MATH 1530: Abstract Algebra

Spring 2017

Notes for Abstract Algebra: Part II

Nicholas Tomlin

Contents

1 Applications of group theory

In the past, mathematicians studied extrinsic properties of groups rather than intrinsic properties. As we'll see in the following theorem, every finite group can be "embedded" as an isomorphism to some subgroup of the symmetric group S_n. Today, we focus less on the properties of S_n and more on the properties of groups at a general level.

Theorem 1.0.1: Cayley's Theorem
Every finite group G is isomorphic to a subgroup of S_n for some $n \in \mathbb{Z}$. In fact, we may take $n = |G|$.

Proof. Consider the action of left multiplication of the group G on the set G. I.e., $g \cdot x = gx$, which is a product in G. Thus we have the permutation representation $\varphi : G \to S_G \cong S_n$. As an exercise: check that φ is injective. □

Definition 1.0.2: *A **representation** of a group G is a homomorphism $\varphi : G \to \mathrm{GL}(V)$, which is an invertible linear transformation of a vector space V.*

2 Introduction to rings

We're all familiar with some examples of rings. For example, the real numbers, the complex numbers, etc. all have addition and multiplication which are compatible via the distributive law. Now, we'll formally define it:

Definition 2.0.1: *A **ring** is a set R together with binary operations $+$ and $\times$ such that the following ring axioms hold:*
(1) $(R, +)$ is an abelian group.
(2) $\times$ is associative.
(3) $\times$ distributes over $+$, i.e., for all $a, b, c \in R$, then we write $(a+b)\times c = a\times c+b\times c$ and also $c \times (a + b) = c \times a + c \times b$.
(4) We say R has a (multiplicative) identity if there exists $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$.
*Further, we say R is **commutative** if $\times$ is commutative.*

Theorem 2.0.2
Let R be a ring. Then $a \times 0 = 0 \times a = 0$ for all $a \in R$.

Proof. We can write the following derivation:

$$\begin{aligned} a \times 0 &= a \times (0+0) \\ &= a \times 0 + a \times 0 \\ 0 &= a \times 0 \end{aligned}$$

where the last step follows from subtracting $a \times 0$ from both sides of the equation. □

Theorem 2.0.3
Let R be a ring. Then $(-a) \times b = a \times (-b) = -ab$ for all $a, b \in R$.

Theorem 2.0.4
Let R be a ring. The multiplicative identity $1 \in R$ is unique if it exists. Further, $(-1) \times a = -a$.

Proof. If $1 \in R$ and $1' \in R$ are multiplicative identities, then $1 = 1 \times 1' = 1'$ as desired. Then, note that $0 = 0 \times a = (1 + (-1)) \times a = 1 \times a + (-1) \times a = a + (-1) \times a$, so therefore $(-1) \times a = -a$ is the additive inverse. □

2.1 Examples of rings

Many of the groups we have discussed previously can also be considered rings with the usual definition of addition and multiplication: $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, and $\mathbb{Z}/n\mathbb{Z}$ are all examples of this. The group $2\mathbb{Z}$ may also be considered a ring; however, it's notable that $2\mathbb{Z}$ has no multiplicative inverse. (This does not violate the ring axioms.)

Definition 2.1.1: *Given a ring R, a **subring** is a subset $S \subseteq R$ such that $+$ and $\times$ are closed with respect to S and $(S, +, \times)$ is also a ring.*

Example 1: Given a ring R, let $\text{Mat}_{n \times n}(R)$ be the ring of $n \times n$ matrices with entries in R. This is a good example of a (typically) noncommutative ring.

2.1.1 Polynomial rings

Definition 2.1.2: *Given any ring R, define $R[x]$ to be the **polynomial ring** with coefficients in R. Formally:*

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 : a_i \in R, n \geq 0\}$$

*where we call a_n the **leading coefficient** and n is the **degree**.*

Addition on the polynomial ring is defined component-wise as follows:

$$(a_0 + a_1x + \cdots) + (b_0 + b_1x + \cdots) = (a_0 + b_0) + (a_1 + b_1)x + \cdots$$

Meanwhile, multiplication is defined via distribution. So each term of one polynomial is multiplied by each term of the other, and then all terms are summed:

$$(a_0 + a_1x + \cdots) \times (b_0 + b_1x + \cdots) = (a_0b_0) + (a_0b_1 + a_1b_0)x + \cdots$$

We can extend this to multivariable polynomial rings via induction. Indeed, we'll write $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$ to define polynomial rings with an arbitrary number of variables.

2.1.2 Trivial rings

Given any abelian group $(R, +)$, define $\times$ on R by $a \times b = 0$ for all $a, b \in R$. If $(R, +) = \{0\}$, then we have the zero ring. This is the unique ring with an identity $1 = 0$. This is also the only ring which is a group under multiplication. (Some other rings can be made into multiplicative groups by deleting the additive identity, e.g., $\mathbb{R}$.)

2.1.3 Group rings

Definition 2.1.3: *Let G be a group[a] and R be a ring. The* ***group ring***

$$RG = \{r_1g_1 + \cdots r_kg_k : r_i \in R, g_i \in G\}$$

uses the definition of a "formal sum," which will be explained briefly.

[a] Dummit and Foote requires that $|G|$ be finite, but this is not strictly necessary.

As before, addition behaves component-wise:

$$(r_1g_1 + \cdots + r_kg_k) + (r'_1g_1 + \cdots + r'_kg_k) = (r_1 + r'_1)g_1 + \cdots + (r_k + r'_k)g_k$$

Multiplication may be defined by setting $(rg) \cdot (r'g') = (rr')(gg')$ and extending this definition via addition.

Definition 2.1.4: *A* ***formal sum*** *of elements of G with coefficients in R is a map of sets $f : G \to R$ such that $f(g) = 0$ for all but finitely many $g \in G$.*

Example 2: The formal sum of elements in $\mathbb{N} = \{0, 1, 2, \ldots\}$ with $\mathbb{R}$ coefficients are naturally in bijection with $\mathbb{R}[x]$, which is the set of polynomials with real-valued coefficients.

Given a ring R, we might also consider the Laurent polynomial ring $R[x^{\pm}] = \{a_mx^m + \cdots + a_nx^n : m \leq n\}$ where $m, n \in \mathbb{Z}$. For example, the element $x^{-2} + 3x^{-1} + 5x^7 \in \mathbb{R}[x^{\pm}]$ is a member of the Laurent polynomial ring with real coefficients. Then $\mathbb{R}[x^{\pm}] \cong \mathbb{R}\mathbb{Z}$, which is the group ring. For example, $(x^{-2}) \cdot (x^3 + x^5) = x + x^3$.

2.2 The structure of rings

But what does it mean to say that $\mathbb{R}[x^{\pm}]$ is isomorphic to $\mathbb{RZ}$? Even though we have defined isomorphism between groups, we need to re-define the concept of isomorphism for rings. We can do so with the following definition:

Definition 2.2.1: *An* ***isomorphism*** $\varphi : R \to S$ ***of rings*** *is a bijection* φ *such that:*

$$\varphi(r + r') = \varphi(r) + \varphi(r')$$
$$\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$$

for all elements $r, r' \in R$*. If* φ *is not a bijection, we call this a* ***homomorphism****.*

Definition 2.2.2: *A nonzero element* $a \in R$ *is a* ***zero divisor*** *if* $ab = 0$ *or* $ba = 0$ *for some* $b \neq 0$*.*

Definition 2.2.3: *An element* $a \in R$ *is a* ***unit*** *if there exists* $c \in R$ *with* $ac = ca = 1$ *(in a ring where the multiplicative identity exists).*

Example 3: Consider the following groups:

- $\mathbb{Z}$ has no zero divisors and units $\{\pm 1\}$.
- $\mathbb{Z}/n\mathbb{Z}$ has units $\{\bar{m} : (m, n) = 1\}$ and the zero divisors are non-zero non-units.

