Ring Theory

Boran Erol

March 2024

1 Definitions and Basic Properties

1.1 Definition and Examples

Algebraists usually assume that rings are unital whereas analysts don't.

Here are some examples of rings:

Example 1.1. The zero ring $R = \{0\}$.

Example 1.2. Given any additive Abelian group G, we can define the product operation as $\forall a, b \in G : a \cdot b = 0$. This gives G a ring structure. This is called the **trivial ring**.

Example 1.3. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are commutative unital rings.

Example 1.4. $\mathbb{Z}/n\mathbb{Z}$ is a ring. One needs to check that the operations are well-defined. This is called the **ring of congruence classes**.

Example 1.5. Let A be an additive Abelian group. End(A) is a ring where addition is defined as pointwise addition and the product operation is composition of functions.

End($\mathbb{Z}$) $\cong Z$ since every group endomorphism of $\mathbb{Z}$ is fully determined by where it takes the identity.

Example 1.6. Let R be a ring. $M_n(R)$ is also a ring and it is unital if and only if R is unital.

There's an easy way and a hard way to prove that $M_n(R)$ is a ring. The easy way is to remember the correspondence between matrices and linear transformations. The hard way is to write out the associativity rule using matrices.

Definition 1. Let R be a ring. $a, b \in R$ are said to be **relatively prime (coprime)** if their only common divisors are units.

1.2 Basic Properties

Lemma 1.7. Let u be a unit in R. If $a \mid u$, a is also a unit in R.

Proof. Easy. □

Corollary 1.7.1. Let R be a commutative ring and u be a unit in R. If $ab = u$, both a and b are units.

1.3 Integral Domains

Lemma 1.8. Every finite integral domain is a field.

Proof. Let R be a finite integral domain. □

We can also prove this using the characteristic of the domain R. See Section 3 what that is.

Proof. □

Lemma 1.9. The subring of an integral domain is an integral domain.

1.4 Exercises

Lemma 1.10. Let R be a ring and $u \in R$. If u has a left and a right inverse, u is a unit and the left and right inverses are the same.

Proof. Let r be the right inverse of u and x be the left inverse. Then,

$$x = x(ur) = (xu)r = r$$

Thus, $x = r$ and they're just the inverse of u. □

Lemma 1.11. Let R be a ring with identity and u be an element with a right inverse. Then, the following are equivalent:

1. u has another right inverse.
2. u is a zero divisor.
3. u is not invertible.

Proof. If u has two right inverses x, y, $u(x - y) = ux - uy = 0$, so u is a zero divisor. If u is a zero divisor, u is not invertible. □

Lemma 1.12. $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

Proof. Assume by contradiction that $f : 2\mathbb{Z} \to 3\mathbb{Z}$ is an isomorphism. Then, $f(2) = 3k$ for some $n, k \in \mathbb{N}$. Then, $f(4) = 9k^2 = 6k$, so $3k = 2$, which is a contradiction. □

Lemma 1.13. Let R be a ring. R is a division ring if and only if the only ideals are the zero ideal and the unit ideal.

2 Ideals

Definition 2. Let R be a ring and $I \subseteq R$.

Definition 3. Let R be a ring and I be an ideal. I is a **principal ideal** if $I = aR$ for some $a \in R$.

Definition 4. Let R be a ring. The **sum of ideals** I and J in R, denoted $I + J$, is the set $\{i + j : i \in I, j \in J\}$.

Definition 5. Let R be a ring. The **product of ideals** I and J in R, denoted IJ, consists of all finite sums $\sum a_i b_i$, where $a_i \in I$ and $b_i \in J$.

This definition warrants an explanation. The natural definition would be $IJ = \{ij : i \in I, j \in J\}$. However, this definition is not closed under addition, as the next examples show. Therefore, to ensure that IJ is an ideal, we use the definition above.

Example 2.1. Let IJ denote the broken product definition. Let F be a field and consider $R = F[x, y]$. Consider $I = (2x)$ and $J = (y)$. $2xy \in I$ and $xy \in J$ so they're both in IJ. But $2xy - xy = xy \notin IJ$.

Example 2.2. Let $R = \mathbb{Z}$. Let $I = 4\mathbb{Z}$ and $J = 2\mathbb{Z}$. $4 \in I$ and $2 \in J$ so they're both in IJ. But $4 - 2 = 2 \notin IJ$.

Notice that $IJ \subseteq I \cap J$ for any two ideals I, J in a ring R.

Lemma 2.3. Let R be a commutative ring. The product of principal ideals is a principal ideal.

Proof. Let aR, bR be principal ideals. Notice that $aR \cdot bR \subseteq abR$ by a simple rearrangement of the terms in the finite sum. The reverse inclusion is also trivial. □

Example 2.4. If R is not commutative, we can use nilpotent elements of order 2 to contradict $aR \cdot bR = abR$. For example, consider the following matrix in $M_2(\mathbb{R})$:

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

Letting $a = b$ be the matrix above, we get a counterexample.

Lemma 2.5. Let $\phi : R \to S$ be a surjective ring homomorphism and I be an ideal of R. Then, $\phi(I)$ is an ideal of S.

Proof. We'll show that $\phi(I)$ is closed under addition and multiplication. $\phi(I)$ is non-empty since $0 \in \phi(I)$.

Additive property here.

Let $y \in \phi(I)$. Then, $\exists x : \phi(x) = y$. Let $s \in S$. Since ϕ is surjective, $\exists r : \phi(r) = s$. Then, $sy = \phi(r)\phi(x) = \phi(rx) \in \phi(I)$. □

To see that surjectivity is necessary, consider the identity mapping from $\mathbb{Z}$ to $\mathbb{Q}$ and the ideal of even numbers in $\mathbb{Z}$. Clearly, this is no longer an ideal in $\mathbb{Q}$.

3 Characteristic of a Ring

Let R be a ring. Recall that there is a unique ring homomorphism from $\mathbb{Z}$ to R. Then, the kernel of this homomorphism is $n\mathbb{Z}$ for some natural number $n \in \mathbb{N}$. n is called the **characteristic of R** and denoted $char(R)$. Intuitively, this is just the number of times you have to add 1 to itself to get 0.

