

RINGS AND FIELDS

AMIN WITNO

Preface

Written at Philadelphia University, Jordan for Math 442, these notes¹ were used first time in the Spring 2007 semester. They have since been revised² and shall be revised again as often as the author teaches the course. Outline notes are more like a revision. No student is expected to fully benefit from these notes unless they have regularly attended the lectures.

1 Introduction

Definition. Let R be a set together with two binary operations, referred to as *addition* (+) and *multiplication* (\times). Then R is a *ring* if it has the following properties.

- 1) R is an abelian group under addition.
- 2) Multiplication in R is *associative*, meaning that $a \times (b \times c) = (a \times b) \times c$ for every $a, b, c \in R$.
- 3) *Distributive laws* hold in R , meaning that $a \times (b + c) = (a \times b) + (a \times c)$ and $(a + b) \times c = (a \times c) + (b \times c)$ for every $a, b, c \in R$.

Note that the first property is composed of the following four.

- 1) Addition in R is commutative: $a + b = b + a$ for every $a, b \in R$.
- 2) Addition in R is associative: $a + (b + c) = (a + b) + c$ for every $a, b, c \in R$.
- 3) There exists a unique identity element in R under addition—the *zero element*, written 0, such that $a + 0 = a$ for every $a \in R$.
- 4) For each $a \in R$ there exists a unique inverse element—the *negative* of a , written $-a$, such that $a + (-a) = 0$.

Example. Let us illustrate this idea with a few examples.

¹Copyrighted under a Creative Commons License

²Last Revision: 15-02-2009

- 1) The set \mathbb{Z} of integers under ordinary addition and multiplication is a ring. The zero element is given by the integer 0 and the negative of $a \in \mathbb{Z}$ is the integer $-a$.
- 2) Similarly the sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ of rational numbers, real numbers, and complex numbers, respectively are rings under ordinary addition and multiplication.
- 3) The subset of even numbers is a ring on its own. More generally the set of multiples of n , that is, $\langle n \rangle = \{nk \mid k \in \mathbb{Z}\}$ is a ring under ordinary addition and multiplication.
- 4) The set \mathbb{Z}_n of modular integers under addition and multiplication mod n is a ring. The zero element is $0 = [0]_n$ and the negative of $[a]_n$ is given by $-[a]_n = [-a]_n$.
- 5) The set $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is a ring under ordinary addition and multiplication.
- 6) The set $M(2, \mathbb{R})$ of 2×2 matrices with real entries is a ring under matrix addition and matrix multiplication. Similar statement holds with \mathbb{R} replaced by \mathbb{Z}, \mathbb{Q} , or \mathbb{C} as well.

Remark. From now on we write ab instead of $a \times b$. Moreover associativity implies that the sum $a + b + c$ and the product abc may be written without requiring brackets. This can be generalized to any finite number of elements, such as $a_1 a_2 \cdots a_k$.

Definition. Unlike addition, multiplication is not assumed commutative in a ring. However, if it is then the ring R is called *commutative*. Moreover if there exists an identity element under multiplication then it is called *unity*, written 1. Hence, a unity in R is an element $1 \in R$ satisfying $a1 = 1a = a$ for every $a \in R$.

Note that all the examples given above are commutative rings with unity, except the last one is not commutative since matrix multiplication is generally not.

Proposition 1.1. Let R be a ring. For every $a, b, c \in R$,

- 1) $0a = a0 = 0$
- 2) $a(-b) = -(ab) = (-a)b$
- 3) $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$
- 4) if exists, $(-1)a = -a$.

Proof. Using the definition of zero and the distributive law, $a0 = a(0 + 0) = a0 + a0$. Adding $-(a0)$ to both sides produces $0 = a0$. Similarly we show $0a = 0$ to establish (1). The rest of the proof is left as an exercise. ∇

Theorem 1.2. If R and S are two rings, with their respective additions and multiplications, then the set $R \times S = \{(r, s) \mid r \in R \text{ and } s \in S\}$ is also a ring under the usual componentwise operations. The name for this ring is the *direct product* of R and S .

Proof. An exercise. ∇

Definition. A subset S of a ring R is a *subring* if S is itself a ring with respect to the same addition and multiplication of R .

For example we have the sequence of subrings given by $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Also, the even numbers form a subring of \mathbb{Z} . Because a subring is necessarily a subgroup with respect to addition, from group theory we know that all subrings of \mathbb{Z} must come in the form $\langle n \rangle$. The next theorem can be used to show that for each $n \in \mathbb{Z}$, the subgroup $\langle n \rangle$ is indeed a subring of \mathbb{Z} .

Theorem 1.3. Let R be a ring. A subset S is a subring if and only if S is a subgroup of R under addition and is closed under multiplication. (Being closed under multiplication means that $ab \in S$ whenever $a, b \in S$.)

Proof. An exercise. ▽

Exercise 1

- 1) Let R be the collection of all subsets of an arbitrary set. Define $A + B = A \cup B$ and $A \times B = A \cap B$ for all $A, B \in R$. Is R a ring? Prove true or false.
- 2) Show that the set $\left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R} \right\}$ is a subring of $M(2, \mathbb{R})$. What about the set $\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R} \right\}$? $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$? $\left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \mid a, c \in \mathbb{R} \right\}$?
- 3) Prove that the intersection of two subrings of R is again a subring of R .
- 4) Define the *center* of a ring R by $Z(R) = \{x \in R \mid ax = xa \text{ for all } a \in R\}$.
 - a) Show that $Z(R)$ is a subring of R .
 - b) What is $Z(\mathbb{Z})$?
 - c) When is $Z(R) = R$?
 - d) Find $Z(M(2, \mathbb{Q}))$.

2 Integral Domains

Definition. Let a and b be two nonzero elements in a ring R . If $ab = 0$ then each of a, b is called a *zero divisor* of R .

Example. There are zero divisors in $M(2, \mathbb{R})$, such as $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$. You may check that AB is the zero matrix. Another example, in \mathbb{Z}_6 we have $3 \times 4 \equiv 0 \pmod{6}$, hence 3 and 4 are zero divisors there.

Lemma 2.1. A nonzero element $m \in \mathbb{Z}_n$ is a zero divisor if and only if m and n are not relatively prime.

Proof. Suppose m, n have a common divisor $d > 1$. Then $m(n/d) \equiv 0 \pmod{n}$ where $1 \leq n/d < n$ is a nonzero element. Hence m is a zero divisor. Conversely if m, n are relatively prime, the relation $mb \equiv 0 \pmod{n}$ implies, by Euclid's lemma, that $b \equiv 0 \pmod{n}$. Hence m is not a zero divisor. ▽

Remark. Equivalently, $m \in \mathbb{Z}_n$ is neither zero nor a zero divisor if and only if $m \in U_n$. Hence, the zero divisors of \mathbb{Z}_n are precisely nonzero elements of the set $\mathbb{Z}_n - U_n$.

Definition. A ring R is an *integral domain* if it is a commutative ring with unity but without zero divisors. For examples $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all integral domains.

Theorem 2.2. The ring \mathbb{Z}_n is an integral domain if and only if n is prime.

Proof. This follows from the lemma since a number n is prime if and only if it is relatively prime to $1, 2, \dots, n - 1$. ∇

Proposition 2.3. Let a be a nonzero element in an integral domain R . For any $b, c \in R$, if $ab = ac$ then $b = c$. Similarly $ba = ca$ implies $b = c$.