Observe that an element $a \in R$ cannot be both a unit and a zero divisor. If a is a unit and $ab = 0$, then we can show that $b = 0$. Indeed, let $c \in R$ with $ca = 1$. Then $b = (ca)b = c(ab) = 0$ as desired. Hence a is not also a zero divisor.

2.3 Other structures

Definition 2.3.1: *A commutative ring with identity* $1 \neq 0$ *and no zero divisors is called an* ***integral domain****.*

Definition 2.3.2: *A* ***field*** *is a commutative ring with identity* $1 \neq 0$ *such that every nonzero element is a unit.*

Examples of fields include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

2.4 Examples of ring homomorphisms

Recall that a homomorphism $\varphi : R \to S$ is a map of sets preserving the structure of addition and multiplication. For example, consider reduction modulo n: to do so, let $n \leq 1$ and:

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ a &\mapsto \bar{a} \end{aligned}$$

Previously, we checked that $\overline{a+b} = \bar{a} + \bar{b}$ for addition and $\overline{ab} = \bar{a} \cdot \bar{b}$ for all $a, b \in \mathbb{Z}$. This is sufficient to show that φ is a homomorphism.

We might also consider the evaluation homomorphism on polynomial rings:

$$\begin{aligned} \text{ev}_3 : \mathbb{R}[x] &\to \mathbb{R} \\ p &\mapsto p(3) \end{aligned}$$

As an exercise, check that his is a homomorphism. For example, check that $(p+q)(3) = p(3) + q(3)$ and similarly for multiplication. A related example expresses $\mathbb{R}$ as a subring of $\mathbb{R}[x]$ via the inclusion map defined below:

$$\begin{aligned} i : \mathbb{R} &\to \mathbb{R}[x] \\ a &\mapsto a \end{aligned}$$

Next, we can consider an example of a homomorphism to the product group. However, let us first re-define the concept of products for rings, even though it is essentially the same as direct products on groups.

Definition 2.4.1: *Given A, B rings, we can define the* ***product*** *$A \times B$ as the ring*

$$\{(a, b) : a \in A, b \in B\}$$

with addition and multiplication defined coordinate-wise.

Given this definition, we can define the following homomorphism into a product group:

$$\begin{aligned} \varphi : A &\to A \times B \\ a &\mapsto (a, 0) \end{aligned}$$

This is a homomorphism. Note that if $1_A \in A$ and $1_B \in B$ are identities, then $(1_A, 1_B)$ is an identity in $A \times B$. Then assuming $1_B \neq 0 \in B$, we have $\varphi(1_A)$ as the identity in $A \times B$.

We can define the kernel of a ring based on the underlying group homomorphism, so $\ker \varphi := \{a \in R : \varphi(a) = 0\}$, i.e., elements sent to the additive identity.

Theorem 2.4.2
Given $\varphi : R \to S$, then $\operatorname{im} \varphi \subseteq S$ and $\ker \varphi \subseteq R$ are subrings.

Proof. Check that $\operatorname{im} \varphi$ and $\ker \varphi$ are closed under multiplication in S, R respectively. □

Theorem 2.4.3
Let $\varphi : R \to S$ be a homomorphism of rings. Then $K = \ker \varphi$ satsifies:
(1) K is an additive subgroup of R.
(2) Given $x \in K$ and $a \in R$, then $ax, xa \in K$.

Proof. Indeed, $\varphi(x) = 0$ so $\varphi(ax) = \varphi(a)\varphi(x) = 0$. Similarly for xa. □

2.5 Ideals and quotients

Definition 2.5.1: *An **ideal** of a ring R is a subset $I \subseteq R$ satisfying:*
(1) I is an additive subgroup.
(2L) I is closed under left multiplication by R. That is, if $x \in I$ and $a \in R$, then $ax \in I$.
(2R) I is closed under right multiplication by R. That is, if $x \in I$ and $a \in R$, then $xa \in I$.
*If (1) and (2L) hold, then I is a **left ideal**. Otherwise, I is a **right ideal**.*

Remark that $\ker \varphi \subseteq R$ is an ideal for any $\varphi : R \to S$ ring homomorphism.

Example 4: Let $I \subseteq \mathbb{R}[x]$ be $\{(x-3)f(x) : f(x) \in \mathbb{R}[x]\}$. Note that $I = \ker(ev_3 : \mathbb{R}[x] \to \mathbb{R})$, so based on the previous remark, I is an ideal.

Are left and right ideals always the same? No, we can consider the ring $R = \mathrm{Mat}_{n\times n}(K)$ for any field K, e.g., $\mathbb{R}$. Then, let us define:

$$I = \left\{ \begin{bmatrix} 0 & * & * \\ 0 & * & * \end{bmatrix} \right\}$$

Then I is a left ideal, but not a right ideal. This is because right-multiplication will not necessarily preserve the left-column of zeros in I.

Definition 2.5.2: *Let $I \subseteq R$ be an ideal in a ring R. The **quotient ring** R/I has elements $\{a + I : a \in R\}$ with the following operations:*
- $(a + I) + (b + I) := (a + b) + I$
- $(a + I) \cdot (b + I) := (a \cdot b) + I$

To check that the quotient ring is in fact a ring, we need to check the well-definedness of multiplication as stated above. In particular, given $a + I = a' + I$ and $b + I = b' + I$, then we need to check that $ab + I = a'b' + I$. This is equivalent to checking that $ab - a'b' \in I$:

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' \\ &= (a - a')b + a'(b - b') \end{aligned}$$

but since $(a - a'), (b - b') \in I$, their linear combination must be as well. Therefore multiplication is well-defined as desired.

2.6 A glorious return to the beloved isomorphism theorems

Theorem 2.6.1: First Isomorphism Theorem for Rings
Given a ring homomorphism $\varphi : R \to S$, then $R/\ker\varphi \cong \operatorname{im}\varphi$.

Proof. Let's define a function f as follows:

$$\begin{aligned} f : R/\ker\varphi &\to \operatorname{im}\varphi \\ a + \ker\varphi &\mapsto \varphi(a) \end{aligned}$$

Claim that f is well-defined. Indeed, if $a+\ker\varphi = a'+\ker\varphi$, then $(a-a') \in \ker\varphi$ so we can write $\varphi(a-a') = \varphi(a) - \varphi(a') = 0$. Note that f is surjective by construction, and injective since $\varphi(a) + \varphi(a') \implies a + \ker\varphi = a' + \ker\varphi$.
Finally, f is a ring homomorphism by the definition of addition and multiplication. E.g.:

$$\begin{aligned} f((a+\ker\varphi)(b+\ker\varphi)) &= f(ab + \ker\varphi) \\ &= \varphi(ab) \\ &= \varphi(a)\varphi(b) \\ &= f(a+\ker\varphi)\cdot f(b+\ker\varphi) \end{aligned}$$

We can check addition similarly, which is sufficient to prove the theorem. □

Definition 2.6.2: *If $I \subseteq R$ is an ideal, define the **natural projection** as follows:*

$$\begin{aligned} \pi : R &\to R/I \\ a &\mapsto a + I \end{aligned}$$

for all $a \in R$. Note that this is a surjective homomorphism (check as exercise).

Remark that the kernel of the natural projection map is $\ker(\pi) = \{a \in R : a + I = I\} = I$. So we've realized I, which is an ideal, as the kernel of the natural projection map.

Theorem 2.6.3: Second Isomorphism Theorem for Rings
Let R be a ring. Given a subring $A \subseteq R$ and an ideal $B \subseteq R$, then:

$$A + B = \{a + b : a \in A, b \in B\}$$

is a subring of R and $A \cap B$ is an ideal of A. Then $(A+B)/B \cong A/(A \cap B)$.