Here are some examples:

Example 3.1. Every Boolean Ring has characteristic 2. See Lemma 9.6.

We can prove that finite integral domains are fields by considering the characteristic.

Lemma 3.2. Let R be a finite integral domain. Then, $char(R)$ is a prime.

Proof. Let $f : \mathbb{Z} \to R$. Since R is a domain, $ker(f)$ is a prime ideal. Thus, $\ker(f) = p\mathbb{Z}$ for some prime p. □

Corollary 3.2.1. Finite integral domains are fields.

Proof. Prime ideals are maximal in $\mathbb{Z}$, so R is a field. □

Lemma 3.3. Let R be a ring of characteristic $p > 0$. Then, $f : R \to R$ defined by $f(x) = x^p$ is a ring endomorphism. These are called **Frobenius endomorphisms**.

Proof. The fact that f respects multiplication is immediate. To prove that f respects addition, use the Binomial Theorem. □

4 Products of Rings

Definition 6. Let R be a ring. An **idempotent** is an element $a \in R$ such that $a^2 = a$.

Example 4.1. $0, 1$ are idempotents in every ring. They are called **trivial idempotents**.

Lemma 4.2. Let $e \in R$ be idempotent. Then, $1 - e$ is also idempotent.

Proof. Assume $e \in R$ is idempotent. Then, $(1-e)(1-e) = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$. □

Lemma 4.3. Any non-trivial idempotent is a zero divisor.

Proof. Let $e \in R$ be a non-trivial idempotent. Then, $e^2 - e = 0 \implies e(e-1) = 0$. Since $e \neq 0$ and $e - 1 \neq 0$ e is a zero divisor. □

Corollary 4.3.1. Domains don't have non-trivial idempotents.

Lemma 4.4. Let e, f be central, orthogonal, idempotent elements with $e+f = 1$. Then, $eR \cap fR = \{0\}$.

Proof. □

Lemma 4.5. Let R, S be a ring. Every (left) ideal of the product $R \times S$ is of the form $I \times J$ where I is an ideal of R and J is an ideal of S.

Proof. □

Lemma 4.6. Let R, S be rings. $(R \times S)^\times = R^\times \times S^\times$

Proof. □

5 Chinese Remainder Theorem

5.1 Comaximal (Coprime) Ideals

Definition 7. Let R be a ring and I, J be ideals. I, J are said to be **comaximal (coprime)** if $I + J = R$.

This is a generalization of the Bezout Identity in $\mathbb{Z}$.

Here are some immediate properties of comaximal ideals:

1. If I, J are comaximal, $1 \in I + J$. (This is why it's a generalization of the Bezout Identity.)
2. Let I, M be ideals and M be maximal. If I, M are comaximal, $I \subseteq M$.

Lemma 5.1 (Comaximality is Stronger than Relatively Prime)**.** Let R be a commutative unital ring. Let $a, b \in R$ be comaximal. Then, a, b are relatively prime.

Proof. Let $a, b \in R$ be comaximal and let $c \in R$ such that $c \mid a$ and $c \mid b$. Since $aR + bR = R$, there's $r_1, r_2 \in R$ such that $ar_1 + br_2 = 1$. Then, c divides the left hand side so $c \mid 1$ so c is a unit. We thus conclude the proof. □

The next example shows that there are relatively prime elements that are not comaximal.

Example 5.2. Let F be a field and $R = F[x, y]$. Notice that xR and yR are not comaximal since $1 \notin xR + yR$, but they are relatively prime.

In Lemma 10.2, we prove that these two conditions are equivalent in PIDs. Notice that R in the previous example was a UFD.

We now prove some lemmas that will be useful when proving the Chinese Remainder Theorem for rings.

Lemma 5.3 (Product of Comaximal Ideals)**.** Let R be a commutative ring and I, J be coprime ideals. Then, $IJ = I \cap J$.

Proof. $IJ \subseteq I \cap J$ for any two ideals, so it suffices to prove the reverse inclusion. Since I, J are comaximal, there's $a \in I$ and $b \in J$ such that $a + b = 1$.

Now, let $x \in I \cap J$. Then, $x = x \cdot 1 = x(a + b) = xa + xb$. Notice that both terms are in IJ, so $x \in IJ$. □

Lemma 5.4. Let R be a commutative ring and I, J ideals. The canonical projection map $\phi : R \to R/I \times R/J$ is surjective if and only if I, J are comaximal.

Proof. Let $a \in I$ and $b \in J$ such that $a + b = 1$ Reducing this equation mod I and J gives us $\phi(a) = (1, 0)$ and $\phi(b) = (0, 1)$. Then, let $(r_1, r_2) \in R/A \times R/B$. Notice that $\phi(r_1 a + r_2 b) = (r_1, r_2)$, so ϕ is surjective. □

Corollary 5.4.1. Let R be a commutative ring and I, J coprime ideals. Then, $R/IJ \cong R/I \times R/J$.

Proof. Use the first isomorphism theorem on ϕ. □

Lemma 5.5. Let R be a nonzero commutative ring. Let $I_1, I_2, ..., I_k$ be ideals in R that are pairwise comaximal. Then, I_1 and $I_2 I_3 ... I_k$ are comaximal.

Proof. Since I_1 and I_j are comaximal for every $j = 2, 3, ..., k$, there's some $x_j \in I_1$ and $y_j \in I_j$ such that $1 = x_j + y_j$. Then,

$$1 = (x_2 + y_2)...(x_k + y_k)$$

Notice that the right hand side is in $I_1 + I_2 ... I_k$ since every term with a factor of x_j is in I_1 and $y_2 y_3 ... y_k \in I_2 ... I_k$. □

5.2 Chinese Remainder Theorem

Theorem 5.6. Let R be a ring and $I_1, I_2, ..., I_n$ be pairwise coprime, two-sided ideals. Then, for every $(a_1, ..., a_n) \in R^n$, $\exists a \in R$ such that $a \equiv a_j \mod I_J$ for every $j = 1, 2, ..., n$.