Proof. Since $0 = ab - ac = a(b - c)$ and there is no zero divisor, then $b - c = 0$ and $b = c$. ∇

We say that the *cancellation laws*—right and left, since commutative—hold in an integral domain. In other rings they may not hold, for example, in \mathbb{Z}_6 we have $2 \times 1 \equiv 2 \times 4 \pmod{6}$ but cancelling the 2 results in $1 \equiv 4 \pmod{6}$, which is false.

Definition. Let R be a commutative ring with unity. If $ab = 1$ in R then each of a, b is called a *unit* element. Hence, unit elements are those with a multiplicative inverse. We denote the inverse of a under multiplication by a^{-1} , and reserve the word *inverse* for mutiplication, since under addition we have agreed to use the word *negative*.

Example. The units of \mathbb{Z}_n form the subset U_n . (Recall, U is for *units*.) In particular, we will see that zero divisors and units are mutually exclusive properties.

Theorem 2.4. Let R be a commutative ring with unity.

- 1) No zero divisor is a unit.
- 2) No unit is a zero divisor.
- 3) If $a \in R$ is a unit then $ab = ac$ implies $b = c$.
- 4) The units of R form a group under multiplication.

Proof. The proof is omitted as a healthy exercise. ∇

Definition. A ring R is a *field* if it is a commutative ring with unity in which every nonzero element is a unit. In other words, the nonzero elements of a field form an abelian group under multiplication.

Example. The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields. But \mathbb{Z} is not a field since no integer can have a multiplicative inverse except ± 1 .

Theorem 2.5. A field is an integral domain.

Proof. Let F be a field and $a \in F$, nonzero. It suffices to show that a is not a zero divisor, which is not since a is a unit. ∇

Theorem 2.6. A finite integral domain is a field.

Proof. Let $R = \{a_1, a_2, \dots, a_n\}$ be an integral domain and choose $a \in R$, nonzero. It suffices to show that $ab = 1$ for some $b \in R$. The elements aa_1, aa_2, \dots, aa_n are all distinct since $aa_j = aa_k$ implies $a_j = a_k$ by the cancellation law, hence they make up all the elements of R . In particular one of them is $aa_i = 1$. ∇

Corollary 2.7. Let p denote a prime number. The ring \mathbb{Z}_p is a field.

Proof. \mathbb{Z}_p is finite and is an integral domain by Theorem 2.2. ∇

Remark. Alternatively, we can see that \mathbb{Z}_p is a field because its nonzero elements make up the abelian group U_p under multiplication mod p . The converse of the corollary is true as well: \mathbb{Z}_n is not a field if n is not prime, since it would not even be an integral domain, by Theorem 2.2.

Definition. Let F be a field. A subset $S \subseteq F$ is a *subfield* if S is itself a field with respect to the addition and multiplication associated with F .

Theorem 2.8. A subset S of a field F is a subfield if and only if S is a subgroup of F under addition and S^* is a subgroup of F^* under multiplication.

Proof. This is a result from group theory. ▽

Remark. The notation F^* means the set of nonzero elements of F , and similarly for S^* . The theorem in particular implies that the zero and unity of the subfield S are the same as those of F , respectively.

Exercise 2

- 1) Prove that the direct product of two integral domains is never an integral domain.
- 2) Assuming the cancellation laws, show that a ring can have no zero divisors.
- 3) Find all the zero divisors and units in each ring \mathbb{Z}_{10} , \mathbb{Z}_{24} , $\mathbb{Q} \times \mathbb{Q}$, and $M(2, \mathbb{R})$.
- 4) Prove that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a subfield of \mathbb{R} .

3 Ideals

Definition. A subset I of a ring R is an *ideal* if I is a subgroup under addition such that if $a \in I$ and $r \in R$ then $ar, ra \in I$.

By Theorem 1.3 an ideal is a subring, but it is more than just a subring. (It is the analogue of a normal subgroup for a ring, in the sense that it is the kernel of a homomorphism.) For example the subring $\langle n \rangle$ of \mathbb{Z} is an ideal, since if a is a multiple of n then ar is still a multiple of n for any $r \in \mathbb{Z}$.

Definition. Let R be a commutative ring with unity. For every $a \in R$ define the set $(a) = \{ra \mid r \in R\}$. The next theorem demonstrates that (a) is an ideal of R , called the *principal ideal generated by a* . More generally, an ideal is *principal* if it is given by (a) , for some $a \in R$. (A principal ideal is comparable to a cyclic subgroup, where it is generated by one element.)

Theorem 3.1. Let R be a commutative ring with unity. For every $a \in R$, the set $(a) = \{ra \mid r \in R\}$ is an ideal.

Proof. If $r, s \in R$, the fact that $ra - sa = (r - s)a$ shows that (a) is a subgroup under addition. Moreover, given $ra \in (a)$ and $s \in R$, we have $s(ra) = (sr)a \in (a)$. ▽

Remark. Note that the ideal $\langle n \rangle$ of \mathbb{Z} is really the principal ideal (n) . For this reason, we loosely refer to the elements of (a) as *multiples* of a in R .

Recall that every subgroup of a cyclic group is cyclic; The next definition is the ring analogue of this property, which is still true for \mathbb{Z} .

Definition. A ring R is a *principal ideal domain* if R is an integral domain in which every ideal is principal.

Theorem 3.2. The ring \mathbb{Z} is a principal ideal domain.

Proof. It is an integral domain whose only ideals are (n) for any element $n \in \mathbb{Z}$. ∇

Theorem 3.3. Let F be a field. The only ideals of F are $\{0\}$ and F itself. Conversely let R be a commutative ring with unity and no ideals other than $\{0\}$ and itself. Then R is a field.

Proof. Let I be an ideal of F . Suppose there is $a \in I$, nonzero. Since $a^{-1} \in F$, an ideal means $a^{-1}a = 1 \in I$. Then $1r = r \in I$ for all $r \in F$. Hence $I = F$. Conversely, let $a \in R$, nonzero. Then $(a) = R$ by assumption. In particular, $ra = 1$ for some $r = a^{-1} \in R$. Hence R is a field. ∇

Remark. As a result, although trivial, we see that all fields are principal ideal domains since their only ideals are (0) and (1) .

Exercise 3

1) If I and J are two ideals of a ring R , so are the following sets. Prove all.

- a) $\{r \in R \mid ra = 0 \text{ for all } a \in I\}$
- b) $I \cap J$
- c) $I + J = \{i + j \mid i \in I \text{ and } j \in J\}$
- d) $IJ = \{\sum ij \mid i \in I \text{ and } j \in J\}$

- 2) Prove that if an ideal contains a unit element then it contains the whole ring.
- 3) Show that the center of $M(2, \mathbb{R})$ is not an ideal.
- 4) Let R be a commutative ring. An ideal $I \neq R$ is called *prime* when, for all $a, b \in R$, if $ab \in I$ then either $a \in I$ or $b \in I$. Prove that the ideal (n) of \mathbb{Z} is prime if and only if the integer n is prime.

4 Factor Rings

Let I be a subring of a ring R . Since R is an abelian group, under addition, then I is a normal subgroup of R . Hence we have the factor group of cosets, $R/I = \{I+r \mid r \in R\}$, in which $(I+r) + (I+s) = I + (r+s)$. We now wish to make R/I a ring by introducing the multiplication $(I+r)(I+s) = I + (rs)$. This will work, however, only if I is an ideal.