Theorem 2.6.4: Third Isomorphism Theorem for Rings
Let $I, J \subseteq R$ be ideals of a ring R, and say $I \subseteq J$. Then: (J/I) is an ideal in R/I, which allows us to write

$$(R/I)/(J/I) \cong (R/J)$$

Theorem 2.6.5: Fourth Isomorphism Theorem for Rings
Let $I \subseteq R$ be an ideal of a ring R. Then there is a bijective, inclusion-preserving correspondence between $\{$subrings A of R containing $I\}$ and $\{$subrings A/I of $R/I\}$. Further, A is an ideal of R iff A/I is an ideal of R/I.

2.7 Properties of ideals

2.7.1 Some ways to construct left, right, and two-sided ideals

Let $A \subseteq R$ where R is a ring containing a multiplicative identity. Then, we can construct the following ideals:

(1) The "smallest" ideal containing A. That is, define $I = \cap J$ where $J \subseteq R$ is an ideal containing A. Note that $0 \in I$ and I is actually an ideal.

Definition 2.7.1: *Given a subset $A \subseteq R$, the ideal I thus defined is called the **ideal generated by** A. We write $I = (A)$.*

(2) We may also construct the smallest left ideal containing A. Define $RA = \{r_1a_1 + \cdots + r_na_n : r_i \in R, a_i \in A\}$ to be the inner product whose elements are linear combinations of elements in A and R. Then RA is a left ideal of the ring R. Indeed, you can check that the following equality is satisfied:

$$RA = \cap L$$

where $L \subseteq R$ is a left ideal containing A. As an exercise: come up with an alternate description for (A) similar to what we did with left ideals.

2.7.2 Principal ideals

Definition 2.7.2: *A **principal ideal** $I \subseteq R$ is an ideal $I = (A)$ where A has only a single element. If $A = \{x\}$ where $x \in R$, then we write $I = (x)$ instead of $I = (\{x\})$.*

Definition 2.7.3: *A **finitely generated ideal** is an ideal generated by a finite subset.*

Theorem 2.7.4
Assume that R is a commutative ring. Given $A \subseteq R$, we have that $RA = (A)$.

Proof. We need to show that $RA = \cap J$ as above. Note that $\cap J \subseteq RA$ because RA is an ideal containing A via commutativity. To show $RA \subseteq \cap J$, take any linear combination in RA. Since any ideal J containing A must be closed under addition and multiplication by ring elements, then $RA \subseteq \cap J$. □

Corollary 2.7.5
If R is commutative and $x \in R$, then the principal ideal $(x) = \{rx : r \in R\}$.

Now, let's consider some examples of principal and non-principal ideals:

(1) Principal ideals in $\mathbb{Z}$ - the only subgroups of $\mathbb{Z}$ are $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. All these subgroups are ideals, so all ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z} = (n)$.

In $\mathbb{Z}$, $(\{n, m\}) = (\gcd(m, n))$. (cf. midterm exam)

(2) In $\mathbb{Z}[x]$, not every ideal is principal. Consider $(\{2, x\})$. If $(\{2, x\}) = (p(x))$ with $p(x) \in \mathbb{Z}[x]$, then p has to be a factor of both 2 and x. Thus $p = \pm 1$.

But for any $q \in (\{2, x\})$, q has even constant coefficients. Thus $p \notin (\{2, x\}) = (p(x))$ is a contradiction. Hence this is not a principal ideal.

2.7.3 Divisibility in ideals

Definition 2.7.6: *Given $a, b \in R$ where R is a commutative ring, we say that a **divides** b if there exists $c \in R$ such that $b = ac$.*

Theorem 2.7.7
Given that $a, b \in R$ where R is a commutative ring with a dividing b, we can say:

$$(a) = \{b \in R : a \text{ divides } b\}$$

Theorem 2.7.8
For $a, b \in R$ where R is a commutative ring, then $(b) \subseteq (a)$ iff $a \mid b$.

2.7.4 Further results about ideals

Assume that R is a ring with $1 \neq 0$, not necessarily commutative.

Theorem 2.7.9
Let $I \subseteq R$ be an ideal. Then $I = R$ iff I contains a unit.

Proof. If $I = R$, then $1 \in I$. If $x \in I$ is a unit, then for all $r \in R$, $r = (rx^{-1})x \in I$. □

Theorem 2.7.10
Let $I \subseteq R$ be an ideal. If R is commutative:

$$[\forall x \in R - \{0\},\ x \text{ is a unit}] \iff [\{\text{ideals of } R\} = \{0, R\}]$$

Proof. First, suppose that all nonzero elements of the ring have an inverse. Then any nonzero element is a unit. By the previous theorem, a nonzero ideal I thus equals R. Inversely, suppose that the only ideals in R are $\{0, R\}$. Then take $x \in R - \{0\} \implies (x) \in \{0, R\}$. Since $x \in (x)$, $(x) \neq 0$. Thus $(x) = R \implies x \mid 1$ is a unit. □

2.7.5 Other types of ideals

Definition 2.7.11: *Suppose $M \subseteq R$ is an ideal of a ring R. Then we say M is a **maximal ideal** if $M \neq R$ and M is not contained by any such ideals.*

Note that maximal ideals are not necessarily unique. For example, every $p\mathbb{Z} \subseteq \mathbb{Z}$ is a maximal ideal for primes $p \in \mathbb{Z}$. Further, these are the only maximal ideals in $\mathbb{Z}$.

Theorem 2.7.12
Let R be a commutative ring. An ideal $M \subseteq R$ is maximal iff R/M is a field.

Proof. By the fourth isomorphism theorem for rings, ideals of R/M correspond with ideals of R containing M. If M is maximal, then the only ideals containing M are $\{M, R\}$. Thus: $\{M/M, R/M\}$ are the only two ideals in the quotient ring via the fourth isomorphism theorem. Any nonzero $x \in R/M$ is a unit, so R/M is a field.
To check the inverse direction, suppose R/M is a field. Then all the nonzero elements are units. By the previous result, this means that the only ideals of R/M are $\{0, R/M\}$. Thus, by the fourth isomorphism theorem, all ideals of R containing M are simply

$$\{\pi^{-1}(M/M), \pi^{-1}(R/M)\} = \{M, R\}$$

Because there are only these two ideals containing M, we can determine that M must be maximal. □

Definition 2.7.13: *Let R be a ring, with $I \subseteq R$ a proper ideal. Then I is **prime** if for all $f, g \in R$, $fg \in I \implies f \in I$ or $g \in I$.*

Recall: we stated that the maximal ideals of $\mathbb{Z}$ are $p\mathbb{Z}$ for all prime numbers p. The prime ideals are the same, plus 0, which is not a maximal ideal.

Before stating the next theorems, recall that every field is an integral domain, but the reverse does not necessarily hold. However, remark that finite integral domains are fields. To see this, let A be a finite integral domain with element $a \neq 0$. Then, consider the map of sets

$$\begin{aligned} A &\to A \\ b &\mapsto a \cdot b \end{aligned}$$

which must be injective since there are no zero divisors. Due to finiteness, it's also surjective, and there must exist a $b \in A$ such that $a \cdot b = 1$. Thus, we have shown that an arbitrary nonzero element is a unit, so A is a field as desired.

Theorem 2.7.14
Let S be a commutative ring with a multiplicative identity $1 \neq 0$. Then S is a field iff 0 is a maximal ideal of S.