Proof. We'll induct on $n \geq 2$. Let $I_1 + I_2 = R$. Let $a_1, a_2 \in R$. Then,

$$a_1 - a_2 \in R \implies \exists x_1 \in I_1 : \exists x_2 \in I_2 : x_1 + x_2 = a_1 - a_2$$

Let $a := a_1 - x_1 = a_2 + x_2$. Then, $a - a_j \in I_j$, so the condition is satisfied. Equivalently, Lemma 5.4 is a more elegant way of stating the base case.

Let's now do the inductive step. Assume the statement holds for some $n \in \mathbb{N}$. Let $I_1, I_2, ..., I_{n+1}$ be pairwise coprime, two-sided ideals. Let $a_1, a_2, ..., a_{n+1} \in R$. By the inductive hypothesis, $\exists b \in R : \forall j = 1, 2, ..., n : b \equiv a_j \mod I_j$. In other words, the canonical projection map $\phi : R \to R/I_1 \times ... \times R/I_n$ is surjective. In other words,

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

Since $I_1I_2...I_n$ and I_{n+1} are comaximal, there's a surjective homomorphism $\psi : R \to R/I_1...I_n \times R/I_{n+1}$. By the inductive hypothesis, $R/I_1...I_n \cong R/I_1 \times ... \times R/I_n$, so we conclude the proof.

□

Corollary 5.6.1. Let R be a ring and $I_1, I_2, ..., I_n$ be pairwise coprime, two-sided ideals. Then,

$$R/(I_1 \cap I_2... \cap I_n) \cong (R/I_1) \times ... \times (R/I_n)$$

Proof. Combine the theorem with Lemma 5.3. □

Let $n = p_1^{\alpha_1}...p_m^{\alpha_m}$. We'll now use CRT in conjunction with Lemma 4.6 to better understand $(\mathbb{Z}/n\mathbb{Z})^\times$. Combining these statements, we get

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times ... \times (\mathbb{Z}/p_m^{\alpha_m}\mathbb{Z})^\times$$

Also notice that this is another way to derive Euler's Totient Function for arbitrary numbers by using $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = p^{n-1}(p-1)$.

6 Prime and Maximal Ideals

6.1 Prime Ideals

Definition 8. An *non-zero* ideal $P \subsetneq R$ is a **prime ideal** if

$$\forall a, b \in R : ab \in P \implies a \in P \vee b \in P$$

Here's a basic consequence of the definition:

Lemma 6.1. *Let R be a ring and I be an ideal of R. Then, I is a prime ideal if and only if the set-theoretic complement of I is closed under multiplication and non-empty.*

This characterization, coupled with Zorn's lemma, produces the following result:

Corollary 6.1.1. *Let R be a commutative ring. Then, the set of prime ideals has a minimal element under inclusion. (This could be the zero ideal.)*

Proof. Consider the subsets of R that are closed under multiplication ordered using inclusion. Since R is closed under multiplication, every chain in this poset has an upper bound, namely, R. Applying Zorn's lemma produces the desired result. □

Example 6.2. If R is a domain, the zero ideal is prime.

Lemma 6.3. *Let R be a ring and I be an ideal of R. The set of all prime ideals containing I is in bijection with all prime ideals of R/I.*

Proof. Let P be a prime ideal of R containing I. Then, $(R/I)/(P/I) \cong R/P$. Using the fact that an ideal is prime if and only if the quotient ring is a domain, we conclude the proof. □

6.2 Maximal Ideals

Definition 9. Let M be a *proper* ideal of a ring R. M is said to be a **maximal ideal** if the only ideals containing M are M and R.

Here are some equivalent characterizations:

Lemma 6.4. Let R be a ring and I be an ideal of R. I is maximal if and only if R/I is a field.

Proof. □

Corollary 6.4.1. Every maximal ideal is a prime ideal.

Let R be a ring. Notice that every non-unit element of R lies in a maximal ideal M of R by using Zorn's lemma. This is useful when one studies local rings.

6.2.1 Existence of Maximal Ideals using Zorn's Lemma

Theorem 6.5. A nonzero commutative ring has a maximal ideal.

Proof. □

Notice that the theorem isn't constructive.

Corollary 6.5.1. A nonzero commutative ring has a prime ideal.

The corollary is often more useful than the theorem itself.

6.3 Prime and Maximal Ideals under Ring Homomorphisms

Let's first examine whether primality and maximality is preserved when taking preimages of ring homomorphisms.

Lemma 6.6. Let R, S be rings and $\phi : R \to S$ be a ring homomorphism. Let P be a prime ideal of S. Then, $\phi^{-1}(P)$ is a prime ideal in R.

Proof. Define $T = \phi^{-1}(P)$. Since $1_S \notin P$, $1_R \notin T$ since otherwise $1_S \in P$ using the fact that $\phi(1) = 1$. Thus, T is not the unit ideal.

Now, let $x, y \in R$ such that $xy \in T$. Then, $\phi(xy) \in P \implies \phi(x) \in P$ without loss of generality as P is prime. Then, $x \in T$. We thus conclude the proof. □

However, this fails for maximal ideals, as the next example demonstrates.

Example 6.7. Let p be a prime in $\mathbb{Z}$. $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$. Now, consider the inclusion homomorphism from $\mathbb{Z}$ into $\mathbb{Q}$. $p\mathbb{Z}$ is not even an ideal in $\mathbb{Q}$, so it's not a maximal ideal.

To prove an analogous lemma for maximal ideals, we need to assume that ϕ is surjective. This is because surjectivity ensures that $\phi(I)$ is an ideal when I is an ideal.

Lemma 6.8. Let R, S be rings and $\phi : R \to S$ be a *surjective* ring homomorphism. Let M be a maximal ideal of S. Then, $\phi^{-1}(M)$ is a maximal ideal in R.

Proof. Define $J = \phi^{-1}(M)$. Since $1_S \notin P$, $1_R \notin J$ since otherwise $1_S \in P$ using the fact that $\phi(1_R) = 1_S$. Thus, J is not the unit ideal.

