MATH-UA 349: Honors Algebra II

James Pagan

March 12, 2024

Contents

1 Exposition

MATH-UA 349 studies primarily **Ring Theory**, following *Algebra* by Michael Artin (2nd edition). At various times, we will use materials from other texts: for example, *Topics in Algebra* by Herstein. The grading policy is as follows:

1. 20%: Homework
2. 20%: Quizzes
3. 40%: Two midterms
4. 20%: Final Exam

More information can be found on Brightspace.

2 Rings

2.1 Definition

A **ring** is a tuple $(R, +, \cdot, 1)$ for binary operaitons $+ : R \times R \to R$ and $\cdot : R \times R \to R$ that satisfies the following axioms:

1. $(R, +)$ is an Abelian group. We denote its additive identity by 0.
2. Multiplication is associative.
3. Distributive laws: For all $a, b, c \in R$, we have $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$.
4. 1 is a multiplicative identity: for all $a \in A$, we have $a1 = 1a = a$.

We can view left multiplication ab by a for $b \in R$ as a mapping $\ell_a : R \to R$; if so, we only require that ℓ_a is an Abelian group homomorphism with respect to adition.

Remark 1. *Some texts do not assume the existence of multiplicative identity.*

2.2 Examples

1. **Integers**: The integers $\mathbb{Z}$ are the most motivating example of a ring, under addition and multiplication.

2. **Other Types of Numbers**: The rationals $\mathbb{Q}$, the reals $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are all rings under addition and multiplication.

3. **Zero Ring**: The zero ring $\{0\}$ with multiplicative and additive identity 0 is a ring.

4. **Functions over a Ring**: For a ring R and a set S, the set $\{f : S \to R\}$ is a ring under the ring's addition and multiplication — namely, $(f+g)(s) = f(s) + g(s)$ and $(f \cdot g)(s) = f(s) \cdot g(s)$.

5. **Functions over the Reals**: Setting $R = S = \mathbb{R}$ in the above example yields that real-valued functions are rings. It contains notable subrings, such as continuous functions, continuously differentiable functions, real analytic functions, and so on.

6. **Homomorphisms**: For an Abelian group A (with operation denoted by addition), the set $\mathrm{Hom}(A, A)$ is an Abelian group under addition and composition. The mulitiplicative operation is *not* commutative!

7. **Vector Spaces**: For a vector space V, the set of all linear operators $\mathcal{L}(V, V)$ is a ring under addition and composition of operators. This is actually a special case of the group homomorphisms above.

8. **Group Rings**: Let G be any group, not necessarily Abelian. If G is a group and R is a ring, then we can form a group ring:

$$RG = \left\{ \sum_{g \in G} a_g g \,\middle|\, a_g \in R,\ a_g = 0 \text{ for all but finitely many } g. \right\}$$

   Addition is defined naturally via the above definition. Multiplication is defined as follows:

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{g' \in G} b_{g'} g' \right) = \sum_{g, g' \in G} \Big((a_g g) \cdot (b_{g'} g') \Big)$$

9. **Quaternions**: Suppose that $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4$ are the basis vectors of $\mathbb{R}^4$. We often denote these by the following names:

$$\mathbf{e}_1 = 1, \quad \mathbf{e}_2 = \mathbf{i}, \quad \mathbf{e}_3 = \mathbf{j}, \quad \mathbf{e}_4 = \mathbf{k}.$$

   Addition is defined naturaly, treating each of the above as variables. As per multiplication, we declare

$$-1 = \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk},$$

   from which we can derive the full Cayley table for $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$. To multi0ply arbitrary quaternions, we simply distribute the following:

$$(a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k})(b_1 + b_2\mathbf{i} + b_3\mathbf{j} + b_4\mathbf{k})$$

   The set of all quaternions is denoted $\mathbb{H}$, and is *not* commutative; we have $\mathbf{ij} = -\mathbf{ji}$.

2.3 Motivation

Rings appear naturally in various contexts. For instance

1. **Factorization**: The unique factorization of integers over $\mathbb{Z}$ can generalize to certain clases of rings.

2. **Solving Equations**: Suppose we have a polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where coefficents lie in some number system $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Trying to solve equations pushes us to consider new number fields: the equation $x+1$ pushes us to consider $\mathbb{Z}$, the equation $2x = 1$ pushes us to consider $\mathbb{Q}$, and so on for $x^2 = 2$ and $x^2 = -1$.

3. **Systems of Linear Equations**: Suppose we have a system of equations

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n &= b_n, \end{aligned}$$

   where coefficents lie in some ring. The natural approach to solve such systems is Linear Algebra, with coefficents in a ring.

4. **Systems of Polynomial Euations**: For polynomials over some $\mathbb{R}$, if we have equations

$$p_i(x_1, \ldots, x_n) = 0$$

   for each $i \in \{1, \ldots, n\}$. Their study is enormous and beautiful, constituting the subject of **Algebraic Geometry**. The foundation of this theory (and indeed, the first page of Hartshorne) depends on the classical results of Commutative Ring Theory.

Rings appear in numerous areas of mathematics, including Geometry, Topology, and Analysis.

2.4 Terminology

STANDING ASSUMPTION: All rings are *assumed commutative* unless stated otherwise. We now introduce the following notions for $a \in R$:

1. **Units**: a is a unit if there exists $b \in R$ such that $ab = 1$.

2. **Field**: A ring R is a field if nonzero elements form a group under multiplication — notably, if every nonzero element is a unit. Since this group cannot be nonzero (as all groups), we mandate that R contains more than one element.

3. **Zero Divisors**: a is a zero divisor if there exists *nonzero* b such that $ab = 0$. Zero itself is a zero divisor.

4. **Modulo**: The ring $\mathbb{Z}/p\mathbb{Z}$ is the set of integers $0, \ldots, p-1 \pmod{p}$. This set is actually a field.

