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, $d' \mid d$. □