Now, assume there's some ideal I such that $J \subseteq I$. Then, $\phi(I)$ is an ideal of S that contains M. Then, $\phi(I) = M$ or $\phi(I) = S$. If $\phi(I) = S$, I contains the unit of R and therefore $I = R$. If $\phi(I) = M$, $I = \phi^{-1}(M) = J$. Therefore, J is maximal in R. □

Let's now examine whether primality and maximality are preserved when we take images of homomorphisms. Surjectivity of ϕ is needed to ensure that the image is an ideal, so it's definitely needed to ensure that the image is a prime/maximal ideal.

Using the lemma for preimages, we can say the following: if P is a prime/maximal ideal of R such that $\ker(\phi) \subseteq P$ and ϕ is surjective, $\phi(P)$ is a prime/maximal ideal.

In fact, this follows from the correspondence between prime/maximal ideals of R and R/I, where $I = \ker(\phi)$ in this case.

6.4 Exercises

Lemma 6.9. Let R be a commutative, non-zero ring and P be a prime ideal of R. If P contains no zero divisors, R is a domain.

Example 6.10. Let's now examine some ideals in $R = \mathbb{Z}[x, y]$ and decide whether they're prime or maximal.

Let $I = (x, y)$. This ideal is prime since $R/I = \mathbb{Z}$ is a Euclidean domain.

Let $I = (5, x, y)$. This ideal is not prime $R/I = \mathbb{Z}/5\mathbb{Z}$ which is not even an integral domain.

Let $I = (6, x)$.

Lemma 6.11. Let R be a finite commutative ring. Then, every prime ideal is maximal.

Proof. Let R be a finite commutative ring and I be a prime ideal. Then, R/I is a finite domain. Then, by Lemma 1.8, R/I is a field. Then, I is maximal. □

7 Localization of a Ring and Local Rings

Serge Lang's book has a chapter on this, which I liked. I didn't like (and understand) the exposition in Dummit and Foote.

Localization is a formal way to introduce denominators to a given ring or module.

Let S be a multiplicatively closed set.

We'll define an equivalence relation on (R, S) by

$$(r_1, s_1) \sim (r_2, s_2) := \exists s : s(r_1 s_2 - r_2 s_1) = 0$$

Denote the equivalence classes by $S^{-1}R$.

Intuitively, we're introducing a formal inverse for every element of S.If S if the set of non-zero elements from an integral domain, the localization is the field of fractions.

We usually assume that S doesn't contain nilpotent elements, since otherwise $S^{-1}R$ is the zero ring.

Lemma 7.1. There's a bijection between prime ideals of $S^{-1}R$ and the set of prime ideals of R that don't intersect S.

Definition 10. A ring R is called **local** if it has a unique maximal ideal M.

Lemma 7.2. Let R be a local ring. $R^* = R - M$.

Proof. □

8 The Nil and Jacobson Radicals

Radical ideals try to capture the bad elements of a ring.

8.1 Nilradical

Definition 11. $x \in R$ is called **nilpotent** if $\exists m > 0 : x^m = 0$. The set of nilpotent elements of a ring R is called the **nilradical of** R and denoted $\mathrm{Nil}(R)$.

Notice that every nilpotent element is a zero divisor. Therefore, domains have trivial nilradicals.

Also notice that if R is unital $R \neq \mathrm{Nil}(R)$ since $1 \notin \mathrm{Nil}(R)$.

We now prove some basic properties of nilpotents in commutative rings:

Lemma 8.1. Let R be a commutative ring. $\mathrm{Nil}(R)$ is an ideal.

Let's now show that this doesn't hold in non-commutative rings.

Example 8.2. Let $R = M_2(\mathbb{R})$. Consider

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

and

$$B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

A and B are nilpotent but $A + B$ is not nilpotent.

Lemma 8.3. Let x be a nilpotent element in a commutative ring R. Then, $\forall u \in R^\times : u + x \in R^\times$.

Proof. □

Lemma 8.4. Let $\phi : R \to S$ be a ring homomorphism and $x \in \mathrm{Nil}(R)$. Then, $\phi(x) \in \mathrm{Nil}(S)$.

Lemma 8.5. Let R be a commutative unital ring. Then,

$$\forall a \in \mathrm{Nil}(R) : \forall b \in R : 1 - ab \in R^\times$$

Lemma 8.6. Let R be a ring and I be an ideal with $\mathrm{Nil}(R) \subseteq I$. Then, $\mathrm{Nil}(R/I) = \{0\}$.

Lemma 8.7 (Nilradical is contained in prime ideals)**.** Let R be a commutative ring and P be a prime ideal of R. Then, $\mathrm{Nil}(R) \subseteq P$.

Proof. Let x be a nilpotent element. Then, $x^m = 0$ for some $m > 0$. Let m be the smallest such m. Then, $x \cdot x^{m-1} = 0 \in P$ so either $x \in P$ or $x^{m-1} \in P$. If $x \in P$, we're done. Otherwise, notice $x \cdot x^{m-2}$ and repeat. By a simple inductive argument, $x \in P$. □

Theorem 8.8. The nilradical of a commutative ring R is the intersection of all prime ideals in R.

Proof. Let I be the intersection of all prime ideals in R. $\mathrm{Nil}(R) \subseteq I$ is given by Lemma 8.7.

In order to show the converse, it suffices to show that for any non-nilpotent element $r \in R$ there's a prime ideal that doesn't contain r.

Let r be an element of R that is not nilpotent and S be the set of ideals of R that don't contain any element of the form r^n. Since r is not nilpotent, the zero ideal is in S, so S is not-empty.

Thus, S has a maximal element M. It suffices to show that M is a prime ideal. By contradiction, assume there's $x, y \notin M$ such that $xy \in M$.

Consider the ideal $J = \{z : zx \in M\}$. Notice that $y \in J$ and $M \subseteq J$, so M is properly contained in J. By the maximality of M, $\exists n > 0 : R^n \in J$. Then, $r^n x \in M$.

Now, consider $K = \{z : r^n z \in M\}$. Similar to J, $x \in J$ and $M \subseteq K$, so M is properly contained in K. By the maximality of M, $\exists m > 0 : R^m \in K$. Then, $r^{n+m} \in M$, which is a contradiction.