   Claim 1. *$\mathbb{Z}/p\mathbb{Z}$ has no zero-divisors.*

   Proof. We claim that $\mathbb{Z}/p\mathbb{Z}$ contains no zero divisors. Suppose for contradiction that there exists a, b such that $ab \cong 0 \pmod{p}$. Then by Euclid's Lemma,

$$\begin{aligned} ab \equiv 0 \pmod{p} &\implies p \mid ab \\ &\implies p \mid a \text{ or } p \mid b \\ &\implies a \equiv 0 \pmod{p} \text{ or } b \equiv 0 \pmod{p}. \end{aligned}$$

   Thus $\mathbb{Z}/p\mathbb{Z}$ contains no zero-divisors. We now claim that

   Claim 2. *A finite ring R with no zero divisors other than $0 \in R$ is a field.*

   Proof. Let R have n elements. For each $a \in R$, consider the set

$$a, a^2, \ldots, a^{n+1}.$$

   It has $n+1$ elements, all of which lie in R; then two must be equal. There exists $i, j \in \{1, \ldots, n+1\}$ with $i > j$ such that $a^i = a^j$. Then

$$a^{i-j} = 1 \qquad \text{and} \qquad a^{i-j-1} = a^{-1},$$

   Then each $a \in R$ is a unit, so R is a field.

   We conclude that $\mathbb{Z}/p\mathbb{Z}$ is a field.

2.5 Subrings

A **subring** of R is a subset $S \subseteq R$ which is also a ring using the same operations and 1.

It is easy to verify that S is a subring if and only if S is closed under addition, subtraction, multiplication, and contains 1. If $\Sigma \subseteq R$ is a subset, then the ring generated by *Sigma* is the smallest subring of R that contains Σ. Examples:

1. **Gaussian Integers**: The set $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. They are generated by $\mathbb{Z}$ and i.

2. **More Generally**: If $\alpha \in \mathbb{C}$, the set

$$\mathbb{Z}[\alpha] = \left\{ \sum_{j=1}^{k} a_j \alpha^j \,\middle|\, a_j \in R \text{ for each } j \in \{1, \dots, n\} \right\}$$

is a subring of $\mathbb{C}$. There are two subcases to consider:

   (a) **Case 1**: If for some n, there exists $a_n, \dots, a_0$ such that

$$\sum_{j=1}^{n} a_j \alpha^j,$$

   then α is an **algebraic number**.

   (b) **Case 2**: If no such n exists, then α is **transcendental**.

3. **Polynomial Rings (Informal)**: For a ring R, the set $R[x]$ is the set of all polynomials in x with coefficents in R. An element $f \in R[x]$ is a formal linear combination of powers of powers of x with coefficents in R:

$$a_n x^n + \cdots + a_1 x + a_0.$$

4. **Polynomial Rings (Formal)**: We define the set

$$\overline{R} = \{(a_n, \dots, a_1, a_0) \mid a_i \in R \text{ for each } i\}.$$

Elements of this set are *functions* from x to a ring R, expanding this into the expression in the informal definition.

Addition and multiplication are defined upon these objects as follows: for coefficents c_k of the product of $(a_n, \dots, a_0)$ and $(b_m, \dots, b_0)$, we set

$$c_k = \sum_{i+j=k} a_i b_j,$$

for $k \in \{0, \dots, n + m\}$.

3 Polynomial Rings

Recall that if R is a ring, then $R[x]$ denotes the ring of polynomials in x with coefficents in R. For a nonzero polynomial

$$f = a_n x^n + \cdots + a_1 x + a_0,$$

Several definitions are in order:

1. The **degree** of f is the largest power with a nonzero coefficent.
2. The **leading coefficent** of f is the coefficent of the term with the largest power.
3. A **monic polynomial** is a polynomial with leading coefficent 1.
4. A **constant polynomial** is a polynomial f such that $f = 0$ or $\deg f = 0$.

It is **not** true in general that $\deg f = n$ and $\deg g = m$ implies $\deg fg = n + m$ — so long as the leading terms of f and g are $a_n x^n$ and $b_m x^m$ and $a_n b_n = 0$. If the leading coefficents of f and g are not zero divisors, we may write $\deg fg = n + m$.

It is critical to distinguish between polynomials $f \in R[x]$ as *functions* versus *elements*. For some $\alpha \in R$, we may define $\Phi_\alpha : R[x] \to R$ by $\Phi_\alpha(f) = f(\alpha)$. We could also define for $f \in R[x]$ a mapping $\hat{f} : R \to R$ as $\hat{f}(x) = f(x)$. This function is not injective; the entirety of $\mathbb{Z} \,/\, 2\mathbb{Z}$ by

$$f = x^2 + x$$

For a ring R, the set $R[x_1, \ldots, x_n]$ denotes the set of **multivariate polynomials** in the variables $x_1, \ldots, x_n$ with coefficents in R. Addition and multiplication of these polynomials is similar to before.

4 Homomorphisms and Ideals

4.1 Homomorphisms

A **ring homomorphism** is a mapping $\varphi : R \to R'$ for rings R and R' such that the following properties are satisfied for any two $r, s \in R$:

$$\begin{aligned} \varphi(r) + \varphi(s) &= \varphi(r + s) \\ \varphi(rs) &= \varphi(r)\varphi(s) \\ \varphi(1) &= 1. \end{aligned}$$

The first condition states that φ is an Abelian group homorphism of the additive groups of R and R'. The usual categories of morphisms apply here:

1. A **monomorphim** φ is a injective homomorphism.

2. An **epimorphism** φ is a surjective homomorphism.

3. An **isomorphism** φ is a bijective homomorphism.

4. An **endomorphism** φ is a homomorphism $R \to R$.

5. An **automorphism** $\delta_w phi$ is an isomorphism $R \to R$.

Theorem 1. *If R is a ring, then there is a unique homomorphism $\phi : \mathbb{Z} \to R$.*

Proof. By definition, we have $\phi(1) = 1$. Then we may define for each $n \in \mathbb{Z}$:

$$\phi(n) = \phi(1 + \cdots + 1) = 1 + \cdots + 1.$$

A routine calculation verifies that this is a ring homomorphism. □

In a similar veign, a homomorphism $\Phi : R[x] \to R'$ is determined exclusively by the images of the constant polynomial.

Theorem 2 (Substitution Principle)**.** *If $\phi : R \to R'$ is a homomorphism and $\alpha \in R'$, then there exists a unique homomorphism $\Phi : R[x] \to R'$ such that $\Phi(x) = \alpha$ and*

$$\Phi(c) = \phi(c)$$

for all constant polynomials $c \in R$.