Lemma 4.1. Let I be an ideal of a ring R . For every elements $I+r$ and $I+s$ in the factor group R/I , the multiplication $(I+r)(I+s) = I + (rs)$ is well defined.

Proof. Suppose that $I+r = I+r'$ and $I+s = I+s'$, hence $r-r' \in I$ and $s-s' \in I$. It follows that the multiples $rs - r's$ and $r's - r's'$ belong to I as well. Then $rs - r's' \in I$, and so $I + (rs) = I + (r's')$. ∇

Theorem 4.2. Let I be an ideal of a ring R . The factor group R/I is a ring.

Proof. It is left to show associativity and the distributive laws. These are trivial as these properties are simply inherited from those of R . ∇

Definition. Let I be an ideal of R . The ring R/I is called the *factor ring* or *quotient ring* of R mod I .

Example. We have the old example of \mathbb{Z} and the ideal (n) . The factor group $\mathbb{Z}/(n) \approx \mathbb{Z}_n$ is now a ring with multiplication mod n , but we already know that.

Exercise 4

- 1) Show that if R has a unity then $I + 1$ is the unity in the factor ring R/I .
- 2) Prove that the factor ring R/I is commutative if and only if $ab - ba \in I$ for all $a, b \in R$.
- 3) Let R be a principal ideal domain. Show that every ideal of the factor ring R/I is principal. Does this make R/I a principal ideal domain?
- 4) Let R be a commutative ring with unity and an ideal $I \neq R$. Prove that I is a prime ideal if and only if R/I is an integral domain.

5 Ring Homomorphisms

Definition. Let R and R' be two rings each with their own addition and multiplication. A function $\theta : R \rightarrow R'$ is called a (ring) *homomorphism* if for every $a, b \in R$,

- 1) $\theta(a + b) = \theta(a) + \theta(b)$
- 2) $\theta(ab) = \theta(a)\theta(b)$

We also define the *range* $\theta(R) = \{\theta(a) \mid a \in R\}$ and the *kernel* $\ker(\theta) = \{a \in R \mid \theta(a) = 0\}$. Both the zero elements for R and R' are denoted by 0, but they should be distinguishable in the context.

Example. Let $\theta : \mathbb{Z} \rightarrow \mathbb{Z}_n$ be given by $\theta(a) = [a]_n$. This is the familiar group homomorphism, under addition, where $\ker(\theta) = (n)$ and $\theta(\mathbb{Z}) = \mathbb{Z}_n$. Now since $[ab]_n = [a]_n[b]_n$, we have θ a ring homomorphism as well.

Example. Let $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ and $\theta : R \rightarrow R$, where $\theta(a + b\sqrt{2}) = a - b\sqrt{2}$. It is not hard to show that θ is a homomorphism, and that $\theta(R) = R$ and $\ker(\theta) = \{0\}$.

Proposition 5.1. Let $\theta : R \rightarrow R'$ be a ring homomorphism.

- 1) $\theta(0) = 0$ and $\theta(-a) = -\theta(a)$ for every $a \in R$.
- 2) θ is one-to-one if and only if $\ker(\theta) = \{0\}$.
- 3) $\theta(R)$ is a subring of R' .
- 4) $\ker(\theta)$ is an ideal of R .

Proof. An exercise. ▽

Definition. A ring homomorphism $\theta : R \rightarrow R'$ is called an *isomorphism* if it is one-to-one and onto, in which case we say that R and R' are *isomorphic*, written $R \approx R'$.

Like the isomorphism between two groups, a ring isomorphism preserves the structure of the one ring onto the other, with respect to both addition and multiplication. Hence two isomorphic rings are essentially the same ring except for the different labelling of the elements. In particular if $R \approx R'$, then R is an integral domain, or a field, if and only if R' is an integral domain or a field, respectively.

Theorem 5.2 (The Fundamental Homomorphism Theorem for Rings). Suppose that $\theta : R \rightarrow R'$ is a homomorphism of rings. Then $R/\ker(\theta) \approx \theta(R)$.

Proof. Let $I = \ker(\theta)$ and $\Theta(I+r) = \theta(r)$. We have seen that $\Theta : R/I \rightarrow \theta(R)$ is a group isomorphism under addition. It is left to show that Θ preserves multiplication: $\Theta((I+r)(I+s)) = \Theta(I+(rs)) = \theta(rs) = \theta(r)\theta(s) = \Theta(I+r)\Theta(I+s)$. ∇

Example. From the previous example we have $\mathbb{Z}/(n) \approx \mathbb{Z}_n$, as rings.

Theorem 5.3 (Chinese Remainder Theorem for Rings). Suppose that $m, n \in \mathbb{Z}$ are relatively prime. Then $\mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn}$ (as rings).

Proof. Recall the homomorphism $\theta : \mathbb{Z} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$, as additive groups, given by $\theta(a) = ([a]_m, [a]_n)$. This map is onto and $\ker(\theta) = (mn)$. The fundamental theorem gives the result, since $\theta(ab) = \theta(a)\theta(b)$, showing that it is a ring homomorphism. ∇

Exercise 5

- 1) Let $\theta : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_4$ be given by $\theta([a]_{12}) = [a]_4$.
 - a) Show that θ is a well-defined homomorphism.
 - b) Find $\ker(\theta)$. Is θ one-to-one? Onto?
 - c) Describe the factor ring $\mathbb{Z}_{12}/\ker(\theta)$. What is this isomorphic to?
 - d) Construct the Cayley tables (addition and multiplication) for this factor ring.
- 2) Let $\theta : R \rightarrow R'$ be a ring homomorphism. If R is a field, show that θ is one-to-one or otherwise $\theta(R) = \{0\}$.
- 3) Let θ be a ring homomorphism which is onto. Prove that, if exists, $\theta(1) = 1$. Give a counterexample where θ is not onto.
- 4) Prove that the set $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ is a subring of $M(2, \mathbb{R})$ which is a field isomorphic to \mathbb{C} .

6 Polynomial Rings

Definition. Let $R[x] = \{a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n \mid a_i \in R\}$, where R is a commutative ring. Every element $f = f(x) \in R[x]$ is a *polynomial* with coefficients in R . For each polynomial f we define its *degree*, written $\deg f$, to be the largest integer k for which $a_k \neq 0$. The *zero polynomial*, $f = 0$, does not have a degree. Note that $\deg f = 0$ if and only if $f \in R$, in which case f is a *constant*.

We define addition and multiplication of polynomials the usual way. If $f = \sum a_i x^i$ and $g = \sum b_i x^i$ then

$$f + g = \sum_{i=0}^M (a_i + b_i) x^i$$

$$fg = \sum_{i=0}^N c_i x^i \quad \text{where} \quad c_k = \sum_{i=0}^k a_i b_{k-i}$$

and where $M = \max\{\deg f, \deg g\}$ and $N = \deg f + \deg g$.

Theorem 6.1. If R is a commutative ring then so is the set $R[x]$ under polynomial addition and multiplication. Its zero is the zero polynomial $f = 0$ and for each polynomial $f = \sum a_i x^i$, its negative is given by $-f = \sum (-a_i) x^i$.

Proof. A straightforward exercise. ▽

Proposition 6.2. If R is an integral domain then $\deg(fg) = \deg f + \deg g$ for every polynomials $f, g \in R[x]$.