We thus conclude the proof. □

Example 8.9. Let R be the ring of functions from a non-empty set X to a field F. Then, the nilradical of R is the zero ring.

8.2 Jacobson Radical

Definition 12. Let R be a commutative ring. The **Jacobson Radical, denoted** $J(R)$ is the intersection of all maximal ideals in R.

There's a more general definition that works for non-commutative rings as well.

Lemma 8.10. The nilradical is contained in the Jacobson radical.

Proof. The nilradical is contained in every prime ideal by Lemma 8.7, so it's also contained in every maximal ideal. □

9 Boolean Rings

Definition 13. A ring R is called a Boolean ring if every element of R is idempotent. In other words, $\forall r \in R : r^2 = r$.

Lemma 9.1. Every Boolean ring is commutative.

Proof. Notice that $a(ab)b = a^2b^2 = ab = (ab)^2 = abab$. □

Example 9.2. Let X be a non-empty set. Define addition and multiplication on $\mathcal{P}(X)$ to be

$$A + B = (A - B) \cup (B - A) \text{ and } A \times B = A \cap B$$

In other words, addition is symmetric difference and multiplication is intersection.

Addition and multiplication are associative by the associativity of the union and intersection. Multiplication is distributive using the distributivity of the union operation. Therefore, this operations turn $R = \mathcal{P}(X)$ into a ring.

Notice that X is the identity in R. Moreover, R is a Boolean ring, so it is commutative.

Lemma 9.3. Let R be a Boolean integral domain. Then, $R \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. Since every non-trivial idempotent is a zero divisor and every element of R is idempotent, $R \cong \mathbb{Z}/2\mathbb{Z}$. □

Lemma 9.4. In a Boolean ring, every prime ideal is a maximal ideal.

Proof. □

Lemma 9.5. Every finitely generated ideal in a Boolean ring is principal.

Proof. □

Lemma 9.6. Let R be a Boolean ring. Then, $\forall x \in R : 2x = 0$.

Proof. Let $x \in R$. Then, $(1 + x) = (1 + x)^2 = 1 + 2x + x^2 = 1 + 3x$, so $2x = 0$. □

Corollary 9.6.1. A nonzero Boolean ring has characteristic 2.

Example 9.7. Let X be a non-empty set and R be the ring of all functions from X into $\mathbb{Z}/2\mathbb{Z}$. Let $S = \mathcal{P}(X)$ be the Boolean ring of all subsets of X. For every $A \in S$, let $f_A : X \to \mathbb{Z}/2\mathbb{Z}$ be defined as $f_A(x) = 1$ if and only if $x \in A$. Then, the map $A \mapsto f_A$ is a ring homomorphism.

Check the properties of a ring homomorphism.

Example 9.8. The infinite direct product of $\mathbb{Z}/2\mathbb{Z}$ is an infinite Boolean ring.

Lemma 9.9. Let R be a finite unital Boolean ring. Then, $R \cong \mathbb{Z}/2\mathbb{Z} \times ... \times \mathbb{Z}/2\mathbb{Z}$.

10 Principal Ideal Domains

10.1 Principal Ideal Rings

Definition 14. A ring R is said to be a **principal ideal ring** if every ideal in R is principal.

Notice that principal ideal rings are Noetherian.

Lemma 10.1. Let R be a principal ideal ring and I be an ideal of R. Then, R/I is also a principal ideal ring.

Proof. Let J be an ideal of R/I. Consider the canonical surjective homomorphism $\phi : R \to R/I$. $\phi^{-1}(J)$ is an ideal in R, so $\phi^{-1}(J) = xR$ for some $x \in R$. Then, $\phi(xR) = \phi(x)(R/I) = J$, so we conclude the proof. □

10.2 Principal Ideal Domains

Lemma 10.2. Let R be a PID and $a, b \in R$. aR and bR are comaximal if and only if a and b are coprime.

Proof. Recall that the greatest common divisor d is a generator for the smallest ideal containing both aR and bR. Then, $(d) = (a, b)$. Then, $(d) = R$ if and only if d is a unit, so we conclude the proof. □

Example 10.3. Notice that this implies that if $n, m \in \mathbb{Z}$ are relatively prime, $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$.

Lemma 10.4. The quotient of a PID by a prime ideal is a field.

Proof. Prime ideals are maximal in PIDs. Therefore, the quotient of a PID by a prime ideal is a field. □

Lemma 10.5. Let R be a PID and D be a multiplicatively closed subset of R. Then, $D^{-1}R$ is a PID.

Proof. □

Lemma 10.6. Let R be a ring that is not a PID. Then, the set of non-principal ideals has a maximal element.

Proof. Let S be the set of non-principal ideals. Since R is not a PID, S is not-empty. □

Lemma 10.7. Let R be a ring and assume every prime ideal of R is principal. Then, R is a PID.

Proof. By the lemma above, the set S of non-principal ideals of R contains a maximal element.

Let I be an ideal which is maximal in S. Since $I \in S$, I is not prime. Therefore, $\exists a, b \in R : a, b \notin I \wedge ab \in I$. Let $I_a = (I, a)$ and $I_b = (I, b)$. Define $J = \{r \in R : rI_a \subseteq I\}$.

Since I is a proper subset of I_a and I_b, they're both principal ideals. Moreover, $I_b \subseteq J$ since $(a + I)(b + I) = ab + (aI) + (bI) + I$, and these are all in I. Since I is a proper subset of I_b, it's also a proper subset of J, which implies that J is a principal ideal. Since I_aJ is a product of principal ideals, it's also principal.

Moreover, by definition of J, $I_aJ \subseteq I$. Let's now prove the opposite inclusion.

Let α be the generator for I_a. Let $x \in I$. Then, $x \in I_a$, so $x = r\alpha$ for some $r \in R$. By definition, $r \in J$ so $x \in I_aJ$. Thus, $I \subseteq I_aJ$.