Proof. For uniqueness, it is easy to verify that

$$\Phi(a_n x^n + \cdots + a_0) = \sum_{i=0}^{n} \Phi(a_j)\Phi(x)^j = \sum_{i=0}^{n} \Phi(a_j)\alpha^j.$$

The rest of the proof is an exercise to the reader. □

Artin calls this the **substitution principle**, although this term is not standard. As an example, suppose we apply the substitution principle to

$$\Phi : \mathbb{Z}[x] \to \mathbb{Z}[i].$$

For instance, if $\Phi(x) = i$ and $\Phi(m) = m$, the homomorphism Φ is surjective. The substitution principle also verifies that

$$R[x_1, x_2] \cong (R[x_1])\,[x_2].$$

The **kernel** of a ring homomorphism $\phi : R \to R'$ is the set $\operatorname{Ker} f = \{a \in R \mid \phi(a) = 0\}$. Kernels satisfy the following properties:

1. The kernel is an additive subgroup of R.
2. For all $a \in \operatorname{Ker} f$ and $b \in R$, we have
$$\phi(ab) = \phi(a)\phi(b) = 0\phi(b) = 0,$$
so $ab \in \operatorname{Ker} f$. The kernel is thus closed under multiplcation by arbitrary ring elements.

This motivates the following definition:

4.2 Ideals

An **ideal** in a ring R is a nonempty set $\mathfrak{a} \subseteq R$ such that for all $a \in \mathfrak{a}$ and $r \in R$, we have

- $\mathfrak{a}$ is an additve subgroup of R.
- $ra \in \mathfrak{a}$.

All rings have at least two ideals: the zero ideal (denoted by 0 by abuse of notation) and R itself. The smallest ideal that contains $a_1, \ldots, a_n \in R$ is denoted
$$(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n \mid r_1, \ldots, r_n \in R\}.$$

An ideal is **principal** if it is generated by a single element: if $\mathfrak{a} = (a)$ for some $a \in R$. The ring R itself is a principal ideal generated by the multiplicative identity 1.

Subrings and ideals are almost always distinct: a subset S is a subring and an ideal if and only if $S = R$ or $S = 0$. Subrings contain the multiplicative identity 1, but ideals are closed under multplication by arbitrary ring elements.

Theorem 3. *R has precisely two ideals if and only if R is a field.*

Proof. Suppose R is a field, and pick $\mathfrak{a} \neq 0$. Then if $a \in \mathfrak{a}$, there exists a multiplicative inverse $a^{-1} \in R$. Hence, for all $r \in R$,
$$aa^{-1} = 1 \in \mathfrak{a} \implies r1 = r \in \mathfrak{a} \implies \mathfrak{a} = R.$$

Thus R has two ideals: 0 and R itself.

Suppose R has two ideals: R itself and 0. Then if $a \in R$ is nonzero, we have $(a) = R$; then $1 \in R \in (a)$, so there exists $r \in R$ such that $ar = 1$. Hence all nonzero $a \in R$ is invertible, so R is a field. □

Theorem 4. *Every ideal in $\mathbb{Z}$ is principal: if $\mathfrak{a} \neq 0$, then $\mathfrak{a} = (m)$, where m is the smallest positive element of I.*

Proof. Let $n \in \mathfrak{a}$; we may use the divison algorithm to deduce that there exist $a, b \in R$ such that

$$n = am + b,$$

where $0 \leq b < m$. Then $n - am \in R$, so $b \in R$; by the minimality of m, we have $b = 0$; thus $n = am$. We conclude that $\mathfrak{a} = (m)$. □

4.3 Applications to Polynomial Rings

Theorem 5 (Division Algorithm)**.** *Supppose that R is a ring, $f, g \in R[x]$, and f is monic. Then there exist unique $q, r \in R[x]$ such that*

$$g = qf + r,$$

where $0 \leq \deg r < \deg f$ *or* $r = 0$.

Proof. **Uniqueness**: Suppose there exist r_1, r_2 and $q_1 \neq q_2 \in R[x]$ such that

$$g = q_1 f + r_1 = q_2 f + r_2.$$

where $\deg r_1 < \deg f$ and $\deg r_2 < \deg f$. Then

$$(q_1 - f_1)f = r_1 + r_2.$$

This is a contradiction, since the degrees of both sides are not equal: $\deg(q_1 - q_2)f \geq \deg f > \deg r_1 + r_2$. We conclude that $q_1 = q_2$, so $r_1 = r_2$ too.

Existence: Consider the following set:

$$S = \{g - q'f \mid q' \in R[x]\}.$$

By the Well-Ordering Principle, there exists an element $r \in S$ of smallest degree. Define q such that

$$g = qf + r \implies r = g - qf.$$

If we suppose that $\deg r \geq \deg f$, then it is possible to subtract r by a multiple of f to eliminate the leading coefficent of f, which contradicts its minimality. We conclude that $\deg r < \deg f$, which completes the proof. □

Theorem 6. *If R is a field, then ever ideal $\mathfrak{a} \subseteq R[x]$ is principal: if $\mathfrak{a} \neq 0$, then $\mathfrak{a} = (f)$, where f is the monic polynomial in $\mathfrak{a}$ of smallest degree.*

Proof. The proof proceeds almost identally as before; suppose $g \in \mathfrak{a}$. Then there exists unique $q, r \in R[x]$ such that

$$g = qf + r,$$

where $0 \leq \deg r \leq degf$. Then $g = qf \in \mathfrak{a}$, so $r \in \mathfrak{a}$; by the minimality of $\deg f$, we conclude that $r = 0$. Hence $g = qf$; we conclude that $\mathfrak{a} = (f)$. □

Corollary 1. *Suppose $f \in R[x]$ and $\alpha \in R$. Then $f(\alpha) = 0$ if and only if $(x - \alpha) \mid f$.*

5 Quotient Rings

5.1 Definition

Let R be a ring with an ideal $\mathfrak{a}$. We can extend the notion of a quotient ring as follows, yielding a **quotient ring**:

Theorem 7. *The quotient group $R / \mathfrak{a}$ is a ring under the product $(a+\mathfrak{a})(b+\mathfrak{a}) = ab+\mathfrak{a}$ for $a, b \in R$.*

Proof. The quotient group $R / \mathfrak{a}$ exists, since $\mathfrak{a}$ is an additive subgroup of R and all subgroups of Abelian groups are normal. We must demonstrate that the product is well-defined.