Proof. Let $\deg f = n$ and $\deg g = m$. By definition of multiplication it is clear that $\deg(fg) \leq m + n$ with $c_{m+n} = a_n b_m$. Since $a_n, b_m \neq 0$ and R has no zero divisors, then $c_{m+n} \neq 0$. Hence $\deg(fg) = m + n$. ▽

Corollary 6.3. With R integral domain, $\deg(fg) \geq \deg f$ for all $f, g \in R[x]$.

Proof. This follows since the degree of any polynomial is a non-negative number. ▽

Proposition 6.4. If R is an integral domain, so is $R[x]$.

Proof. $R[x]$ is commutative with unity $f = 1$, the unity of R . And if f, g are nonzero polynomials then $fg \neq 0$ because, for one thing, it has a degree by Proposition 6.2. ▽

Exercise 6

- 1) Let R be an integral domain. Show why $R[x]$ is never a field.
- 2) Given two commutative rings, $R \approx S$, prove that $R[x] \approx S[x]$.
- 3) Show that the constants in $R[x]$ form a subring which is not an ideal.
- 4) Prove that $\{\sum a_i x^i \in \mathbb{Z}[x] \mid a_0 \text{ is even}\}$ is an ideal of $\mathbb{Z}[x]$ which is not principal. Hence, $\mathbb{Z}[x]$ is not a principal ideal domain.

7 Polynomials Over A Field

We consider polynomials whose coefficients lie in a field F . The integral domain $F[x]$ shares many arithmetical properties enjoyed by the ring \mathbb{Z} of integers.

Definition. Let $f, g \in F[x]$. We say that f divides g if $g = hf$ for some $h \in F[x]$. In this case we write $f \mid g$ and say that g is divisible by f , or that g is a multiple of f . Also, f is called a divisor or factor of g .

Example. Over the field \mathbb{Q} , the polynomial $2x + 1$ divides $2x^3 - 4x^2 + 7x + 5$ because $(2x + 1)(x^2 - 3x + 5) = 2x^3 - 4x^2 + 7x + 5$.

Proposition 7.1. In $F[x]$ the following statements hold.

- 1) The polynomial $f = 1$ divides all other polynomials.
- 2) If $f \mid g \neq 0$ then $\deg f \leq \deg g$.
- 3) If $f \mid g$ and $g \mid h$ then $f \mid h$.
- 4) If $f \mid g$ and $f \mid h$ then $f \mid ag + bh$ for all $a, b \in F[x]$.

Proof. An exercise. ▽

Corollary 7.2. If $f \mid g$ and $g \mid f$ then $g = af$ for some $a \in F$.

Proof. We have $\deg f \leq \deg g \leq \deg f$ hence both degrees are equal. It follows that $g = hf$ with $\deg h = 0$, that is, h is a constant. ∇

Theorem 7.3 (The Division Algorithm in $F[x]$). Let f and g be two nonzero polynomials over a field F . Then there exist unique polynomials $q, r \in F[x]$ such that $g = qf + r$, where either $r = 0$ or $\deg r < \deg f$.

Proof. If $g = 0$ then let $q = r = 0$. If $\deg g < \deg f$ then we let $q = 0$ and $r = g$. Suppose now $m = \deg g \geq \deg f = n$. By way of induction we assume the theorem is true for all g of degree less than m . Let $g' = g - cf x^{m-n}$ where $c = a_m(a_n)^{-1}$. Then either $g' = 0$ or else $\deg g' < \deg g$. By induction hypothesis, we have $g' = q'f + r$ where $r = 0$ or $\deg r < \deg f$. It follows that $g = qf + r$ with $q = q'cx^{m-n}$.

To prove uniqueness, suppose that $g = qf + r = Qf + R$ where also $R = 0$ or $\deg R < \deg f$. Then $(q - Q)f = R - r$. If $R - r \neq 0$ then $\deg(R - r) < \deg f$, whereas $\deg((q - Q)f) \geq \deg f$ by Corollary 6.3. To avoid contradiction we must have $R = r$ and $(q - Q)f = 0$, which, since $F[x]$ has no zero divisors, implies $q = Q$. ∇

Definition. The polynomials q and r in the theorem are referred to as the *quotient* and *remainder*, respectively, upon dividing g by f . Also, if $a \in F$, the notation $f(a)$ means the element in F obtained by substituting x by a in the expression $f(x) = \sum a_i x^i$.

Corollary 7.4 (Remainder Theorem). Let $a \in F$ and $g \in F[x]$. The remainder when g is divided by $x - a$ is $g(a)$. In particular $x - a \mid g$ if and only if $g(a) = 0$.

Proof. Divide g by $x - a$, and $g(x) = q(x - a) + r$. Then $g(a) = r$, the remainder. ∇

Theorem 7.5. The ring $F[x]$ is a principal ideal domain.

Proof. Let I be an ideal of $F[x]$ and let f be a polynomial of least degree in I . By the division algorithm, for each $g \in I$ there are $q, r \in F[x]$ such that $g = qf + r$ with either $r = 0$ or $\deg r < \deg f$. But since I is an ideal, $r = g - qf \in I$, so $\deg r < \deg f$ is not possible. Hence $r = 0$ and $g \in (f)$. We have proved that $I = (f)$. ∇

Lemma 7.6. Let $f, g \in F[x]$. The set $\{af + bg \mid a, b \in F[x]\}$ is an ideal of $F[x]$.

Proof. This set is the ideal $(f) + (g)$ of Exercise 3.1. ∇

Definition. Let $f, g \in F[x]$. A *greatest common divisor* of f and g is a polynomial $d \in F[x]$ such that $(d) = \{af + bg \mid a, b \in F[x]\}$.

Proposition 7.7. Let d be a greatest common divisor of f and g in $F[x]$. Then

- 1) $d \mid f$ and $d \mid g$
- 2) $d = af + bg$ for some $a, b \in F[x]$
- 3) if $c \mid f$ and $c \mid g$ then $c \mid d$
- 4) if c is another greatest common divisor of f and g then $c = ad$ for some $a \in F$.

Proof. An exercise. ∇

Definition. If $f = \sum a_i x^i \in F[x]$ has degree n , we call a_n the *leading coefficient* of f . A polynomial $f \in F[x]$ is *monic* when its leading coefficient is the unity of F . Given $f, g \in F[x]$ we define $\gcd(f, g) = d$, where d is the monic greatest common divisor of f and g . Such d is unique, for if c is another then $c = ad$ for some constant a . But both leading coefficients are 1, hence $a = 1$.

Example. Let us find $\gcd(x^{81} - 1, x^{24} - 1)$ in $\mathbb{Q}[x]$. The Euclidean algorithm for \mathbb{Z} works in the same way for $\mathbb{Q}[x]$. (Why?)

$$\begin{aligned} (x^{81} - 1) - (x^{24} - 1)(x^{57} + x^{33} + x^9) &= x^9 - 1 \\ (x^{24} - 1) - (x^9 - 1)(x^{15} + x^6) &= x^6 - 1 \\ (x^9 - 1) - (x^6 - 1)(x^3) &= x^3 - 1 \\ (x^6 - 1) - (x^3 - 1)(x^3 + 1) &= 0 \end{aligned}$$

The result, $\gcd(x^{81} - 1, x^{24} - 1) = x^3 - 1$ since it is already monic.