Since $I_aJ = I$, I is also a principal ideal, which is a contradiction. □

11 Greatest Common Divisor and Least Common Multiple

Definition 15. d is said to be the **greatest common divisor** of a and b if $d \mid a$ and $d \mid b$ and every common divisor of a and b divides d.

The least common multiple is a generator for the largest principal ideal contained in $aR \cap bR$. Therefore, the least common multiple exists in all principal ideal domains and is the generator for the (trivially principal) ideal $aR \cap bR$. Therefore, the least common multiple is unique modulo multiplication by units.

Lemma 11.1. Let R be a Euclidean domain. Then, $lcm(a,b)gcd(a,b) = ab$.

Proof. □

12 Algebraic Number Theory

Lemma 12.1. Let p be a prime number such that $p \equiv 3 \pmod 4$. Then, p is prime in $\mathbb{Z}[i]$.

Proof. Notice $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(x^2+1)/(p) \simeq \mathbb{Z}[x]/(p)/(x^2+1) \simeq \mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$ .If $\mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$ is a field, (p) is maximal in $\mathbb{Z}[i]$ and therefore (p) is prime in $\mathbb{Z}[i]$. Thus, it suffices to show that $\mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$ is a field. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, $\mathbb{Z}/p\mathbb{Z}[x]$ is a PID. Therefore, it suffices to check that x^2+1 is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$. This holds if and only if x^2 is a quadratic residue modulo p, which is true if and only if $p \equiv 1 \pmod 4$. □

Lemma 12.2. Let p be a prime number such that $p \equiv 1 \pmod 4$. Then, p is not prime in $\mathbb{Z}[i]$.

Proof. Since $p \equiv 1 \pmod 4$, $\exists x \in \mathbb{Z} : x^2 \equiv -1 \pmod p \implies p \mid x^2+1 = (x-i)(x+i)$. Therefore, to prove that p is not prime in $\mathbb{Z}[i]$, it suffices to show that $p \nmid x \pm i$. In order to show this, we'll show that $x \pm i$ is prime. Notice that $N(x \pm i) = p$, so if $ab = x \pm i$, $N(a) = 1$ without loss of generality. Then, $a \in \mathbb{Z}[i]^\times$, so $x \pm i$ is a prime. Therefore, $p \nmid x \pm i$. □

Corollary 12.2.1. Let p be a prime number such that $p \equiv 1 \pmod 4$. Then, $\exists a, b \in \mathbb{Z} : p = a^2 + b^2$.

Proof. Since p is not prime in $\mathbb{Z}[i]$, there's a non-unit $a + bi$ that properly divides p. Then, the norm of $a + bi$ divides p. Since p is prime $N(a + bi) = a^2 + b^2 = p$, so we conclude the proof. □

12.1 Exercises

Find all prime integers p such that the ring $\mathbb{Z}/p\mathbb{Z}[i]$ is a product of two fields.

Recall that $\mathbb{Z}[i]$ is a Euclidean domain.

Let $p \equiv 3 \mod 4$. Then, p is prime in $\mathbb{Z}[i]$ so $p\mathbb{Z}[i]$ is a prime ideal, so it's a maximal ideal and $\mathbb{Z}/p\mathbb{Z}[i]$ is a field. A field can't be written as the product of two rings, so it's not a product of two fields.

Let $p \equiv 1 \mod 4$.

Lemma 12.3. Every quotient ring of $\mathbb{Z}[i]$ is finite.

Proof. □

13 Noetherian Rings

Lemma 13.1. Let R be a commutative ring. Then, the following are equivalent:

1. Every ideal in R is finitely generated.
2. Every increasing sequence of ideals $I_1 \subseteq I_2 ...$ terminates, i.e. $\exists n \in \mathbb{N} : I_n = I_{n+1} = ...$
3. Every non-empty set of ideals has a maximal element (by inclusion).

Proof. □

Definition 16. A ring R is called **Noetherian** if any of the conditions above hold.

Notice that every PID is Noetherian since every ideal is generated by one element, so the first condition is satisfied.

Theorem 13.2 (Hilbert's Basis Theorem)**.** Let R be a (left) Noetherian ring. Then, $R[x]$ is also (left) Noetherian.

Lemma 13.3. A ring R is left-Noetherian if and only if every finitely generated left R-module is a Noetherian module.

Proof. Let R be a Noetherian ring and M be a finitely-generated left R-module. Then, there's a surjective module homomorphism $f : R^n \to M$. Let N be a submodule of M and let $I = f^{-1}(N)$. Then, I is an ideal of the product ring R^n, so I is finitely generated since the product of Noetherian rings is Noetherian. Let $x_1, ..., x_m$ be a generating set for I. Then, $f(x_1), ..., f(x_m)$ is a generating set for N.

We can use a similar argument to prove the converse. □

14 Factorization in Integral Domains

Definition 17. An element $x \in R$ is said to be **irreducible** if x is not invertible and can't be written as the product of two non-invertible elements in R.

Definition 18. An element $x \in R$ is said to be **prime** if x is non-zero, non-unit and for any $a, b \in R$, $x \mid ab \implies x \mid a \wedge x \mid b$.

Proposition 14.1. Let R be a domain.

1. Suppose R admits factorization. If the factorization is unique, every irreducible element is prime.
2. If every irreducible element in R is prime, then factorization is unique.

Proof. □

Corollary 14.1.1. Let R be a Noetherian domain. Then, R is a UFD if and only if every irreducible element in R is prime.

Proof. □

14.1 Exercises

Lemma 14.2. Consider $R = \mathbb{Z}[\sqrt(-n)]$ where n is a square-free integer greater than 3. Then, R is not a UFD.

Proof. Notice that 2 is prime in R since $N(2) = 4$. □

Lemma 14.3. $F[x,y]/(y - x^2)$ is not isomorphic to $F[x,y]/y^2 - x^2$ for any field F.

Proof. Notice that $y - x^2$ is a linear polynomial in $F[x][y]$ and therefore irreducible. However, $y^2 - x^2 = (y - x)(y + x)$ and therefore is reducible. Thus, one ring has zero divisors while the other one doesn't. □

Let's now actually figure out what $F[x,y]/(y - x^2)$ is.