Suppose $a + \mathfrak{a} = a' + \mathfrak{a}$ and $b + \mathfrak{a} = b' + \mathfrak{a}$. Then since $a - a' \in \mathfrak{a}$ and $b - b' \in \mathfrak{a}$,

$$ab - a'b \in \mathfrak{a} \qquad \text{and} \qquad a'b - a'b' \in \mathfrak{a}.$$

Thus, $ab - a'b' \in \mathfrak{a}$ and $ab + \mathfrak{r} = a'b' + \mathfrak{a}$. Then the product is well-defined. Proving that the product is closed and associative is trivial; the multiplicative identity of $R / \mathfrak{a}$ is $1 + \mathfrak{a}$, and the distributivity with addition is trivial — so $R / \mathfrak{r}$ is a ring. □

There is a natural surjective homomorphism $\phi : R \to R / \mathfrak{a}$ defined by $\pi(a) = a + \mathfrak{a}$. This is called the **canonical surjection** with respect to the ideal $\mathfrak{a}$.

5.2 Mapping Properties of Quotients

Suppose $\phi : R \to R'$ is a homomorphism such that $\mathfrak{k} = \ker \phi$, and let $\mathfrak{a}$ be an ideal such that $\mathfrak{a} \subseteq \mathfrak{k} \subseteq R$. Let $\pi : R \to R \,/\, \mathfrak{a}$ be the canonical surjection. Then two properties hold:

1. There is a unique mapping $\bar{\varphi} : R \,/\, \mathfrak{a} \to R'$ such that $\phi = \bar{\varphi} \circ \pi$: for all $a \in R$, we have $\phi(a) = \bar{\varphi}(a + \mathfrak{a})$.
2. If ϕ is surjective, then $\mathfrak{k} = I$ and $\bar{\varphi} : R \,/\, \mathfrak{a} \to R'$ is an isomorphism.

The idea is simple: simply define $\bar{\varphi}(a + \mathfrak{a}) = \phi(a)$, and demonstrate this mapping a well-defined homomorphism.

Theorem 8 (Correspondence Theorem)**.** *There is a one-to-one correspondence between ideals of $\phi(R)$ and ideals of R that contain $\mathfrak{k}$.*

Proof. For an ideal $\mathfrak{a}'$ of $\phi(R)$, define $\mathfrak{a} = \{a \in R \mid \phi(a) \in \mathfrak{a}'\}$. By the Correspondence Theorem for groups, $\mathfrak{a}$ is an additive subgroup of R. For all $a \in \mathfrak{a}$ and $b \in R$, we have $\phi(a) \in \mathfrak{a}'$; thus

$$\phi(ab) = \phi(a)\phi(b) \in \mathfrak{a}'$$

since $\mathfrak{a}'$ is an ideal. Thus $ab \in \mathfrak{a}$, so $\mathfrak{a}$ is an ideal of R. Since $0 \in R'$, we have that $\mathfrak{k}$ is a subideal of $\mathfrak{a}$. It is now relatively trivial to establish a one-to-one correspondence. □

Corollary 2. *There is a one-to-one correspondence between ideals of $R \,/\, \mathfrak{a}$ and ideals of R that contain $\mathfrak{a}$.*

The Correspondence Theorem expands upon the result of the First Isomorphism Theorem.

5.3 Applications to Polynomials

Suppose that R is a ring, and for $a \in R$,

$$b_n a^n + \cdots + b_1 a + b_0 = 0.$$

Consider the quotient ring $R \,/\, (b_n a^n + \cdots + b_0)$: all $\bar{a}$ in the ring's zero ideal satisfy $b_n \bar{a}^n + \cdots + b_0 = 0$.

As an unrelated example, suppose $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[i]$ substitutes x for i. Question: what is the kernel of φ? Let $\phi(x) = i$ and $\phi(a) = a$ for all $a \in \mathbb{Z}$; observing that $i^2 + 1 = 0$ leads us to propose the following:

Claim 3. $\operatorname{Ker}\varphi = (x^2+1)$*, where* (x^2+1) *is a principal ideal.*

Proof. Pick $g \in \operatorname{Ker}\varphi$. Then $\phi(g) = 0$ implies $g(i) = 0$, so $(x^2+1) \mid g$; we conclude that $g \in (x^2+1)$. The converse is easy to demonstrate as well, so $\operatorname{Ker}\varphi = (x^2+1)$. □

Therefore, we deduce that $\mathbb{Z}[x] \,/\, (x^2+1) \cong \mathbb{Z}[i]$. By examining the homomorphism $\psi : \mathbb{Z}[x] \to \mathbb{Z}$ defined by $\psi(x) = a$ for $a \in \mathbb{Z}$, we find that $\mathbb{Z}[x] \,/\, (x-a) \cong \mathbb{Z}$; the same is true if we substitute $\mathbb{Z}$ for $\mathbb{R}$, or some other number system.

6 Adjoining Elements

6.1 Definition

An **extension** of a ring R is a ring R' which contains R. Now, suppose we have a composition of mappings

$$R \to R[x] \to R[x] \,/\, \big(f_1(x), \ldots, f_n(x)\big);$$

this is called **adjoining elements** to the ring R. In fact, we can use this to construct the complex numbers independenetly:

$$\mathbb{R} \cong \mathbb{R}[x] \,/\, (x^2+1).$$

The proof is relatively easy, defining $\phi : \mathbb{R}[x] \to \mathbb{C}$ by $\phi(x) = i$ and $\phi(a) = a$ for $a \in \mathbb{R}$. Naturally, ϕ is is a surjective homomorphism with kernel (x^2+1), so the First Isomorphism Theorem yields the desired isomorphism.

Theorem 9. *Suppose* R *is a ring, and* $f(x) \in R[x]$ *is monic of degree* n*: that* f *is of the form*

$$f(x) = x^n + h_{n-1}x^{n-1} + \cdots + h_0.$$

Then two claims about $R[x] \,/\, (f(x))$ *are in order:*

1. *Any residue* $\beta \in R[x] \,/\, (f(x))$ *has a unique representation as* $a_{n-1}x^{n-1} + \cdots + a_1x + a_0$.
2. *If* $g_1, g_2 \in R[x]$*, then the product of the residues in* $R[x] \,/\, (f(x))$ *is represented by* $r(x)$*, where*

$$g_1(x)g_2(x) = q(x)f(x) + r(x)$$

such that $r = 0$ *or* $\deg r < deg f$.

