractions

In this section, we will generalize the construction of the rational numbers from the integers (where we look at all possible fractions of integers). We will prove that any ring R is contained in a larger ring Q such that every nonzero element of R that is not a zero divisor is in fact a unit (i.e. in Q, every element is either zero, a zero divisor, or a unit). In particular, if R is a domain, Q will be a field.

We construct Q as the **field of fractions** (or fraction field, or quotient field) of R: for example, if $R = \mathbb{Z}$, then the field of fractions of $\mathbb{Z}$ will be $\{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$, which is also known as $\mathbb{Q}$.

We construct Q as follows.

Theorem 2.1. *Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain zero divisors, and is closed under multiplication. Then, there is a commutative ring Q with identity such that Q contains R as a subring and every element of D is a unit in Q.*

Furthermore, every element in Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$, then Q is a field.

The ring Q is the unique smallest ring with these properties. Precisely, let S be any commutative ring with identity and let $\phi : R \to S$ be an injective homomorphism such that $\phi(d)$ is a unit for each $d \in D$. Then, there is an injective homomorphism $f : Q \to S$ such that $f|_R = \phi$.

Proof. Let $\mathcal{F} = \{(r, d) \mid r \in R, d \in D\}$. Define the relation $\sim$ on $\mathcal{F}$ by $(r, d) \sim (s, e)$ if and only if $re = sd$. (Think of the elements (r, d) as fractions r/d. Then, this is just saying $r/d = s/e$ if and only if $re = sd$.) This is symmetric and reflexive by definition, and one can check that it is transitive, so it is an equivalence relation.

Let r/d be the equivalence class of (r, d), so $r/d = \{(a, b) \mid a \in R, b \in R, rb = ad\}$ and let Q be the set of equivalence classes.

Then, Q is a commutative ring with identity where:

1. $+$ is given by $a/b + c/d = (ad + bc)/bd$
2. $\times$ is given by $a/b \times c/d = ac/bd$
3. the additive identity is the element $0/d$ (for any $d \in D$) and the additive inverse of a/d is $-a/d$
4. the identity is d/d (for any $d \in D$)
5. we think of $R \subset Q$ by writing $r = rd/d$ (for any $d \in D$)
6. for any $d \in D$, $d = de/e \in Q$ where $e \in D$ is any element, so d has a multiplicative inverse: $d^{-1} = e/de$, so any $d \in D$ is a unit in Q.

Finally, the uniqueness property follows because, if $\phi : R \to S$ is an injective homomorphism where $\phi(d)$ is a unit, then we can define $f : Q \to S$ by $f(r/d) = \phi(r)\phi(d)^{-1}$. For any $r \in R$, $r = rd/d \in Q$, so $f(r) = f(rd/d) = \phi(rd)\phi(d)^{-1} = \phi(r)\phi(d)\phi(d)^{-1} = \phi(r)$, so $f|_R = \phi$. □

Definition 2.2. The ring Q constructed in the previous theorem is called the **ring of fractions of** D and is denoted $D^{-1}R$. If R is an integral domain and $D = R - \{0\}$, then Q is called the **field of fractions of** R.

Example 2.3. Some common examples:

- $R = \mathbb{Z}$, $D = \mathbb{Z} - \{0\}$. Then, $D^{-1}R = \mathbb{Q}$ is the field of *rational numbers*.
- If F is a field, $R = F[x]$, and $D = F[x] - \{0\}$, then $D^{-1}F = F(x) = \{p(x)/q(x) \mid q(x) \neq 0\}$ is the fields of *rational functions*.
- (Harder, but still checkable): if R is the ring of integers $\mathcal{O}$ in the quadratic field $\mathbb{Q}(\sqrt{D})$, then the field of fractions of $\mathcal{O}$ is just $\mathbb{Q}(\sqrt{D})$.

3. 7.6: The Chinese Remainder Theorem

In this section, we will assume that all rings are commutative with identity $1 \neq 0$. Just as we did for groups, we can define the direct products of rings. We will use direct products to state the Chinese Remainder Theorem.

Definition 3.1. Let A and B be ideals of a ring R. A and B are said to be **comaximal** if $A + B = R$.

We state and prove the main theorem of this section.

Theorem 3.2. *Let $A_1, \dots, A_k$ be ideals in a ring R. The map*

$$R \to R/A_1 \times \cdots \times R/A_k$$

given by

$$r \mapsto (r + A_1, \dots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap \cdots \cap A_k$. If, for each i, j with $i \neq j$, the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap \cdots \cap A_k = A_1 \dots A_k$ so this says

$$R/(A_1 \dots A_k) \cong R/A_1 \times \dots R/A_k.$$

Before we prove it, we first do an example. Let $n \in \mathbb{Z}$ be an integer such that $n = ab$ where a and b are relatively prime. Let $R = \mathbb{Z}$ and $A_1 = (a)$ and $A_2 = (b)$. Because a and b are relatively prime, there exist integers i, j such that $1 = ia + jb$, so $R = (1) \in A_1 + A_2$, so $R = A_1 + A_2$. Because $A_1 \cap A_2 = A_1A_2 = (n)$, the theorem says

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(a) \times \mathbb{Z}/(b).$$

Because $\mathbb{Z}/(k) \cong \mathbb{Z}_k$ for any positive integer k, and the cosets in $\mathbb{Z}/(k)$ are just the integers mod k, this says:

$$\mathbb{Z}_n \cong \mathbb{Z}_a \times \mathbb{Z}_b$$

where the isomorphism is given by $x \mapsto (x \pmod a, x \pmod b)$.

This can be generalized to any factorization of an integer into relatively prime factors (for example, its prime factorization). In that case, it says if $n = p_1^{a_1} \dots p_k^{a_k}$ is the prime factorization of n, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$$

where the map is

$$x \mapsto (x \pmod{p_1^{a_1}}, \dots, x \pmod{p_k^{a_k}}).$$

Because this gives an isomorphism of rings, it also says the groups of units on both sides are isomorphic. For instance, in the previous example, it says

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{a_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{a_k}}^\times.$$

Let us finally prove the theorem. (We ran out of time to do this in class, but I have included it here.) We prove this only in the case $k = 2$ (then, induction takes care of the full proof).

Proof. Let A_1 and A_2 be ideals of R. Let $\phi : R \to R/A_1 \times R/A_2$ be the map $\phi(r) = (r + A_1, r + A_2)$. This is a ring homomorphism because projection is a ring homomorphism. The kernel is exactly the elements such that $r + A_1 = A_1$ and $r + A_2 = A_2$, so $r \in A_1$ and $r \in A_2$, i.e. $r \in A_1 \cap A_2$, as desired.

Now, suppose A_1 and A_2 are comaximal. Because $A_1 + A_2 = R$, there exist elements $x \in A_1$ and $y \in A_2$ such that $x + y = 1$, so $\phi(x) = (A_1, 1 + A_2)$ and $\phi(y) = (1 + A_1, A_2)$, so if $(r_1 + A_1, r_2 + A_2)$ is any element of $R/A_1 \times R/A_2$, then $\phi(r_2 x + r_1 y) = (r_1 + A_1, r_2 + A_2)$, so ϕ is surjective.

Finally, by definition of $A_1 A_2$ (because A_1, A_2 are ideals), we have $A_1 A_2 \subset A_1 \cap A_2$. Then, if $c \in A_1 \cap A_2$, $c = c1 = cx + cy = xc + cy \in A_1 A_2$, so $A_1 \cap A_2 \subset A_1 A_2$ and we have shown $A_1 \cap A_2 = A_1 A_2$. □