Lemma 14.4. $F[x,y]/(y - x^2) \cong F[t]$ for any field F.

Proof. □

15 Polynomial Rings

Lemma 15.1. Let R be a ring. If I is a prime ideal in R, (I) is a prime ideal in $R[x]$.

Proof. □

This is not true for maximal ideals. However, the ideal generated by I and x is maximal in the polynomial ring, since it just gives back R/I.

15.1 Exercises

Lemma 15.2. (x) and (x, y) are prime in $\mathbb{Q}[x, y]$ but only (x, y) is maximal.

Proof. $\mathbb{Q}[x, y]/(x) \cong (\mathbb{Q}[x]/(x))[y] \cong Q[y]$.

$\mathbb{Q}[x, y]/(x, y) \cong \mathbb{Q}$ □

Lemma 15.3. (x, y) is not a principal ideal in $\mathbb{Q}[x, y]$.

Proof. x and y are relatively prime, so any element that divides has to be a unit. However, (x, y) is not a unit ideal. □

Notice that this lemma can be extended to the following lemma:

Lemma 15.4. Let R be a commutative unital ring. Then, a polynomial ring in more than one variable over R is not a PID.

The statements above can also be proven by using module theory. In particular, we can show that these modules are not free modules.

Lemma 15.5. Let $f(x) \in R[x]$ be a zero divisor. Then, $\exists b \in R : bf(x) = 0$.

Proof. □

Lemma 15.6. Let R be a commutative ring. Prove that $f \in R[x]$ is nilpotent if and only if all coefficients of f are nilpotent in R.

Proof. Let $f \in R[x]$ be nilpotent. We'll induct on the degree of f. If f is a constant polynomial, the statement is trivial. Thus, assume the statement holds for polynomials of degree n. Let f be a degree $n + 1$ polynomial. Then,

□

16 Factorization over Polynomial Rings

Let R be a UFD.

Definition 19. Let $0 \neq f \in R[x]$ and $f = a_0 + ... + a_n x^n$. The **content of** f, denoted $C(f)$ is defined to be the ideal generated by the greatest common divisor of the coefficients of f.

The greatest common divisor is defined up to a multiplication by a unit. However, $C(f)$ is unique since it is defined on the level of ideals.

Definition 20. f is said to be **monic** if $a_n = 1$.

Definition 21. f is said to be **primitive** if $C(f) = R$.

16.1 Examples

1. All monic polynomials are primitive.
2. Let $0 \neq f \in R[x]$ and $a \in R$. Then, $aC(f) = C(af)$.
3. Let $0 \neq f \in R[x]$ such that $C(f) = aR$. Then, there's a $g \in R[x]$ such that $f = ag$. Then, $C(g) = R$, so g is primitive. **In other words, we can divide every polynomial by its content to get a primitive polynomial.** (We're dividing by the greatest common divisor to ensure that the coefficients are relatively prime.)

Lemma 16.1. Let R be a UFD and $f, g \in R[x]$ be primitive polynomials. Then, fg is also primitive.

Proof. Let $p \in R$ be a prime element. It suffices to show that p doesn't divide all coefficients of fg since every element in a UFD is a product of primes. Consider the canonical surjective ring homomorphism from R to R/pR. This induces a homomorphism from $R[x]$ to $R/pR[x]$. Notice that $\hat{f}, \hat{g}$ are non-zero since f and g are primitive. Since $R/pR[x]$ is a domain, $\hat{f}\hat{g} = \hat{f}g$ is also non-zero. We thus conclude the proof. □

Notice that we avoided analyzing the coefficients of fg.*How did we do this?*

Corollary 16.1.1. Let $0 \neq f, g \in R[x]$. Then, $C(fg) = C(f)C(g)$.

Proof. Let $C(f) = aR$ and $C(g) = bR$. Then, $a = af'$ and $g = bg'$, where f' and g' are primitive. Then, $f'g'$ is primitive by the lemma above. Then, $C(fg) = aC(f')bC(g') = abR = (aR)(bR) = C(f)C(g)$. □

Lemma 16.2 (Division in polynomial ring over fields is stronger)**.** Let $f, g \in R[x]$ and assume g is primitive. $g \mid f$ in $F[x]$ implies $g \mid f$ in $R[x]$.

Proof. Assume $f = gh$ for some $h \in F[x]$. Pick $a \in R$ such that $ah \in R[x]$. Intuitively, we're just clearing the denominators of the coefficients of h. Then, $af = g \times (ah) \implies C(af) = C(gah)$. Then, $aC(f) = C(ah)$. Then, all coefficients of ah are divisible by a, so $ah/a \in R[x]$. But $ah/a = h$, so we're done. □

The next proposition shows that irreducibility in $R[x]$ is stronger than irreducibility in $\mathbb{Q}[x]$, though the two notions are quite close.

Proposition 16.3. Let $f \in R[x]$ be a non-constant polynomial. Then, the following are equivalent:

- f is irreducible in $R[x]$
- f is irreducible in $\mathbb{Q}[x]$ and f is primitive

Proof. □

Let F, K fields and assume F is a subfield of K. irreducibility in F is irrelevant to irreducibility in K. Notice that $x^2 - 2$ is irreducible in $\mathbb{Q}$ but reducible in $\mathbb{R}$.

Proposition 16.4. Let R be a UFD. Then, $R[x]$ is a UFD.

Let R be a UFD. We've classified the irreducible elements in $R[x]$:

1. Irreducible constants $0 \neq a \in R$.
2. Non-constant polynomials $f \in R[x]$ such that f is irreducible in $F[x]$ and f is primitive

Now, let's show that the assumption that R is a UFD is necessary. Consider $R = \mathbb{Z}[2i]$. $f(x) = x^2 + 1$ is irreducible over $R[x]$ since f doesn't have any factors in R. However, it's clearly reducible in $F[x]$ since $F = \mathbb{Q}[i]$.

Restricting to $\mathbb{Z}$ and $\mathbb{Q}$, we get the following lemma:

Lemma 16.5. Let $f \in \mathbb{Q}[x]$. $f \in \mathbb{Z}[x]$ if and only if $Cont(f) \in \mathbb{Z}$.