Proof. (1) follows from the division algorithm, dividing β by f; the desired representation is the remainder polynomial. (2) is natural. □

As an example: if we set $f(x) = x^2 + 1$, we attain the multiplication formula for complex numbers.

If we wished to adjoin $\mathbb{Z}_5$ by $\sqrt{3}$ to get $\bar{R}$, we adjoin δ such that $\delta^2 = 3$; the desired ring $\bar{R}$ is isomorphic to

$$\mathbb{Z}_5[\delta] \,/\, (\delta^2 - 3).$$

We attain that the elements are of the form $a\delta + b$ for integers a and b by Theorem 9; there are 25 elements. It is not difficult to demonstrate that $\bar{R}$ is a field.

6.2 A Question

Suppose f is a polynomial over R with a leading coefficent which is not a unit: what if we adjoin f to R? Let us consider an example:

1. **Integers**: Suppose we would like to adjoint $\frac{1}{2}$ to the integers: since $\frac{1}{2}$ satisfies $2x - 1 = 0$, the ring we seek is
$$\mathbb{Z}[x] \,/\, (2x - 1) \;\cong\; \mathbb{Z}\left[\tfrac{1}{2}\right].$$
The isomorphism shown above is quite easy: let $\phi(x) = \frac{1}{2}$ and $\phi(n) = n$ for $n \in \mathbb{Z}$. It is easy to demonstrate that ϕ is injective (well-ordering principle on the degree of a polynomial in the kernel) and surjective.

2. **Modulo 4**: Suppose we would like to adjoint $\frac{1}{2}$ to the integers modulo 4: then
$$\mathbb{Z}_4[x] \,/\, (2x - 1) \cong 0,$$
actualy. Be careful: adjoining elements can have strange consequences.

6.3 Direct Product

Suppose R and R' are rings. Then the **product ring** $R \times R'$ is defined as follows:

$$R \times R' = \{(r, r') \mid r \in R, r' \in R'\},$$

with componentwise addition and multiplication. The multiplicative identity of the product ring is $(1, 1)$. Properties of the Quotient Ring are as follows:

1. **Projections**: The product induces homomorphisms $\pi : R \times R' \to R$ and $\pi' : R \times R' \to R'$ that isolate each coordinate. The kernel of these objects is easy to observe: they are $0 \times R'$ and $R \times 0$ respectively, which are principal ideals of $R \times R'$ and isomorphic to R' and R respectively. In fact,
$$R \times R' = (R \times 0) + (0 \times R'),$$

where that is the sum of ideals. We could further write

$$R = (R \times R') \,/\, (0 \times R').$$

How can we tell if a ring R is isomorphic to a product? There are two approaches:

1. **Approach 1**: Look for idempotent elements (like $(1, 0)$ and $(0, 1)$ in the prior examples). Observe that if e is idempotent, then $e' = 1 - e$ is idempotent too, and $ee' = 0$; then

   Claim 4. *If $S_e = (e)$ and $S_{e'} = (e')$, then $R \cong S_e \times S_{e'}$.*

   Here is an example from Artin: suppose we would like to "adjoin $\sqrt{3}$" to $\mathbb{Z}_{11}$. Then the ring we seek is

   $$\mathbb{Z}_{11}[\delta] \,/\, (\delta^2 - 3).$$

   Now, observe that

   $$(\delta^2 - 3) = (\delta^2 - 25) = (\delta + 5)(\delta - 5).$$

   It is relatively easy to verify that $\delta + 5$ and $\delta - 5$ are both idempotent. Utilizing principal ideals, we conclude that

   $$\mathbb{Z}_{11}[\delta] \,/\, (\delta^2 - 3) \;\cong\; (\delta + 5) \times (\delta - 5)$$

   Those ideals $(\delta + 5)$ and $(\delta - 5)$ mod *twice*. They are congruent to $\mathbb{Z}_{11} \,/\, (\delta - 5, \delta^2 - 3) = \mathbb{Z}_{11} \,/\, (\delta - 5)$, so we actually have

   $$\mathbb{Z}_{11}[\delta] \,/\, (\delta^2 - 3) \quad \cong \quad \Big(\mathbb{Z}_{11}[\delta] \,/\, (\delta + 5)\Big) \times \Big(\mathbb{Z}_{11}[\delta] \,/\, (\delta - 5)\Big).$$

6.4 Field of Fractions

Let R be an integral domain. Then we define **fractions** as the two operations on $R \times (R \backslash 0)$, ordered pairs $(a, b) \sim \frac{a}{b}$, where $b \neq 0$, as shown:

$$(a, b) + (c, d) = (ad + bc, bd) \qquad \text{and} \qquad (a, b) \times (c, d) = (ac, bd).$$

We write that $(a, b) \sim (c, d)$ if and only if $ad = bc$. It is easy to verify that $R \times (R \setminus 0)$ under these operations is a field. Properties are as follows:

1. **Embedding**: The embedding $\phi : R \to F$ defined by $\phi(r) = (r, 1)$ is an injective homomorphism. Hence, $R \cong \phi(R)$.

2. **Fractions of Polynomials**: Since $\mathbb{Q}[x]$ is an integral domain, we can defined the field of fractions on $\mathbb{Q}[x]$ — the **field of rational functions**.

7 Maximal Ideals

A **maximal ideal** $\mathfrak{m}$ of R is a *proper* ideal of R such that no other ideals contain $\mathfrak{m}$, aside from $\mathfrak{m}$ itself and R.

Theorem 10. *An ideal $\mathfrak{m}$ of R is maximal if and only if $R \,/\, \mathfrak{m}$ is a field.*

Proof. By the Correspondence Theorem, there is a one-to-one correspondence between ideals of R that contain $\mathfrak{m}$ and ideals of $R \,/\, \mathfrak{m}$. Then

$$\begin{aligned} \mathfrak{m} \text{ is maximal} &\iff \text{The only ideals of } R \,/\, \mathfrak{m} \text{ are } (0) \text{ and } R \,/\, \mathfrak{m} \text{ itself.} \\ &\iff R \,/\, \mathfrak{m} \text{ is a field,} \end{aligned}$$

yielding the desired result □

Examples of maximal ideals are as follows:

1. **Integers**: The maximal ideals in $\mathbb{Z}$ are preisely the prime ideals, (p) for prime p.