Proof. Note that for all $a \in S$, the following equivalence holds: $(a) = S \iff ab = 1$ for some $b \in S$, which means that a is a unit. Then, we know that S is a field precisely if $(a) = S$ for all nonzero $a \in S$. This holds iff 0 is a maximal ideal. □

Theorem 2.7.15
Let S be a commutative ring with a multiplicative identity $1 \neq 0$. Then S is an integral domain iff 0 is a prime ideal of S.

Proof. S is an integral domain precisely when $\forall f, g \in S,\ fg = 0 \implies f = 0$ or $g = 0$. This occurs exactly when 0 is a prime ideal in S. □

Theorem 2.7.16
Let R be a commutative ring with $1 \neq 0$. Say that $I \subseteq R$ is a proper ideal. Then the following pairs of equivalences hold:
(1a) I is maximal.
(1b) R/I is a field.
(2a) I is prime.
(2b) R/I is an integral domain.
Further, (1a) $\implies$ (2a) and (1b) $\implies$ (2b).

Proof. First, note that (1a) and (1b) are both equivalent to saying that 0 is a maximal ideal in R/I per the previously stated theorems and the fourth isomorphism theorem. Similarly, (2a) and (2b) are both equivalent to saying that 0 is a prime ideal in R/I. Part of this follows from the previous theorems; it remains to show that I is prime $\iff$ 0 is a prime ideal in R/I. To show this, write $\bar{f} = f + I$ and $\bar{g} = g + I$. Then:

$$\begin{aligned} I \text{ is prime} &\iff (fg \in I \implies f \in I \text{ or } g \in I) \\ &\iff \bar{f}\bar{g} \in 0 \\ &\iff \bar{f} \in 0 \text{ or } \bar{g} \in 0 \\ &\iff 0 \text{ is prime in } R/I \end{aligned}$$

In this way, we have shown both pairs of equivalencies. The implicatures from (1a) to (2a) and from (1b) to (2b) remain to be shown. □

Example 5: WTS $(x^2 + 1) \subseteq \mathbb{R}[x]$ is a maximal ideal. Then define the homomorphism:

$$\begin{aligned} \varphi : \mathbb{R}[x] &\to \mathbb{C} \\ p(x) &\mapsto p(i) \end{aligned}$$

Note that φ is surjective and $(x^2 + 1) \subseteq \ker \varphi$. In fact, $\ker \varphi = (x^2 + 1)$.

Theorem 2.7.17: Fundamental Theorem of Algebra
Any complex polynomial P factors as $a \cdot (x - c_1) \cdots (x - c_n)$ for $a_1, c_1, \ldots, c_n \in \mathbb{C}$. Further, if $P \in \mathbb{R}[x]$, then complex c_is come in conjugate pairs.

We can use this theorem to complete the previous example. By the first isomorphism theorem, conclude that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$, so (x^2+1) is maximal. On the other hand, any polynomial that can be factored in the reals, e.g., $x^2 - 3x + 2 = (x-1)(x-2) \subset (x-1)$.

2.8 Operations on ideals

Let R be a ring, with ideals $I, J \subseteq R$.

Definition 2.8.1: *The **sum** is $I + J = \{a + b : a \in I, b \in J\}$.*

Note that $I + I = I$, since this might be unintuitive.

Definition 2.8.2: *The **product**, denoted IJ, consists of all finite sums[a] of elements of the form ab where $a \in I$ and $b \in J$.*

[a] Don't forget the "finite sum" part of this definition!

Definition 2.8.3: *The nth **power** $I^n = I \cdots I$ (n times).*

For example, note that $I^2 = \{\text{finite sum of elements of form} ab \text{ with } a, b \in I\}$. In general, we can write $R = I^0 \supset I \supset I^2 \supset I^3 \supset \cdots$.

2.8.1 Monomial ideals

Definition 2.8.4: *A **monomial** in $\mathbb{R}[x, y]$ is a polynomial of form $a \cdot x^i y^j$ where $a \in \mathbb{R}$ and $i, j \geq 0$ are integers. A **monomial ideal** is an ideal generated by monomials, e.g., (x^3, xy, y^2).*

Lemma 2.8.5
If $I = (m_1, \ldots, m_n)$ is a monomial ideal, then a polynomial

$$f = \sum_{i,j \geq 0} a_{ij} x^i y^j$$

is in I iff each of the monomials in f is in I.

For example, $f = x^4 + 5xy + 6y^7 \in I$ since $x^4, 5xy, 6y^7 \in I$. However, $f = x + y + xy \notin I$.

Proof. We'll show the two separate directions of the equivalence below:
($\Longleftarrow$) Follows from I being closed under addition.
($\Longrightarrow$) Say $f = \sum a_{ij}x^iy^j \in I$ implies that $f = \sum_{i=1}^{n} P_i(x,y)m_i$ for some polynomials P_i. Thus, each monomial appearing in f is a monomial multiple of some m_i. □

3 Euclidean domains

Definition 3.0.1: *Let R be an integral domain. Then a* ***norm*** *on R is any function $N : R \to \mathbb{Z}_{\geq 0}$ such that $N(0) = 0$. N is* ***positive*** *if $N(a) > 0$ for all $a \neq 0$, $a \in R$.*

Definition 3.0.2: *An integral domain R is a* ***Euclidean domain*** *if there exists a norm $N : R \to \mathbb{Z}_{\geq 0}$ such that for all $a, b \in R$ with $b \neq 0$, then $a = qb + r$ for some $q, r \in R$ such that $r = 0$ or $N(r) < N(b)$.*

Consider the following examples of Euclidean domains:

- $\mathbb{Z}$ with $N(a) = |a|$, i.e., integer division with remainders.
- Any field with zero norm (norm function sends all to 0).
- Given any field F, then $F[x]$ is a Euclidean domain with $N(p(x)) :=$ degree of $p(x)$.
- Quadratic fields, quadratic integer rings.

3.1 Quadratic fields and quadratic integer rings

Definition 3.1.1: *Let D be a square-free integer. The field $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$ with multiplication is isomorphic to $\mathbb{Q}[x]/(x^2 - D)$. This is a* ***quadratic field****.*

Definition 3.1.2: *Inside $\mathbb{Q}(\sqrt{D})$, let $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$. This is called a* ***quadratic integer ring****.*

For example, if $D = -1$, then $Z[\sqrt{-1}] = \mathbb{Z}[i]$ is the ring of Gaussian integers.

Definition 3.1.3: *We can define the* ***field norm*** $\mathrm{N} : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ *as follows:*

$$\begin{aligned} \mathrm{N}(a + b\sqrt{D}) :&= (a + b\sqrt{D})(a - b\sqrt{D}) \\ &= a^2 - b^2 D \end{aligned}$$

which restricts to $\mathrm{N} : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$.

For example: $\mathrm{N}(a+bi) = (a+bi)(a-bi) = a^2+b^2$. Now, claim that $\mathbb{Z}[i]$ is a Euclidean domain with respect to this norm.

Theorem 3.1.4
The Gaussian integers are a Euclidean domain.

Proof. Say $\alpha = a+bi$ and $\beta = c+di$ where $\beta \neq 0$ and $\alpha, \beta \in \mathbb{Z}[i]$. Write $\alpha = (r+si)\beta$ for $r, s \in \mathbb{Q}$. Choose $p+qi \in \mathbb{Z}[i]$ such that $\mathrm{norm}((r+si)-p+qi) \leq \frac{1}{4}+\frac{1}{4} = \frac{1}{2}$. Then:

$$\alpha = ((r-p)i + (s-q)i)\beta + (p+qi)\beta$$

so check that $\mathrm{N}(((r-p)+(s-q)i)\beta)$ □

This can be adapted to show that $\mathbb{Z}[\sqrt{D}]$ is a Euclidean domain for $D = -2, -3, -7, -11$. However, $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean domain.