Definition. A polynomial $f \in F[x]$ is *reducible* if f is divisible by another polynomial g with $0 < \deg(g) < \deg(f)$. An *irreducible* polynomial means it is not reducible.

Theorem 7.8. If $f \mid gh$ and f is irreducible then $f \mid g$ or $f \mid h$.

Proof. Let $d \mid f$. If $\deg d > 0$ then $\deg d = \deg f$, and $d = af$ for some $a \in F$. If $d \mid g$ as well then $f \mid g$. Hence, if $f \nmid g$ then d is a constant, in which case $\gcd(f, g) = 1$. We then write $1 = af + bg$. Multiply by h to get $h = afh + bgh$. Since f divides the right hand side then $f \mid h$. ▽

Theorem 7.9 (Unique Factorization in $F[x]$). Every nonconstant polynomial in $F[x]$ is a product of a unique collection of irreducible polynomials.

Proof. First we prove that every polynomial is a product of irreducibles. If $\deg f = 1$ then it is irreducible. By way of induction, assume the claim is true up to $\deg < n$ and let $\deg f = n$. If f is reducible then we write $f = gh$ with both degrees $< n$. By assumption both g, h are products of irreducibles, and so is f .

Next we prove uniqueness. Assume that $f = g_1 \cdots g_j = h_1 \cdots h_k$, each irreducible. Cancel out all common terms and constant multiples, so we have equality between products of g 's and h 's, all distinct. But by Theorem 7.8 g_1 divides one of the h 's, so each is a constant multiple of the other, a contradiction. ▽

Theorem 7.10. The factor ring $F[x]/(f)$ is a field if and only if $f \in F[x]$ is irreducible.

Proof. Let $R = F[x]/(f)$. The element $(f) + g \in R$ is nonzero if and only if $f \nmid g$. If f is reducible then $f = gh$, where f divides neither g nor h . In R we then have nonzero elements whose product $((f) + g)((f) + h) = (f) + f = 0$. This shows that R is not an integral domain, nor a field.

Conversely if f is irreducible and $f \nmid g$ then $\gcd(f, g) = 1$. By Proposition 7.7 there exist $a, b \in F[x]$ such that $af + bg = 1$. Then $((f) + b)((f) + g) = (f) + 1 - af = (f) + 1$, the unity in R . This shows that $(f) + g$ is a unit in R , hence R is a field. ▽

Example. Consider $f(x) = x^2 + 1 \in \mathbb{R}[x]$. It is irreducible since it has no real root, hence $\mathbb{R}[x]/(x^2 + 1)$ is a field. What are its elements? Using division algorithm every $g \in \mathbb{R}[x]$ can be written $g = q(x^2 + 1) + r$ with $r = 0$ or $\deg r \leq 1$. Hence $\mathbb{R}[x]/(x^2 + 1) = \{(x^2 + 1) + a + bx \mid a, b \in \mathbb{R}\}$. But $x^2 + 1 = 0$ in the factor ring, so that $x^2 = -1$. We can show that in turn $\mathbb{R}[x]/(x^2 + 1) \approx \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\} = \mathbb{C}$.

Exercise 7

- 1) If $\deg f = n$ in $F[x]$ show that f can have at most n distinct zeros in F .
- 2) Suppose that F is a field of n elements. Prove that $x^n - x = \prod_{a \in F} (x - a)$ in $F[x]$.
- 3) Let $f \in F[x]$ be a polynomial with $\deg f \leq 3$.
 - a) Prove that f is reducible if and only if it has a zero in F .
 - b) Give a counterexample for (a) when $\deg f \geq 4$.
 - c) Determine if $f(x) = x^2 + 1$ is irreducible over the field $\mathbb{Q}, \mathbb{Z}_7, \mathbb{Z}_{11}, \mathbb{Z}_{13}$.
 - d) Repeat (c) with $f(x) = x^2 - 2$.
- 4) Describe the factor ring $\mathbb{Q}[x]/(x^2 - 2)$. What familiar ring is this?

8 Field Extensions

Definition. When we have a field K and a subfield F , we say that K is an *extension field* over F .

Lemma 8.1. Let K be an extension field over F and $a \in K$. The set $\{f \in F[x] \mid f(a) = 0\}$ is an ideal of $F[x]$.

Proof. Exercise. ∇

Definition. Since $F[x]$ is a principal ideal domain, the ideal given by the lemma is in the form (f) for some $f \in F[x]$. If $f \neq 0$ then $a \in K$ is an *algebraic* element over F . In that case there is a unique choice for f which is monic and it is called the *minimal polynomial* of a over F .

Theorem 8.2. Let $a \in K$ be algebraic over F . Then $f \in F[x]$ is the minimal polynomial of a over F if and only if f is monic, irreducible, and $f(a) = 0$. Moreover with such f , if $g(a) = 0$ for any $g \in F[x]$ then $f \mid g$ and in particular $\deg f \leq \deg g$.

Proof. Let f be the minimal polynomial. If $g(a) = 0$ then $g \in (f)$ and $f \mid g$. And if $f = gh$ then either $g(a) = 0$ or $h(a) = 0$, hence one of g, h has degree $\deg f$, meaning that f is irreducible. Conversely, if f' is irreducible and $f'(a) = 0$ then $f \mid f'$, which implies that f' is a constant multiple of f . If f' is also monic then $f' = f$. ∇

Definition. Let $a \in K$ be an algebraic element over F with minimal polynomial f . Then $\deg f$ is referred to as the *degree* of a over F .

Example. Both $\sqrt{2} \in \mathbb{R}$ and $i \in \mathbb{C}$ are algebraic elements over \mathbb{Q} of degree 2. Their minimal polynomials are $x^2 - 2$ and $x^2 + 1$, respectively.

Definition. Let $F \subseteq K$ be a field extension. Recall that the intersection of two subfields is again a subfield. Now for any subset $S \subseteq K$, we define $F(S)$ to be the intersection of all subfields of K which contain both F and S . Hence $F(S)$ is the smallest extension field over F which contains S and is contained in K . In particular, when $S = \{a_1, \dots, a_k\}$ then we may write $F(a_1, \dots, a_k)$ instead of $F(S)$.

Example. Consider $\mathbb{Q}(\sqrt{2})$. Being a field, $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. The latter we know is a field, hence $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$.

Theorem 8.3. Let $a \in K$ be an algebraic element over F with minimal polynomial $f \in F[x]$. Then $F(a) \approx F[x]/(f)$.

Proof. The idea is to define the homomorphism $\theta : F[x] \rightarrow F(a)$ by $\theta(g(x)) = g(a)$ and show that $\ker(\theta) = (f)$, then apply the fundamental homomorphism theorem. ∇

Corollary 8.4. Suppose that $a, b \in K$ have the same minimal polynomial f over F . Then $F(a) \approx F(b)$.

Proof. Both fields are isomorphic to $F[x]/(f)$ by Theorem 8.3. ∇

Remark. To clarify a frequently used terminology, we say that $a \in F$ is a *zero* of a polynomial $f \in F[x]$ when $f(a) = 0$. Not to be confused, a *root* will be used interchangeably with the word *solution* and is always associated with an equation. Hence, a is a zero of f if and only if a is a root of $f(x) = 0$.

Theorem 8.5. Every nonconstant polynomial $f \in F[x]$ has a zero in some extension field K over F .