8 Factoring

Our goal is to substantially generalize the unique factorization of integers to a much more general setting.

Theorem 11. *Let $m > 1$ be an integer. Then we can express m as $p_1^{e_1} \cdots p_n^{e_n}$ uniquely.*

Proof. There are two components to the proof:

1. **Existence**: Strong induction. We just demonstrate that $m+1$ is either prime, or a product of two numbers — which are products of prime by the inductive hypothesis.
2. **Uniqueness**: Since (p) is prime and $\mathbb{Z}$ is a Principal Ideal Domain, (p) is maximal — thus $\mathbb{Z} \,/\, (p)$ is a field. Now, suppose

$$p_1^{e_1} \cdots p_n^{e_n} = p_1^{\prime e'_1} \cdots p_k^{\prime e'_k}.$$

Then since $p_1^{\prime e'_1} \cdots p_k^{\prime e'_k}$ is zero in the ring $\mathbb{Z} \,/\, (p_1)$, it must lie in the ideal (p_1); since this ideal is prime, some $p_j^{\prime e'_j}$ must lie in p. Thus both sides are equal.

□

Let F be a field. Then $f \in F[x]$ is **irreducible** if f is nonconstant and does not factor as a product of nonconstant polynomials. In a ring R, two nonzero elements are **associative** if $a = ub$, where u is a unit.

Theorem 12. *If $f \in F[x]$ is nonconstant, then there exists a factorization*

$$f = p_1^{e_1} \cdots p_n^{e_n},$$

where each p_i is irreducable, and this factorization is unique up to permutation and multiplication by constants.

Proof. There are two components to the proof:

1. **Existence**: Use strong induction on the degree of f. If f is irreducible, we are done; otherwise, $f = gh$ and g and h factor into irreducible polynomials.
2. **Uniqueness**: Since each p_i is irreducible and $F[x]$ is a principal ideal domain, (p_i) is a maximal ideal. The same argument as before applies.

We encourage the reader to flesh out this skeleton of a proof. □

Corollary 3. *Suppose $f \in \mathbb{R}[x]$ is irreducible. Then either f is constant, $f = ax + b$, or $f = c(x + \alpha)(x - \alpha)$ for a complex number $\alpha \notin \mathbb{R}$.*

Corollary 4. *A polynomial of degree n has at most n roots.*

We now extend the notion of $\mathbb{Z}[i]$. We utilize the following lemma:

Lemma 1. *$\alpha \in \mathbb{Z}[i]$ is a unit if and only if $\alpha \in \{1, i, -1, -i\}$.*

Proof. If α is a unit, then there exists $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$. Then

$$|\alpha||\beta| = 1;$$

since the minimum of the absolute value is 1, both α and β must be on the unit circle. The rest of the proof is natural. □

A nonzero $p \in \mathbb{Z}[i]$ is **prime** if p is not a unit and p cannot be expressed as a product of two nonunits — if every factor is a unit or an associate.

Theorem 13. *Any nonzero $\alpha \in \mathbb{Z}[i]$ has a unique factorization $\alpha = p_1^{e_1} \cdots p_n^{e_n}$*

Proof. An intuction argument similar to before demonstrates existence. To demonstrate uniqueness, we would like to prove that $\mathbb{Z}$ is a principal ideal domain.

We use the **division algorithm**: if $a, b \in \mathbb{Z}[i]$ where $a \neq 0$, there exist $q, r \in \mathbb{Z}[i]$ such that

$$b = aq + r,$$

where r is either zero or $|r| < |a|$. To demonstrate that $\mathfrak{a} \subseteq \mathbb{Z}[i]$ is maximal, we pick $a \in \mathfrak{a}$ with minimal absolute value and apply the Division Algorithm. Thus the previous argument holds. □

A ring R is a **Principal Ideal Domain** if R is an integral domain and all ideals of R are principal. An integral domain is a **Euclidean Domain** if there is a function $\sigma : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that for all $a, b \in R$ with $a \neq 0$, there exists $q, r \in R$ such that

$$b = qa + r,$$

where either $r = 0$ or $\sigma(r) < \sigma(a)$. It is clear that any Euclidean Domain is a Principal Ideal Domain, and that prime factoization in a PID is unique.

Theorem 14. *If R is an integral domain, then factoring terminates in R if and only if there does not exist a strictly increasing sequence of principal ideals $(a_1) \subseteq (a_2) \subseteq \cdots$*

Proof. Suppose factoring does not terminate: $a = a_1 a_2 = a_1(a_{21}a_{22}) = a_1 a_{21}(a_{31}a_{32}a_{33}) = \cdots$. Then it is easy to see that we can construct an infinite chain of principal ideals. The other direction is simple. □

Lemma 2. *If R is a principal ideal domain, then factoring terminates.*

Proof. Since each ideal in R is generated by a single element, each ideal is finitely generated —in other words, R is Noetherian. Thus the ascending chain of strictly increasing ideals does not exist, so factoring terminates in R. □

As an example, $\mathbb{Z}[\sqrt{-5}]$ satisfies factorization, but it is not unqiue: $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

9 Modules

9.1 Definition

An **R-module** over a commutative ring R is an abelian group M (with operation written additively) endowed with a mapping $\mu : R \times M \to M$ (written multiplicatively) such that the following axioms are satisfied for all $x, y \in M$ and $a, b \in R$:

1. $1x = x$;
2. $(ab)x = a(bx)$;
3. $a(x + y) = ax + ay$;
4. $(a + b)x = ax + bx$.