Definition 3.1.5: *An integral domain R is a* ***principal ideal domain*** *(abbreviated PID) if every ideal is principal.*

Examples of principal ideal domains include $\mathbb{Z}$ and $K[[x]]$ (ring of formal power series). However, $\mathbb{Z}[x]$ has a non-principal ideal $(2, x)$ and is not a PID.

Theorem 3.1.6
Euclidean domains are PIDs.

Proof. Let $I \subseteq R$ be an ideal where R is a Euclidean domain with norm $N : R \to \mathbb{Z}_{\geq 0}$. We want to show that I is principal. Consider two cases:

- If $I = 0 = (0)$, then we have already shown I is principal.
- If $I \neq (0)$, let $f \in I$ be a nonzero element with minimum norm. Then, claim that $I = (f)$. Indeed, we know $(f) \subseteq I$, so WTS the reverse inclusion. To do so, let $g \in I$, and have $g = qf + r$ for $q, r \in R$ and $r = 0$ or $\mathrm{N}(r) < \mathrm{N}(f)$. But $r \in I$ since $g, qf \in I$, so $r = 0$ by choice of f.

Thus, either $I = (0)$ or $I = (f)$, so every ideal is principal. □

Corollary 3.1.7
Once again, every ideal of $\mathbb{Z}$ is principal.

Corollary 3.1.8
$\mathbb{Z}[x]$ is not a Euclidean domain. (It's not even a PID!)

Definition 3.1.9: *Let R be a commutative ring with $a, b \in R$. Say $b \mid a$ if $a = bx$ for some $x \in R$.*

Definition 3.1.10: *Let R be a commutative ring with nonzero elements $a, b \in R$. Then a **greatest common divisor** of a, b is an element $d \in R$ such that:*
(1) $d \mid a$, $d \mid b$
(2) If $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

This new definition means that both ± 2 are greatest common divisors of $6, 8 \in \mathbb{Z}$. Similarly, we can apply this to polynomial rings: for example, what are the GCDs of $x^2 + x = x(x+1)$ and $x^2 - 1 = (x+1)(x-1)$ in $\mathbb{R}[x]$? Well, $(x+1)$ is a GCD, but so is any scalar multiple of it. So the GCDs are $\{a(x+1) : a \in \mathbb{R} - \{0\}\}$.

Theorem 3.1.11
If $a, b \in \mathbb{R} - \{0\}$ and $(a, b) = (d)$ for some $d \in R$, then d is GCD of a, b.

Proof. We know $d \mid a$ and $d \mid b$ since $a, b \in (d)$. Say $d' \mid a$ and $d' \mid b$; then, $(d') \supseteq (a, b) = (d)$. Therefore, $d' \mid d$. □

3.2 Revisiting the Euclidean algorithm

Theorem 3.2.1
Let R be a Euclidean domain with respect to a norm N, and let $a, b \in R$ be nonzero elements of the ring. Then the Euclidean algorithm operates as below:

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0 q_1 + r_1 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= r_n q_{n+1} + 0 \end{aligned}$$

where $N(r_0) > N(r_1) > \cdots > N(r_n)$ terminates and r_n is a GCD for a, b.

Proof. Same as the proof for the Euclidean algorithm in $\mathbb{Z}$. In particular, $r_n \mid r_{n-1}, r_{n-2}, \ldots, b, a$ and $r_n = ax + by$ for some $x, y \in R$. So $(r_n) = (a, b)$. Therefore, r_n is a greatest common denominator for a, b by the previous theorem.[a] □

[a] This explains why we use the notation (a, b) to denote the greatest common denominator of a, b.

3.3 Unique factorization domains

Definition 3.3.1: *Let R be an integral domain. Say $r \in R$ is a nonzero element that is not a unit. Then r is called **irreducible** if $r = ab \implies a$ or b is a unit.*

Definition 3.3.2: *Let R be an integral domain. A nonzero element $r \in R$ is **prime** if (r) is a prime ideal. That is, (r) is a proper ideal, and if $r \mid ab$, then $r \mid a$ or $r \mid b$. Equivalently, if $ab \in (r)$, then $a \in (r)$ or $b \in (r)$.*

Definition 3.3.3: *Say $a, b \in R$ are **associates** if $a = bu$ for $u \in R$ a unit. Note: this is an equivalence relation.*

Consider the following examples of unique factorization domains:

- In $\mathbb{Z}$, $\{\pm 2, \pm 3, \pm 5, \pm 7, \cdots\} = \{\text{irreducibles}\} = \{\text{primes}\}$. Associates are of form $\pm a$.
- In a field K, there are no irreducible elements, and there are no primes. Indeed, consider any nonzero element in K: such an element must be a unit.
- $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \cong \mathbb{Z}[x]/(x^2 + 5)$. Addition is component-wise, and multiplication behaves as follows:

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5}$$

  This example will demonstrate the difference between irreducibility and prime-ness. Now, claim that 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$. Note the norm on $\mathbb{Z}[\sqrt{-5}]$ is $N(a + b\sqrt{-5}) = a^2 + 5b^2 = (a + b\sqrt{-5})(a - b\sqrt{-5})$, which is multiplicative, i.e., $N(\alpha\beta) = N(\alpha)N(\beta)$. Say $3 = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Then $9 = N(3) = N(\alpha)N(\beta)$. It cannot be the case that $N(\alpha) = N(\beta) = 3$ since $N(a + b\sqrt{-5}) = a^2 + 5b^2$ can never equal 3. We can find a case where $N(\alpha) = 9, N(\beta) = 1$. But then either $\alpha = \pm 1$ or $\beta = \pm 1$, so 3 is irreducible as desired.

  However, 3 is not prime in $\mathbb{Z}[\sqrt{-5}]$. This is because $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, so $3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5})$, but $3 \nmid (2 \pm \sqrt{-5})$. Hence 3 is not prime.

Theorem 3.3.4
Let R be an integral domain, with prime element $p \in R$. Then p is irreducible.

Proof. Say p prime and $p = ab$ for $a, b \in R$. So $p \mid a$ or $p \mid b$; we may assume $p \mid a$, so write $a = pc$ for some $c \in R$. Combining these statements gives $p = pbc \implies bc = 1$ since R is an integral domain. In particular, this means b is a unit. □

Definition 3.3.5: *An integral domain R is called a **unique factorization domain** (UFD) if every nonzero element $r \in R$ that is not a unit, r has a factorization into irreducibles that's unique in the following sense:*
(1) $r = p_1 \cdots p_n$ for p_i irreducible
(2) if $r = q_1 \cdots q_m$ for q_i irreducibles, then $m = n$ and after reordering, p_i is an associate of q_i for each $i = 1, \ldots, n$.

Here are some examples and non-examples:

- $\mathbb{Z}$ is a UFD: for example, $12 = 2 \cdot 2 \cdot 3$. Reordering this factorization and multiplying by units (± 1) gives another factorization, e.g., $12 = (-3) \cdot (-2) \cdot 2$.

- Every principal ideal domain is a unique factorization domain (we'll prove this).
- If R is a unique factorization domain, then so is the polynomial ring $R[x]$.
- $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. As before, note that $9 = 3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$. As we have shown, $3, 2 \pm \sqrt{-5}$ are irreducible in R. Further, 3 and $2 \pm \sqrt{-5}$ are not associates. In fact, $\mathbb{Z}[\sqrt{-5}]$ is not even a principal ideal domain.

Theorem 3.3.6
$(3, 2 \pm \sqrt{-5})$ is not a principal ideal.