Proof. We may assume that f is irreducible for if $g(a) = 0$ for some factor g then $f(a) = 0$ too. Then $F[x]/(f)$ is a field, and the homomorphism $\theta(a) = (f) + a$ shows that $F[x]/(f)$ is a field extension over F , with $[F[x]/(f):F] = \deg f$. Now consider $(f) + x \in F[x]/(f)$. We have $f((f) + x) = (f) + f(x) = (f)$, the zero of $F[x]/(f)$. ∇

Corollary 8.6. For every $f \in F[x]$ there is an extension field K over F such that $f = a \prod (x - a_i) \in K[x]$.

Proof. By the theorem f is divisible by $(x - a)$, where a belongs to some extension field over F . The proof is done by induction on the degree of f . ∇

Definition. A polynomial $f \in F[x]$ *splits* when it factors $f = a \prod (x - a_i)$ in some extension field. The field $F(a_1, \dots, a_n)$ is called a *splitting field* for f over F . It can be shown that any two splitting fields for the same polynomial are isomorphic.

Example. A splitting field for $x^2 + 1$ over \mathbb{Q} is $\mathbb{Q}(\pm i) = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. Over \mathbb{R} , the same polynomial has splitting field \mathbb{C} .

The field \mathbb{C} of complex numbers have a special property where every $f \in \mathbb{C}[x]$ splits without the need of any extension field. Such a field is called *algebraically closed*. We state the big theorem without proof.

Theorem 8.7 (The Fundamental Theorem of Algebra). Let $f \in \mathbb{C}[x]$ have degree n . Then f has n complex zeros, counting multiplicity.

Proof. The proof can be found in a complex analysis text. ∇

Definition. A *multiple zero* of f is a zero a for which $(x - a)$ is a repeated factor in the splitting of f . The next theorem borrows the idea from Calculus in order to classify multiple zeros. Suppose that $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in F[x]$. We define the *derivative* of f to be the polynomial $f' = a_1 + 2a_2x + \dots + na_nx^{n-1}$.

Lemma 8.8. For every $f, g \in F[x]$ we have $(f + g)' = f' + g'$ and $(fg)' = f'g + fg'$.

Proof. Exercise. ∇

Theorem 8.9. Let $f \in F[x]$. Then $a \in F$ is a multiple zero of f if and only if a is a zero of both f and f' .

Proof. Suppose that $f = (x - a)^2g$. Then $f' = 2(x - a)g + (x - a)^2g'$, hence $f'(a) = 0$. Conversely if $f(a) = f'(a) = 0$, write $f = (x - a)g$. Then $f' = g + (x - a)g'$, hence $g(a) = 0$. It follows that $x - a \mid g$ and $(x - a)^2 \mid f$. ∇

Exercise 8

- 1) Find the minimal polynomial over \mathbb{Q} for each $1 + i$, $i + \sqrt{i}$, $\sqrt{1 + \sqrt{2}}$, $\sqrt[3]{2} - \sqrt{3}$.
- 2) Let $a \in K$. Prove that if a^2 is algebraic over F then a is too. Is the converse true?
- 3) Prove that $F(a, b) = (F(a))(b)$ for all a, b in any extension field over F .
- 4) Which one of $2x^7 + 3x^5 - 1$ and $5x^{21} - 6x^7 + 4$ has a multiple zero in its splitting field over \mathbb{Z}_7 ?

9 Finite Fields

By a *finite field* we mean a field F with only finitely many elements, such as \mathbb{Z}_p .

Lemma 9.1. Let G be a finite group. Suppose that $x^k = e$ has at most k solutions in G for each $k \geq 1$. Then G is cyclic.

Proof. Let $|G| = n$. For each $a \in G$ the cyclic subgroup $\langle a \rangle$ has order $d \mid n$. And each $x \in \langle a \rangle$ is a solution of $x^d = e$, hence *all* the solutions to $x^d = e$ are given by $\langle a \rangle$. In particular if an element $g \in G$ has order d then $g \in \langle a \rangle$ and $\langle g \rangle = \langle a \rangle$. So *if* there is an element of order d in G then there are exactly $\phi(d)$ elements of order d . But recall that $n = \sum \phi(d)$, where d ranges through all the divisors of n . It follows that G *does* have $\phi(d)$ elements of order d for each $d \mid n$. In particular there is an element of order n , hence G is cyclic. ∇

Theorem 9.2. Let F be a finite field. The multiplicative group F^* is cyclic.

Proof. This follows from the lemma because the group is finite and the polynomial $x^k - 1$ has at most k zeros over any field. ∇

Corollary 9.3. If p is a prime, the group U_p is cyclic under multiplication mod p .

Proof. U_p is the multiplicative group of nonzero elements in the finite field \mathbb{Z}_p . ∇

Definition. Given a field F we define its *characteristic*, written $\text{char}(F)$, to be the least positive integer n such that $n \cdot 1 := \sum_{i=1}^n 1 = 0$, where 1 denotes the unity of F . If there is no such value of n , we let $n = 0$. For examples, $\text{char}(\mathbb{Z}_p) = p$ and $\text{char}(\mathbb{Q}) = 0$.

Theorem 9.4. The characteristic of a finite field is a prime number.

Proof. Let F be a field of q elements. By the pigeonhole principle, two of the elements $0 \cdot 1, 1 \cdot 1, 2 \cdot 1, \dots, q \cdot 1$ are equal, say $i \cdot 1 = j \cdot 1$ with $i > j$. Then $(i - j) \cdot 1 = 0$ and so the characteristic of F is finite, say $\text{char}(F) = n$. If n were composite then we write $n = ab$ where $a, b < n$. Then $0 = n \cdot 1 = (ab) \cdot 1 = (a \cdot 1) \times (b \cdot 1)$. One of these factors must be 0 since F is a field, contradicting the minimality of n . ∇

Lemma 9.5. If $\text{char}(F) = p$, a prime, then F is an extension field over \mathbb{Z}_p . If $\text{char}(F) = 0$ then F is an extension over \mathbb{Q} .

Proof. Define $\theta : \mathbb{Z} \rightarrow F$ by $\theta(n) = n \cdot 1$. It is easy to verify that this map is a ring homomorphism. If $\text{char}(F) = 0$ then θ is one-to-one, in which case F contains \mathbb{Z} , as well as \mathbb{Q} since F is a field. If $\text{char}(F) = p$ then $\ker(\theta) = (p)$ and F contains $\mathbb{Z}/(p) \approx \mathbb{Z}_p$. ∇

Theorem 9.6. The number of elements in any finite field F is a prime power p^k , where $p = \text{char}(F)$.

Proof. By the lemma F is an extension field over \mathbb{Z}_p , where $p = \text{char}(F)$. Since F is finite, it has a finite basis over \mathbb{Z}_p as a vector space (see Chapter 12), say with k elements. We know \mathbb{Z}_p has p elements, so F has p^k elements. ∇

Lemma 9.7. If $\text{char}(F) = p$ then $(a + b)^p = a^p + b^p$ for all $a, b \in F$.

Proof. According to the binomial theorem,

$$(a + b)^p = \sum_{k=0}^p \binom{p}{k} a^{p-k} b^k, \quad \text{where} \quad \binom{p}{k} = \frac{p!}{k!(p-k)!}$$

Since p is prime, it divides $\binom{p}{k}$ for all except $\binom{p}{0} = \binom{p}{p} = 1$. Now in F every multiple of p disappears. Hence $(a + b)^p = a^p + b^p$. ∇

Theorem 9.8. Let $q = p^k$, a prime power. There exists a field F with q elements.