9.2 Examples

- If R is a ring, $R[x]$ is a module.
- All ideals $\mathfrak{a}$ of R are R-modules using the same additive and multiplicative operations as R — in particular R itself is an R-module.
- If R is a field, R-modules are R-vector spaces. In fact, the axioms above are identical to the vector axioms, defined over commutative rings instead of fields.
- Abelian groups G are precisely the modules over $\mathbb{Z}$.
- Given a F-vector space V and $\mathbf{T} \in \mathcal{L}(\mathbb{F})$, we may regard V as an $F[x]$-module as follows: if $f(x) = a_n x^n + \cdots + a_0$, we have

$$f(x)\,\mathbf{v} \quad \overset{\text{def}}{=} \quad a_n \mathbf{T}^n \mathbf{v} + \cdots + a_n \mathbf{v}.$$

9.3 Homomorphisms of Modules

A map $f : M \to N$ between two R-modules M and N is an **R-module homomorphism** (or is R-linear) if for all $a \in R$ and $x, y \in M$,

$$f(x + y) = f(x) + f(y)$$
$$f(ax) = af(x).$$

Thus, an R-module homomorphism f is a homomorphism of abelian groups that commutes with the action of each $a \in R$. If R is a field, an R-module homomorphism is a linear transformation. A bijective R-homomorphism is called an R-isomorphism.

9.4 Submodules and Quotient Modules

A **submodule** M' of M is an abelian subgroup of M closed under multiplication by elements of the commutative ring R. The following proof outlines a construction of **quotient modules**:

Theorem 15. *The abelian quotient group M/M' is an R-module under the opreation $r(x + M') = rx + M'$.*

Proof. We must perform four rather routine calculations:

1. For all $x \in M$, we have that $1(x + M') = 1x + M' = x + M'$.
2. For all $r, s \in R$ and $x \in M$, we have that $r(s(x+M')) = r(sx+M') = rsx+M' = (rs)(x + M')$.
3. For all $r, s \in R$ and $x \in M$, we have that $(r + s)(x + M') = (r + s)x + M' = (rx + sx) + M' = (rx + M') + (sx + M') = r(x + M') + s(x + M')$.
4. For all $r \in R$ and $x, y \in M$, we have that $r((x + M') + (y + M')) = r((x + y) + M') = r(x + y) + M' = (rx + M') + (ry + M') = r(x + M') + r(y + M)'$.

Therefore, M/M' is an R-module. □

9.5 Assorted Submodules

Let $f : M \to N$ be an R-module homomorphism. Then the **kernel** and **image** of f are defined as follows:

$$\operatorname{Ker} f = \{x \mid x \in M, f(x) = 0\} \qquad \text{and} \qquad \operatorname{Im} f = f(M),$$

and are submodules of M and N respectively. The **cokernel** of f is defined as follows:

$$\operatorname{Coker} f = N \,/\, \operatorname{Im} f.$$

If M' is a submodule of M such that $M' \subseteq \operatorname{Ker} f$, then f induces a natural homomorphism $\bar{f} : M/M' \to N$ defined by $\bar{f}(x + M') = f(x)$. The kernel of $\bar{f}$ is $\operatorname{Ker} f \,/\, M'$ — the distinct cosets of M' in the kernel of f. Taking $M' = \operatorname{Ker} f$ yields the First Isomorphism Theorem for R-modules:

$$M \,/\, \operatorname{Ker} f \cong \operatorname{Im} f.$$

9.6 Cyclic Modules

An R-module M is **cyclic** if it is generated by a single element. The following fact is a consequence of the fact in Atiyah-MacDonald: that M is generated by $x_1, \ldots, x_n$ if and only if $M \cong R^n / \mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq R^n$.

Lemma 3. *Let M be an R-module. Then the following are equivalent:*

1. *M is cyclic.*
2. *$R \to M$ is a surjective R-module homomorphism.*
3. *$M \cong R / \mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq R$.*

We are now ready to prove the following:

Theorem 16. *Let M be a finitely-generated R-module. Then*

$$M = N_1 \oplus \cdots \oplus N_k \oplus L,$$

where $N_i \cong R / (d_i)$ and $d_i \mid d_j$ when $i \leq j$, and L is a finitely-generated free module: $L \cong R^m$.

Proof. Let M be generated by $x_1, \ldots x_n$. By the proof from Atiyah-MacDonald, we have that

$$R \cong R^n / \mathfrak{a}$$

We now utilize the following lemma:

Claim 5. *Any submodule $N \subseteq R^m$ is a finitely-generated free module of rank m or smaller.*

Proof. The proof follows the logic that if ideals $\mathfrak{a} \subseteq R$ are finitely-generated, then submodules of finitely-generated R-modules are finitely generated. □

Observe that $\psi : R^n \to M$ is surjective. Hence $\operatorname{Ker} \psi$ is finitely-generated, so $\operatorname{Ker} \psi \subseteq R^m$, where $\operatorname{Ker} \psi$ is generated by $y_1, \ldots, y_m$. Hence there exists a homomorphism $\phi : R^n \to R^m$ such that $\operatorname{Im} \phi = \operatorname{Ker} \psi$. Hence if $\mathbf{T}$ is the matrix of ϕ, we have

$$M \cong R^m / \mathbf{T} R^n.$$

We may assume without loss of generality that $\mathbf{T}$ is diagonal with entries $d_1, \dots, d_k, 0, \dots$. Then $W_j = R\mathbf{e}_j \subseteq R^m$ is a cyclic submodule. And furthermore $\overline{W}_j = \pi(W_j) \subseteq R^m \,/\, \mathbf{T}R^n$ is cyclic. IF we prove that

$$R_m \,/\, \mathbf{T}R^n \cong \overline{W}_1 \oplus \cdots \oplus \overline{W}_m,$$

the theorem is proven (somehow?????). □

We now take a moment to examine linear operators. If $\mathbf{T} \in \mathcal{L}(V)$ is a linear operator over a F-vector space V, there is a natural $F[x]$-module structure on V for $f = f_n x^n + \cdots + f_0$ and $\mathbf{v} \in V$ as

$$f\mathbf{v} = \sum_j f_j \mathbf{T}^j \mathbf{v}.$$

A routine calculation verifies that V is an $F[x]$-module. If V is a finite-dimensional vector space with a basis $\mathbf{v}_1, \dots, \mathbf{v}_n$, then $\mathbf{v}_1, \dots, \mathbf{v}_n$ is a generating set for V as an $F[x]$-module. Hence

$$V = W_1 \oplus \cdots \oplus W_k \oplus L$$

as before. Observe that $\mathcal{L} \cong F[x]^m$ is infinite-dimensional as an F-module, since each $F[x]$ is infinite-dimensional. The basis of $F[x]$ as an F-vector space is $1, x, x_2, x_3, \dots$ and so on. Thus if V is finite-dimensional, we must have that $L = 0$.