Proof. If instead $(3, 2\pm\sqrt{-5}) = (\alpha)$, then what could $N(\alpha)$ be? Note $N(\alpha) \mid 9$ since N is multiplicative. As we've shown before, $N(\alpha) \neq 3$, so $N(\alpha) = 1$ or 9. Could $N(\alpha) = 1$? If so, $\alpha = \pm 1$. If so, then it would mean that $(3, 2+\sqrt{-5}) = \mathbb{Z}[\sqrt{-5}]$; but that can't happen!
Alternatively, could $N(\alpha) = 9$? If so, $\alpha = \pm 3$, but also $\alpha = \pm(2+\sqrt{-5})$, which is a contradiction. Therefore $(3, 2 \pm \sqrt{-5})$ is not a principal ideal as desired. □

Lemma 3.3.7
If R is a unique factorization domain, p irreducible $\implies$ p prime.

Proof. Let $p \in R$ be an irreducible element. Given $a, b \in R$ such that $p \mid ab$, then we want to show that $p \mid a$ or $p \mid b$. Factor a, b into irreducibles and multiply them:

$$ab = a_1 \cdots a_n b_1 \cdots b_m$$

Then $p \mid ab \implies ab = p \cdot c = p \cdot c_1 \cdots c_k$. We conclude that p is an associate of some a_i or some b_j, so $p \mid a$ or $p \mid b$ as desired.
Alternatively, assume $p \nmid a$, and say $(p, a) = (d)$ for some $d \in R$. So either d is a unit, or $d = pu$ for some unit u via irreducibility. Since $p \nmid a$, then d is a unit. So $a = px + ay$ for $x, y \in R$, and therefore $b = pbx + aby$, so $p \mid b$ since $p \mid$ RHS. □

Corollary 3.3.8
Every nonzero prime ideal of a PID is maximal.

Definition 3.3.9: *Let R be an integral domain. The **field of fractions** of R is the field whose elements are equivalence classes of $\{(a, b) : a, b \in R, b \neq 0\}$ under the relation $(a, b) \sim (c, d)$ if $ad = bc$. Addition and multiplication are defined as follows:*

$$(a, b) \cdot (c, d) = (ac, bd)$$
$$(a, b) + (c, d) = (ad + bc, bd)$$

As an exercise: check this is a field!

For example, $FF(\mathbb{Z}) = \mathbb{Q}$. Now, let's state the following theorem about PIDs and UFDs. We'll work towards the proof in the following lemmas and definitions.

Theorem 3.3.10
Every PID is a unique factorization domain.

Lemma 3.3.11
If R is a PID, then every ascending chain of ideals stabilizes.[a] *That is, if*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

then there exists some N such that $(a_N) = (a_{N+1})$.

[a] This is called the ascending chain condition (ACC).

Proof. Consider $I = \cup_{i \geq 1}(a_i)$, and claim that I is an ideal. We'll prove this:

- **Closure under addition** - given $x, y \in I$, there exists $m \in \mathbb{Z}$ such that $x \in (x_m)$, and similarly $\exists n \in \mathbb{Z}$ such that $y \in (x_n)$. Then $(a_{\max(m,n)}) \ni x, y$, so $I \supseteq (a_{\max(m,n)}) \ni x + y$.
- **Closure under multiplication** - check that $rx \in I$ if $x \in I$.
- **Subgroup** - check that additive inverses exist in I.

So $I = (a)$ for $a \in R$, so $a \in (a_N)$. Therefore $(a_N) = I = (a_{N+1}) = (a_{N+2}) = \cdots$ □

Definition 3.3.12: *A ring is called **Noetherian** if every ideal is finitely generated.*

Theorem 3.3.13
The ascending chain condition (ACC) holds for all Noetherian rings.

Now, let's return to the theorem that all PIDs are UFDs. The proof is below:

Proof. Let $p \in R$ where R is a PID with $p \neq 0$ and non-unit. We'll show the following experessions:

1. Every such p can be factored into irreducibles.
2. Every such expression is unique up to reordering/associates.

We'll prove the first condition now. If p is irreducible, we win. Otherwise, let's say $p = p_1 p_2$ where p_1, p_2 are non-zero, non-unit elements. If p_1, p_2 are irreducible, then we're done. Therefore, let's assume that $p_1 = p_{11} p_{12}$ for p_{11}, p_{12} non-zero, non-units, continuing in this way forever. Observe that

$$(p) \subseteq (p_1) \subseteq (p_1 1) \subseteq \cdots$$

is an ascending chain which stabilizes by the previous element. Therefore, this process stops, so we can factor p into irreducibles.

Now, we need to check the second condition. We'll prove this via induction on $n =$ the number of factors in a minimal factorization of p.

- **Base case** - if $n = 1$, then p is irreducible.
- **Inductive step** - if $n > 1$, say that $p = r_1 \cdots r_n = q_1 \cdots q_m$ for $m \geq n$ (where r_i, q_i are irreducible). Then r_1 irreducible $\implies$ r_1 is prime by the previous lemma. Say $r_1 \mid q_1$ without loss of generality. Then $q_1 = r_1 \cdot u$ for some unit u.
  At this point, we're essentially done. We have "peeled off" a q_1 and r_1 from both expressions of p, and the statement follows by induction. More formally:

  $$p = r_1(r_2 \cdots r_n) = (u \cdot r_1)(q_2 \cdots q_m)$$

  so we're done by the inductive hypothesis applied to $r_2 \cdots r_n = u \cdot q_2 \cdots q_m$.

□

Theorem 3.3.14
If R is a UFD, then $R[x]$ is too. (Converse holds too!)

Here's the key idea behind this theorem: if F is a field, then $F[x]$ is a Euclidean domain. We'll use properties of UFDs and "bootstrap up" to this claim about fields and prove the equivalent statement for UFDs.

As an example, consider $x^2 - 1 \in \mathbb{Z}[x]$. We can write $x^2 - 1 = (2x-2)(\frac{1}{2}x + \frac{1}{2}) = (x-1)(x+1)$, and we want to show that these two expressions are equivalent. To do so, we'll use the field of fractions, as discussed on HW 11.

Lemma 3.3.15: Gauss's Lemma
Let R be a UFD, with $F = \text{Frac}(R)$. Further, let $p(x) \in R[x]$ with $p(x) = A(x) \cdot B(x)$, with $A, B \in F[x]$. Then, there exists $r, s \in F \setminus \{0\}$, such that $a(x) = r \cdot A(x)$, $b(x) = s \cdot B(x)$, and $p(x) = a(x) \cdot b(x)$ and also $a(x), b(x) \in R[x]$.

Proof. Clearing denominators, say $d \cdot p(x) = a'(x) \cdot b'(x)$ for $d \in R \setminus \{0\}$, $a', b' \in R[x]$. If d is a unit, then we're done. Otherwise, let $d = p_1 \cdots p_n$ where each $p_i \in R$ is irreducible. Without loss of generality, let us reduce both sides of the following equality modulo p_1:

$$p_1 \cdots p_n \cdot p(x) = a'(x) \cdot b'(x)$$

In other words, consider images under $R[x] \to R/(p_1)[x]$. Note that p_1 irreducible $\implies$ p_1 prime, so $R/(p_1)[x]$ is an integral domain. We have $0 = \overline{a'(x)} \cdot \overline{b'(x)}$, so without loss of generality, let's say that $\overline{a'(x)} = 0$, i.e., $p_1 \mid a'(x)$. Therefore, we can divide both sides of the equation by p_1, so here's the new equation:

$$p_2 \cdots p_n \cdot p(x) = \frac{a'(x)}{p_1} b'(x)$$

Proceed similarly on $p_2, \ldots, p_n$ to complete the proof. □

Example 6: To make this proof more clear, let's return to the case where $x^2 - 1 = (2x - 2)(\frac{1}{2}x + \frac{1}{2})$. As before, we can clear out denominators via multiplication by two:

$$2(x^2 - 1) = (2x - 2)(x + 1)$$

Then in $\mathbb{Z}/2\mathbb{Z}$, this reduces to $0 = 0 \cdot (x + 1)$. Then, we know that $2 \mid 2x - 2$, so we can divide both sides of the equation to get $(x^2 - 1) = (x - 1)(x + 1)$ as desired.