Proof. We consider an extension K over \mathbb{Z}_p where $x^q - x = (x - a_1) \cdots (x - a_q) \in K[x]$ based on Corollary 8.6. Note that elements of \mathbb{Z}_p are among the zeros. We claim that $F = \{a_1, \dots, a_q\}$ is a subfield of K by showing that it is closed under addition and multiplication. For all $a, b \in F$ we have $(ab)^q = a^q b^q = ab$ and, by the lemma and induction on k , $(a + b)^q = ((a + b)^p)^{p^{k-1}} = (a^p + b^p)^{p^{k-1}} = a^q + b^q$. To complete the proof, we make sure that there is no multiple zero. This follows from Theorem 8.9 because $(x^q - x)' = qx^{q-1} - 1 = -1$ as $\text{char}(K) = p$. ∇

Remark. Since $x^q - x = (x - a_1) \cdots (x - a_q) \in F[x]$ is true for any finite field F of q elements (Exercise 7.2), then the proof above implies that $F = \mathbb{Z}_p(a_1, \dots, a_q)$, the splitting field of $x^q - x$ over \mathbb{Z}_p . We did not prove that splitting fields are unique for a given polynomial, but we can still show that finite fields are unique for a fixed q .

Theorem 9.9. Any two finite fields of order $q = p^k$ are isomorphic.

Proof. Call the fields K and L , both extensions over \mathbb{Z}_p . By Theorem 9.2 we assume $K^* = \langle a \rangle$, so that $K = \mathbb{Z}_p(a) \approx \mathbb{Z}_p[x]/(f)$, where f is the minimal polynomial of a over \mathbb{Z}_p . By Theorem 8.2, $f \mid x^q - x$ in $\mathbb{Z}_p[x]$. But $x^q - x = (x - b_1) \cdots (x - b_q) \in L[x]$, hence $f(b) = 0$ for some $b \in L$. Thus f is also the minimal polynomial of b over \mathbb{Z}_p and, Corollary 8.4 implies $K \approx \mathbb{Z}_p(b)$, a subfield of L . We conclude that $K \approx L$ because they have equal size. ∇

Definition. Without ambiguity, we denote a finite field of order $q = p^k$ using the notation \mathbb{F}_q . The multiplicative group \mathbb{F}_q^* , consisting of the $q - 1$ nonzero elements, is cyclic with $\phi(q - 1)$ generators. In particular $\mathbb{F}_p = \mathbb{Z}_p$ and $\mathbb{F}_p^* = U_p$.

Example. The polynomial $f = x^2 + x + 1$ is irreducible over \mathbb{Z}_2 . (Why?) The field $\mathbb{Z}_2[x]/(f)$ has order 4 since it is represented by $a + bx$ with $a, b = 0$ or 1 . This is the field $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$, where α satisfies $\alpha^2 + \alpha + 1 = 0$, or $\alpha^2 = 1 + \alpha$. We construct the Cayley tables for \mathbb{F}_4 below. Note that α and $1 + \alpha$ are the two generators for \mathbb{F}_4^* .

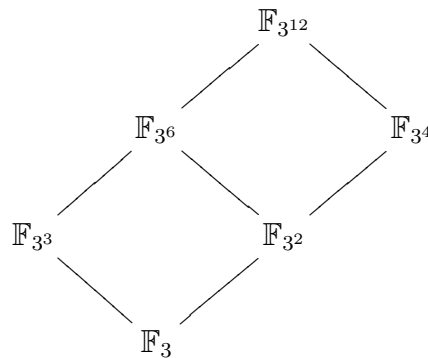
$+$	0	1	α	$1 + \alpha$	\times	0	1	α	$1 + \alpha$
0	0	1	α	$1 + \alpha$	0	0	0	0	0
1	1	0	$1 + \alpha$	α	1	0	1	α	$1 + \alpha$
α	α	$1 + \alpha$	0	1	α	0	α	$1 + \alpha$	1
$1 + \alpha$	$1 + \alpha$	α	1	0	$1 + \alpha$	0	$1 + \alpha$	1	α

Example. Similarly, $f = x^2 - 2$ is irreducible over $F = \mathbb{Z}_{11}$ and the factor ring $F[x]/(f)$ is the finite field \mathbb{F}_{121} . In this case, \mathbb{F}_{121}^* has $\phi(120) = 32$ generators. In general, the field $\mathbb{Z}_p[x]/(f)$ has p^n elements, if $f \in \mathbb{Z}_p[x]$ is an irreducible polynomial of degree n .

Theorem 9.10. The finite field \mathbb{F}_{p^k} has a subfield \mathbb{F}_q if and only if $q = p^j$ with $j \mid k$.

Proof. Having the same characteristic, a subfield of \mathbb{F}_{p^k} is clearly \mathbb{F}_{p^j} with $j \leq k$. Looking at the multiplicative groups, we have $p^j - 1 \mid p^k - 1$, which holds if and only if $j \mid k$. (Why?) Conversely, suppose $j \mid k$. Since $x^{p^j-1} - 1 \mid x^{p^k-1} - 1$, the zeros of $x^{p^j} - x$, which compose \mathbb{F}_{p^j} , are zeros of $x^{p^k} - x$, which form \mathbb{F}_{p^k} . Thus the latter field contains the former as a subfield. ◻

Example. The above theorem allows us to identify all the subfields of a given finite field \mathbb{F}_q in much a similar way we do for groups using a subgroup lattice. The following diagram depicts the *subfield lattice* for $\mathbb{F}_{3^{12}}$.



Exercise 9

- 1) If $\text{char}(F) = p$, prove that $F = \{a^p \mid a \in F\}$ by way of the isomorphism $\theta(a) = a^p$.
- 2) Construct the Cayley tables for the finite field $\mathbb{Z}_2[x]/(x^3 + x + 1)$ and find the multiplicative order of each nonzero element. Do the same with $\mathbb{Z}_3[x]/(x^2 + 1)$.
- 3) Draw the subfield lattice of \mathbb{F}_q for each $q = 7^{16}, 5^{24}, 3^{2009}$, and 1024 .
- 4) In a finite field, show that multiplying all the nonzero elements yields -1 . Use this to prove Wilson’s theorem: if p is prime then $(p - 1)! \equiv -1 \pmod{p}$.

10 Irreducibility Tests in $\mathbb{Q}[x]$

Definition. The polynomial $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ is *primitive* if the only divisors common to all a_i are ± 1 . In particular, if f is monic then it is primitive.

Lemma 10.1. If f, g are primitive then fg is also primitive.

Proof. Let $f = \sum a_i x^i$, $g = \sum b_i x^i$ and $fg = \sum c_i x^i$. By way of contradiction suppose there is a prime $p \mid c_i$ for all i . Since f is primitive, not all its coefficients are divisible by p . Let j be the smallest such that $p \nmid a_j$. Similarly k is the smallest such that $p \nmid b_k$. Since $p \mid c_{j+k} = \sum_{i=0}^{j+k} a_i b_{j+k-i}$ then $p \mid a_j b_k$, contradicting Euclid's lemma. \square

Theorem 10.2 (Gauss' Lemma). Suppose that $f \in \mathbb{Z}[x]$ is primitive. If $f = gh \in \mathbb{Q}[x]$ then there exists $a \in \mathbb{Q}$ such that both ag and $a^{-1}h$ belong to $\mathbb{Z}[x]$. In particular, if f is reducible in $\mathbb{Q}[x]$ then it is reducible in $\mathbb{Z}[x]$.