Proof. The forward implication is trivial. Let's prove the converse. Let $f = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{Q}[x]$ and $m = min\{n : nf \in \mathbb{Z}[x]\}$. Then, $Cont(f) = \frac{1}{m} \gcd(ma_1, ..., ma_n)$. If $Cont(f) \in \mathbb{Z}$, the greatest common divisor is a multiple of m. Then, $\frac{ma_i}{m}$ is an integer for every i, so $f \in \mathbb{Z}[x]$. □

16.2 Exercises

Lemma 16.6. Let R be a UFD with quotient field F and let $p(x)$ be a monic polynomial in $R[x]$. Assume $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are monic polynomials in $F[x]$ with smaller degree than $p(x)$. If $a(x) \notin R[x]$, R is not a UFD.

Proof. □

Lemma 16.7. If $f, g \in \mathbb{Q}[x]$ such that $fg \in \mathbb{Z}[x]$, the product of any coefficient of g and f is an integer.

Proof. Let $f, g \in \mathbb{Q}[x]$ such that $fg \in \mathbb{Z}[x]$. Then, $C(fg) \in \mathbb{Z}$. Let $C(f) = r$ and $C(g) = s$, where r and s are rational numbers and $rs \in Z$. Notice that every coefficient a_i of f is rn for some integer $n \in \mathbb{Z}$ and every coefficient b_j of g is sk for some $k \in \mathbb{Z}$. Thus, $rnsk = (rs)nk \in \mathbb{Z}$. □

Example 16.8. The following example shows us that the subring of a UFD is not necessarily a UFD.

Let F be a field. Let R be the set of polynomials in $F[X]$ whose X-coefficient is 0. This set is clearly closed under addition and multiplication. $f = 1$ is also in R, so R is a subring of $F[X]$. Moreover, notice that X^2 and X^3 are irreducibles in R since $X \notin R$. Moreover, $X^6 = (X^2)^3 = (X^3)^2$ so X^6 has two different factorizations. Thus, R is a subring of $F[X]$ that is not a UFD.

Example 16.9. Here's an example of a ring that's not a UFD and where every irreducible is prime.

Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subseteq \mathbb{Q}[x]$. R is an integral domain with units 1 and -1.

Let f be a non-constant irreducible polynomial in R. Notice that this immediately implies that the constant term of f is ± 1 since otherwise we can write $f = a_0 f'$ and both elements would be non-units. Then, f is primitive. Then, without loss of generality, we can force the constant term of the divisors of f to be ± 1 by multiplying by units, so f is irreducible in R if and only if f is irreducible in $\mathbb{Q}[x]$. Therefore, the irreducibles in R are $\pm p \in \mathbb{Z}$ such that p is prime and irreducibles in $\mathbb{Q}[x]$ with constant term ± 1.

Notice that x is not irreducible since x is not invertible and $x = \frac{x}{2} \cdot 2$ and both $\frac{x}{2}$ and 2 are not invertible in R. This example also shows that x is not prime. By the same argument, qx is reducible for any $q \in \mathbb{Q}$. Since one factor in the factorization of x is going to have the form qx, x can't be written as a product of irreducible elements in R. Thus, R is not a UFD.

Notice that $R/(x)$ has polynomials where the coefficients of x are rational numbers less than 1 and the constant term is an integer. Clearly, this is not a domain.

Lemma 16.10. Let R be a commutative ring such that $R[x]$ is a PID. Then, R is a field.

Proof. □

This immediately implies that $\mathbb{Z}[x]$ is not a PID.

17 Factorization over Polynomial Rings Over Fields

Lemma 17.1. If F is a field, $F[x]$ is a Euclidean domain with $N(f) = deg(f)$.

Lemma 17.2. Let $x = y + a$ for some $a \in \mathbb{Z}$. $f \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if f is irreducible in $\mathbb{Z}[y]$.

Proof. □

17.1 Exercises

Lemma 17.3. $x^{n-1} + x^{n-2} + ... + x + 1$ is irreducible over $\mathbb{Z}$ if and only if n is prime.

Proof. Let's first prove the forward direction using the contrapositive, which is somewhat trivial but hard to write. Suppose n is composite. Then, $n = ab$ for some $a, b \in \mathbb{Z}$. Then, $x^{n-1} + x^{n-2} + ... + x + 1 =$

Let's now prove the reverse direction. Let p be a prime number. We'll use a change of variables to rewrite f and apply Eisenstein's Criterion. □

Lemma 17.4. The polynomial $(x-1)(x-2)...(x-n) - 1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$.

Proof. Let $n \in \mathbb{N}$ and $f(x) = (x-1)(x-2)...(x-n) - 1$. Assume by contradiction that there's non-constant polynomials g, h such that $f(x) = g(x)h(x)$ and $deg(g) = m < n$. Then, notice that for all $y \in \{1, 2, ..., n\} : g(y) = 1$ or $g(y) = -1$.

Assume $g(y) = 1$ for more than m points. Then, $g = 1$, which is a contradiction. Thus, $g(y) = 1$ at at most m points. Then, $h(y) = 1$ at at least $n - m$ points, □

Lemma 17.5. The polynomial $(x-1)(x-2)...(x-n) + 1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$ such that $n \neq 4$.

Proof. □

18 R-Algebras

Definition 22. Let R be a commutative unital ring. An **R-algebra** is a unital ring A and a ring homomorphism $f : R \to A$ such that $f(R) \subseteq Z(A)$.

If A is an R-algebra, A can be given a natural R-module structure by setting $r \cdot a := sr =$

Example 18.1. Every unital ring is a $\mathbb{Z}$-algebra since $\mathbb{Z}$ is the initial object for the category of rings.

Definition 23. Let A, B be R-algebras. An **R-algebra homomorphism** is a ring homomorphism $f : A \to B$ such that

$$\forall r \in R :$$

19 Rings of Formal Power Series

Rings of formal power series are denoted $R[[x]]$. Here's a lemma:

Lemma 19.1. $f \in R[[x]]$ is a unit if and only if a_0 is a unit.

Proof. □