Corollary 3.3.16
Let R be a UFD, with $F = \mathrm{Frac}(R)$. Say $p(x) \in R[x]$ is irreducible or an element of $F[x]$. If a GCD of coefficients of p is 1, then p is irreducible over $R[x]$.

For example, $2x + 2$ is irreducible in $\mathbb{Q}[x]$, but not in $\mathbb{Z}[x]$.

Proof. If $p(x) = a(x)b(x)$ is reducible over $R[x]$ and if gcd(coefficients of p) $= 1$, then a, b are nonconstant polynomials. So $a(x)b(x)$ is a factorization over $F[x]$, too. □

Now, we'll prove the previous theorem: R is a UFD $\iff$ $R[x]$ is a UFD.

Proof. Say $p(x) \in R[x]$. By squeezing out the GCD of coefficients, we may assume that gcd(coefficients of p) $= 1$. That is, using the fact that R is a UFD, write $p(x) = d \cdot \widetilde{p}(x)$ where $d \in R \setminus \{0\}$ and $\widetilde{p}$ satisfies the GCD condition.
Then $p(x) = q_1(x) \cdots q_n(x)$ with $q_i \in R[x]$ that are irreducible over $F[x]$ (using Gauss's lemma). Then q_i are also irreducible over $R[x]$ since the GCD of coefficients of each q_i is 1 (follows from previous corollary).
For uniqueness of factorization, let's say

$$p(x) = q_1'(x) \cdots q_n'(x)$$

is another factorization. We can assume these factorizations have the same number of terms since $F[x]$ is a field and therefore a UFD. Then q_i, q_i' are associates in $F[x]$, and therefore they're also associates in $R[x]$. □

Corollary 3.3.17
If R is a UFD, then $R[x_1, \ldots, x_n]$ is too.

Proof. Via induction on n. □

4 Fields

Recall some examples of fields: $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields. However, we might also consider the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, or the field of fractions $\text{Frac}(R)$ over any integral domain R. We can even consider fields of fractions based on polynomial rings, e.g., $\mathbb{Q}(x) = \text{Frac}(\mathbb{Q}[x])$ and $\mathbb{F}_p(x) = \text{Frac}(\mathbb{F}_p[x])$.

Theorem 4.0.1
Any nonzero homomorphism of a field into a ring is injective.

Proof. Let $\varphi : K \to R$ be such a homomorphism. Then $\ker \varphi \subseteq K$ is an ideal, but $\ker \varphi \neq K$ by the assumption this is a nonzero homomorphism. Therefore, $\ker \varphi = 0$. □

Definition 4.0.2: *The **characteristic** of a field F is the smallest $p \in \mathbb{Z}_{>0}$ such that $0 = 1 + \cdots + 1$ (repeated p times), or is defined as 0 if no such p exists.*

Definition 4.0.3: *The **prime subfield** of F is the smallest subfield containing 1.*

Theorem 4.0.4
Any intersection of subfields of a field F is a field.

Theorem 4.0.5
Let F be a field. Either $\text{char}(F) = 0$ and the prime subfield is $\mathbb{Q}$, or $\text{char}(F) = p$ and the prime subfield is $\mathbb{Z}/p\mathbb{Z}$

Proof. Consider the following homomorphism:

$$\begin{aligned}\varphi : \mathbb{Z} &\to F \\ 1 &\mapsto 1 \\ n &\mapsto 1 + \cdots + 1 \text{ (repeated } n \text{ times)}\end{aligned}$$

First, let's consider the case in which φ is injective. Then we have $\text{char}(F) = 0$. Therefore, φ sends nonzero elements of $\mathbb{Z}$ to the units in F such that the below left diagram commutes:

Therefore, there exists a unique $\widetilde{\varphi}$ such that this diagram commutes. Then, $\widetilde{\varphi} \neq 0$ so $\widetilde{\varphi}$ is injective by the previous proposition, and $\mathbb{Q}$ is a prime subfield.
Now, we'll consider the case where φ is not injective (above right diagram). By the first isomorphism theorem, $\operatorname{im}\varphi \cong \mathbb{Z}/\ker\varphi$ so that $\mathbb{Z}/n\mathbb{Z} \subseteq F$. Then, n must be prime, or else this ring would have zero divisors, which cannot occur because then there would be zero divisors in F. Therefore $\mathbb{Z}/n\mathbb{Z}$ is a prime subfield. □

Definition 4.0.6: *If $F \subseteq K$ for fields F, K, then we say "K over F," often denoted K/F, is a* ***field extension.***[a]

[a] This is equivalent to the concept of a subfield. Don't confuse it with quotients!

In this situation, note that K has the structure of an F-vector space. That is, given elements $a \in F$, $x \in K$, then $a \cdot x = ax \in K$. For example, $\mathbb{C}/\mathbb{R}$ makes $\mathbb{C}$ an $\mathbb{R}$-vector space.

Definition 4.0.7: *The* ***degree*** *of the field extension K/F is $[K : F] = \dim_F K$, i.e., the dimension of K as an F-vector space.*

As an example of degree, note that $[\mathbb{C} : \mathbb{R}] = 2$. Meanwhile, $[\mathbb{R} : \mathbb{Q}] = \infty$ by convention.

4.1 Field extensions to solve polynomial equations

Suppose $p(x)$ is an irreducible polynomial in $F[x]$ for a field F, and we wish it hat a root! For example, $x^2 + 1 \in \mathbb{R}[x]$ is such a polynomial.

Now, let $K = F[x]/(p(x))$. Note that p is irreducible $\implies$ p is prime $\implies$ $F[x]/(p(x))$ is an integral domain. In fact, K is a field, since every nonzero prime ideal in a PID is maximal, and we quotiented by a maximal ideal. Further, there is an injective map $F \hookrightarrow F[x]/(p(x)) = K$. Note that this map is nonzero, and therefore K/X is a field extension in which p now has a root.

For example, the polynomial $x^2 + 1$ now has a root in $\mathbb{R}[x]/(x^2 + 1)$. However, we can't just say the solution is $i = \sqrt{-1}$, rather, we can express this as an equivalence class in $\mathbb{R}[x]/(x^2+1)$. For example, the element $\bar{x} = x+(x^2+1)$ is a root! Then $p(\bar{x}) = \overline{p(x)} = 0 \in K$.

Here's a more specific example: $\bar{x}^2 = (x + (x^2+1))^2 + (1 + (x^2+1)) = |x^2 + (x^2+1)| + |1 + (x^2+1)| = x^2 + 1 + (x^2+1) = 0 \in \mathbb{R}[x]/(x^2+1)$. Stare at this.

Note that if $F \subseteq K$ is a subfield, then we can plug in $a \in K$ into $p(x) \in F[x] \subseteq K[x]$. Warning: on $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, $x^2 + x$ and 0 give the same values on $\{0, 1\}$.

Theorem 4.1.1
Let F be a field. Say $p(x) \in F[x]$ is an irreducible polynomial of degree n. Write $\theta = \bar{x} = x + (p(x)) \in F[x]/(p(x)) =: K$. Then, $1, \theta, \theta^2, \ldots, \theta^{n-1}$ is a basis for K as an F-vector space. $[K : F] = n$.