As per each W_j, we have that $W_j \cong F[x] \,/\, (d_j)$, where $d_j \in F[x]$ is nonzero and monic. If $\deg d_j = 0$, then the quotient is zero; so without loss of generality, suppose $\deg d_j > 0$. (insert matrix of x with respect to th e basis $1, x_1, \dots, x_{n-1}$).

This introduces **rational canonical form**: let $\mathbf{T} : V \to V$ be a linear operator on a finite-dimensional vector space over F. Then there exists a basis $\mathbf{B}$ for V such that $[\mathbf{T}]_{\mathbf{B}}$ has a block diagonal form. This is true because

$$F[x]\text{-submodule of } V \iff \text{linear subspace } W \subseteq V \text{ which is } \mathbf{T}\text{-invariant: } \mathbf{T}(W) \subseteq W.$$

9.7 Noetherian Rings

Recall that R is Noetherian if every ideal $\mathfrak{a} \subseteq R$ is finitely-generated. All PIDs are Noetherian.

10 TIMESKIP!

11 Fields

11.1 Degree of a Field Extension

Let $K \,/\, F$ be a field extension. The **degree** $[K : F]$ is the dimension of K as an F-vector space. Several observations follow:

1. $[K : F] = 1$ if and only if $K = F$.
2. $[K : F] = 2$ if and only if $K = F[\delta]$, where δ is the square root of some element $\alpha \in F$. Namely, δ is a root of $x^2 - \alpha = 0$, so

$$F[\delta] \;\cong\; F[x] \,/\, (x^2 - \alpha).$$

   This implies the quadratic formula: if we select $\alpha \in K \setminus F$, then $(1, \alpha)$ is a basis of K. Hence the minimal polynomial of α has a root with the same form as the quadratic formula.

This leads us to the following theorem:

Theorem 17. *Let $L \,/\, K \,/\, F$ be a chain of field extensions with finite degree.. Then*

$$[L : F] \;=\; [L : K][K : F].$$

Proof. The proof is simple: let $l_1, \dots, l_n \in L$ be a basis over K, and let $k_1, \dots, k_m \in K$ be a basis over F. The claim is that the products $l_i k_j$ is a basis of L over F.

1. **Spanning**: For all $l \in l$, there exist $z_1, \dots, z_m \in K$ such that

$$l \;=\; l_1 z_1 + \cdots + l_n z_n.$$

   Similarly, each $z_i \in K$ is expressible for $f_{i1}, \dots, f_{im} \in F$ as

$$z_i = f_{i1} k_1 + \cdots + f_{im} k_m.$$

   Superimposing these two by substitution expresses l as a linear combination of terms of the form $l_i l_j$ multiplied by scalars in F.

2. **Independent**: If we suppose that there exist constants l_{ij} such that

$$\sum_{i=1}^{n} \sum_{j=1}^{m} f_{ij} l_i k_j.$$

   We can factor this and determine that because k are independent, the scalars f_{ij} must be zero.

This completes the proof. □

It is clear that if α has degree n, then $[F(\alpha) : F] = n$. If we would like to adjoin another element β of degree m, we have

$$[F(\alpha, \beta) : F] \;=\; [F(\alpha, \beta) : F(\alpha)][F(\alpha), F] \;=\; mn.$$

An important corollary is as follows:

Corollary 5 (Artin 13.3.6)**.** *The following two results hold:*

1. *Let $K\,/\,F$ be a finite field extension and let $\alpha \in K$ be algebraic. If $\deg \alpha = [K : F]$, then*
$$F[\alpha] \;=\; F(\alpha) \;=\; F.$$
2. *Let $L\,/\,K\,/\,F$ be a chain of field extensions, not necessarily finite. If $\alpha \in L$ is algebraic over F, then α over K too; we have $\deg_K \alpha \leq \deg_L \alpha$.*
3. *Let $K\,/\,F$ be a field extension. If $\alpha_1, \ldots, \alpha_n \in K$ are algebraic, then $F(\alpha_1, \ldots, \alpha_n)$ is a finite extension of F.*

Proof. $F[\alpha]$ and K are both F-vector spaces of dimension $[K : F]$, so they are isomorphic. They are equal since $F[\alpha] \subseteq K$ is a subspace of the same finite dimension. (2) is also quite clear. □

11.2 Ruler and Compass Construction

We are ready to answer the problem of ruler and compass construction. The key is to classify the types of permitted actions with these tools:

1. Construct the line through two points
2. Construct the circle that contains one point and has a center at another point
3. Mark the intersection point of two (non-parallel) lines
4. Mark the intersection point(s) of a line and a circle (if they intersect)
5. Mark the intersection point(s) two circles (if they intersect).

By repeating these actions, we generate systems of equations that will adjoin elements of degree 1 or 2. Hence the resulting field generated will have a degree that is a power of two. Hence it is not possible to double the cube, since this entails adjoining $\sqrt[3]{2}$ to $\mathbb{Z}$, an element with degree 3. It is also not possible to square the circle, since π is transcendental.

Theorem 18. *Suppose $(x, y) \in \mathbb{R}^2$ can be constructed. Then $[\mathbb{Q}(a_1, a_2) : \mathbb{Q}]$ is a power of two.*

Proof. Since (x, y) is constructible in a finite number of moves, it suffices to show that performing any of the five moves multiplies the degree of the field extension by 1 or 2. This may be calculated by using coordinates; each equation has at most degree 2. □

It is also not possible to construct polygons of arbitrary side length: for instance, the points of the 7-gon are the roots of the roots of unity

$$z^7 = 1 \implies (z-1)(z^6 + z^5 + \cdots + 1).$$

Clearly the right-hand side is irreducible; thus adjoining such an element would entail a field extension that is a multiple of 6. This is not possible; hence this polygon is not constructible.

Theorem 19. *If $(x_1, x_2) \in \mathbb{R}^2$ are such that $[\mathbb{Q}(x_1, x_2) : \mathbb{Q}]$ is a power of two, then (x_1, x_2) is a constructible point.*

Proof. □