Proof. First, we'll check that these elements span the vector space: if $a(x) \in F[x]$, then the Euclidean algorithm on $F[x]$ implies that:

$$a(x) = q(x)p(x) + r(x) \qquad \deg(r(x)) < n \text{ or } r = 0$$

Thus, $a(x) + (p(x)) \in \text{span}(1, \theta, \ldots, \theta^{r-1})$. Specifically, $r(x) = r_0 + r_1 x + \cdots + r_{n-1}x^{n-1}$. Then, $a(x) + (p(x)) = r_0 + r_1\theta + \cdots + r_{n-1}\theta^{n-1}$.
We have checked the span, so now let's see that these elements are linearly independent. Given $c_0, \ldots, c_{n-1} \in F$ such that $c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} = 0 \in K \iff c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in (p(x)) \implies c_0 = \cdots = c_{n-1} = 0$, so they are independent. □

Example 7: Let $p(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Note that p is irreducible, and let $K = \mathbb{F}_2[x]/(x^2 + x + 1)$. Note that $[K : F] = 2 \implies |K| = 4$. Then $1, x$ form a basis for K over $\mathbb{F}_2$. Here's how multiplication and addition work:

+	0	1	x	1+x
0	0	1	x	1+x
1	1	0	1+x	x
x	x	1+x	0	1
1+x	1+x	x	1	0

·	0	1	x	1+x
0	0	0	0	0
1	0	1	x	1+x
x	0	x	1+x	1
1+x	0	1+x	1	x

Theorem 4.1.2
There us a unique (up to isomorphism) field of each prime power.[a]

[a] The proof of this theorem is not within the scope of MATH 1530. (Non-examinable.)

Recall: we showed that if $p(x) \in F[x]$ is an irreducible polynomial of degree n, then $K = F[x]/(p(x))$ is a field extension over F. So if $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, then $\dim_F K = n$ so $|K| = p^n$.

Theorem 4.1.3
Any finite field must have prime power order.

Indeed, such a field a finite-dimensional vector space over its prime subfield $\mathbb{F}_p$, so its order is p^n for some n. Now, let's say K/F is a field extension:

Definition 4.1.4: *If $\{\alpha_i\}_{i\in I}$ is a collection of elements of K, let $F(\{\alpha_i\}_{i\in I})$ be the smallest subfield of K containing F and each α_i.*[a]

[a] "The field generated by $\{\alpha_i\}$ over F."

We need to check that the smallest subfield is equal to the intersection of all subfields of K containing $\{\alpha_i\}$. In other words:

$$\cap_{K\supseteq E\supseteq F} E = F(\{\alpha_i\})$$

If $\{\alpha_i\} \subseteq F$, then $F(\{\alpha_i\}) = F$ and conversely. For example, consider $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Then $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Check that this is a field.

4.2 More field extensions

Note that $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$ where $p(x) = x^2 - 2$.

Theorem 4.2.1
Let K/F be a field extension such that K has a root $\alpha \in K$ of an irreducible polynomial $p(x) \in F[x]$. Then $F(\alpha) \cong F[x]/(p(x))$.

Proof. We want to use the first isomorphism theorem, so let's define a map $\varphi : F[x] \to F(\alpha)$ be the "plugging-in-α" homomorphism, i.e., $\varphi(r(x)) = r(\alpha) \in K$. Note that $r(\alpha) = F(\alpha)$. Then $\ker\varphi \ni p(x)$ or $\ker\varphi \supseteq (p(x))$, so the following diagram commutes:

$$\begin{array}{ccc} F[x] & & \\ {\scriptstyle\pi}\downarrow & \searrow^{\varphi} & \\ F[x]/(p(x)) & \xrightarrow[\overline{\varphi}]{} & F(\alpha) \end{array}$$

and is called the universal property of quotients. Note that $\overline{\varphi}$ is a nonzero map from a field, and is therefore injective. Since $\operatorname{im}\overline{\varphi} \subseteq F(\alpha)$, we conclude that $F[x]/(p(x)) = \operatorname{im}\overline{\varphi} = F(\alpha)$ as desired. □

Theorem 4.2.2: Universal Property of Quotients
If $\varphi : R \to S$ is a ring homomorphism such that $I \subseteq R$ with $\ker\varphi \supseteq I$., then φ factors as shown below:

$$\begin{array}{ccc} R & & \\ {\scriptstyle\pi}\downarrow & \searrow^{\varphi} & \\ R/I & \xrightarrow[\overline{\varphi}]{} & S \end{array}$$

In other words, there exists a unique $\overline{\varphi}$ such that $\varphi = \overline{\varphi}\pi$.

4.3 Algebraic extensions

Let K/F be a field extension.

Definition 4.3.1: *$\alpha \in K$ is **algebraic** over F if it's the root of some nonzero polynomial $p(x) \in F[x]$. Otherwise, we call it **transcendental**.*

Definition 4.3.2: *We say K/F is **algebraic** if every $\alpha \in K$ is algebraic.*

Example 8: Here are some examples of algebraic and non-algebraic fields:

- F/F is algebraic. That is, for any $\alpha \in F$, then α is a root of $x - \alpha \in F[x]$.
- $\mathbb{R}/\mathbb{Q}$ is not algebraic. E.g., e and π are transcendental.
- $F(x)/F = \text{Frac}(F[x])$ is not algebraic.

Given these examples, let's ask: is $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ an algebraic extension over $\mathbb{Q}$? Well, $\sqrt{2}$ is algebraic, since $x^2 - 2 = 0$. For the general case, choose three elements $1, \alpha, \alpha^2 \in \mathbb{Q}(\sqrt{2})$. For example, we might choose

$$1 = 1 + 0\sqrt{2}$$
$$\alpha = 3 + 4\sqrt{2}$$
$$\alpha^2 = 41 + 24\sqrt{2}$$

There are three elements in this two-dimensional $\mathbb{Q}$-vector space $\mathbb{Q}(\sqrt{2})$, so they are dependent over $\mathbb{Q}$. (I.e., $6\alpha - \alpha^2 = -23$.) Therefore, α must be algebraic.

Theorem 4.3.3
Every finite extension K/F is algebraic.

Proof. Given $\alpha \in K$, the $n + 1$ elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly independent in the F-vector space K. Therefore, there exist $c_0, \ldots, c_n$ not all zero such that

$$c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$$

so therefore the field extension is algebraic. □

Definition 4.3.4: *A polynomial $p(x) \in F[x]$ is **monic** if the leading coefficient (i.e., on the highest degree term) is 1.*

Theorem 4.3.5
*Let $\alpha \in K$ be algebraic over F. Then there is a unique, irreducible monic polynomial $m_{\alpha,F}(x) \in F[x]$ having α as a root, and every polynomial for which α is a root is a polynomial multiple of $m_{\alpha,F}$. This $m_{\alpha,F}$ is a **minimal polynomial**.*

For example, consider $\mathbb{C}/\mathbb{R}$ with $\alpha = i$. Then the minimal polynomial is $x^2 + 1$, so any polynomial with root i is divisible by $x^2 + 1$. Also, observe $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$.

Proof. Consider the following "plugging-in-α" homomorphism:

$$\begin{aligned} \varphi : F[x] &\to F(\alpha) \subseteq K \\ p(x) &\mapsto p(\alpha) \end{aligned}$$

We have shown previously that φ is a homomorphism, with $\operatorname{im} \varphi = F(\alpha)$. Note that any $p(\alpha) \in F(\alpha)$.
On the other hand, if q is any nonzero polynomial with $q(\alpha) = 0$, then if $\deg q = n$, we have $F(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} : c_i \in F\}$. By the first isomorphism theorem, $F[x]/\ker \varphi \cong F(\alpha)$. Note that $\ker \varphi$ is ideal in $F[x]$, so $\ker \varphi = (p(x))$ for some p. Moreover, $(p(x))$ is maximal, and therefore prime, and therefore $p(x)$ is irreducible.
There's a unique choice of monic generator, which is the polynomial we want. □