Proof. Let $f = gh \in \mathbb{Q}[x]$. Using least common denominator we can find $a \in \mathbb{Q}$ such that $ag \in \mathbb{Z}[x]$ and is primitive. Similarly, $ah \in \mathbb{Z}[x]$ for some $b \in \mathbb{Q}$. Then the product $agbh = abf \in \mathbb{Z}[x]$ is primitive, which is possible only if $ab = 1$. \square

Theorem 10.3 (Eisenstein Criterion). Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. If there is a prime number p such that $p^2 \nmid a_0$, $p \mid a_0$, $p \mid a_1, \dots, p \mid a_{n-1}$, but $p \nmid a_n$, then f is irreducible in $\mathbb{Q}[x]$.

Proof. We assume f is primitive, otherwise factor out the gcd without affecting the proof. By contradiction suppose f can be factored in $\mathbb{Q}[x]$. Then by Gauss' lemma we may write $f(x) = (b_0 + b_1x + \cdots + b_r x^r)(c_0 + c_1x + \cdots + c_s x^s)$ with integer coefficients, $r, s \geq 1$. Since $p \mid a_0 = b_0c_0$ then $p \mid b_0$ or $p \mid c_0$ but not both since $p^2 \nmid a_0$. Assume $p \mid b_0$ and $p \nmid c_0$. Since f is primitive, let $k < r$ be the least such that $p \nmid b_k$. But $p \mid a_k = b_0c_k + b_1c_{k-1} + \cdots + b_kc_0$ hence $p \mid b_kc_0$ —impossible since $p \nmid b_k$ and $p \nmid c_0$. \square

Theorem 10.4. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Suppose that p is a prime such that $p \nmid a_n$. Taking mod p of the coefficients, if f is irreducible in $\mathbb{Z}_p[x]$ then f is irreducible in $\mathbb{Q}[x]$.

Proof. By contradiction, assume that $f = gh$ in $\mathbb{Q}[x]$ with $\deg g, \deg h < \deg f$. Since $\deg f$ is unchanged when viewed mod p , then $\deg g, \deg h < \deg f$ in $\mathbb{Z}_p[x]$, showing that f is reducible in $\mathbb{Z}_p[x]$. \square

Example. Consider $f = 3x^3 - x^2 + 1$. Mod 2, neither 0 nor 1 is a zero. Since $\deg f = 3$, having no zero means f is irreducible in $\mathbb{Q}[x]$. Note that $p = 3$ cannot be chosen for then $f \equiv -x^2 + 1$, of lesser degree. Also, the theorem does not work the other way, for example $x^4 + 1$ is irreducible over \mathbb{Q} (Why?) although mod 17, it is divisible by $x - 2$.

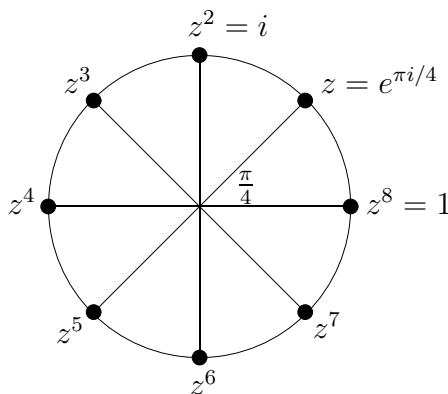
Exercise 10

- 1) Prove that $x^n - p$ is irreducible in $\mathbb{Q}[x]$, where p is any prime number.
- 2) Prove that $3x^4 - 10x^3 + 2x^2 - x + 7$ is irreducible in $\mathbb{Q}[x]$ by working in \mathbb{Z}_2 .
- 3) Let $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Show that if $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, then $a \mid a_0$ and $b \mid a_n$. In particular this explains that if $f \in \mathbb{Z}[x]$ is monic, any rational number solution of $f(x) = 0$ must be an integer.
- 4) Show that $x^4 + 1$ is irreducible over \mathbb{Q} .

11 Cyclotomic Polynomials

Definition. By an n th root of unity we mean a zero of $x^n - 1$ in some splitting field over the underlying field in context. This root is *primitive* if it is not a zero of $x^k - 1$ for any $k < n$.

Example. The n th roots of unity in \mathbb{C} are given by $z, z^2, \dots, z^n = 1$, where $z = e^{2\pi i/n}$. The graph below roughly displays the coordinates of the eight complex eighth roots of unity, which are proportionally dispersed along the unit circle in the complex plane.



Theorem 11.1. Let $z = e^{2\pi i/n} \in \mathbb{C}$. There are exactly $\phi(n)$ primitive n th roots of unity, given by z^k for all positive integers k less than and relatively prime to n .

Proof. The multiplicative cyclic subgroup $\langle z \rangle$ has order n . The primitive n th roots of unity are precisely the generators of $\langle z \rangle$; and the proof is all group theory. \square

Definition. Let $z_1, \dots, z_{\phi(n)}$ denote the $\phi(n)$ distinct primitive n th roots of unity in \mathbb{C} . The n th cyclotomic polynomial is given by $\Phi_n = (x - z_1) \cdots (x - z_{\phi(n)}) \in \mathbb{C}[x]$. Note that Φ_n is monic, of degree $\phi(n)$, and has no multiple zeros. In fact all the $\phi(n)$ zeros of Φ_n in \mathbb{C} are the $\phi(n)$ distinct primitive n th roots of unity.

Example. We give Φ_n for the first few values of n .

$$\begin{aligned} \Phi_1 &= x - 1 \\ \Phi_2 &= x + 1 \\ \Phi_3 &= (x - e^{2\pi i/3})(x - e^{4\pi i/3}) \\ &= \left(x - \frac{-1 + i\sqrt{3}}{2}\right) \left(x - \frac{-1 - i\sqrt{3}}{2}\right) \\ &= x^2 + x + 1 \end{aligned}$$

Theorem 11.2. The factorization $x^n - 1 = \prod_{d|n} \Phi_d$ holds over \mathbb{C} .

Proof. Consider $G = \langle z \rangle$ again, partition it into subsets $G_d = \{a \in G \mid |a| = d\}$. Note that G_d is nonempty if and only if $d \mid n$. Now $a \in G_d$ if and only if a is a primitive d th root of unity. Hence, $x^n - 1 = \prod_{a \in G} (x - a) = \prod_{d|n} \prod_{a \in G_d} (x - a) = \prod_{d|n} \Phi_d$. \square

Example. The above theorem can be used to compute Φ_n for all $n > 1$ in a recursive manner. For example, $x^4 - 1 = \Phi_1\Phi_2\Phi_4 = (x - 1)(x + 1)\Phi_4$, from which we are able to derive Φ_4 —and similarly for other values of n —by performing long division, below.

$$\begin{aligned}\Phi_4 &= x^2 + 1 \\ \Phi_6 &= x^2 - x + 1 \\ \Phi_8 &= x^4 + 1 \\ \Phi_9 &= x^6 + x^3 + 1 \\ \Phi_{10} &= x^4 - x^3 + x^2 - x + 1 \\ \Phi_{12} &= x^4 - x^2 + 1 \\ \Phi_{14} &= x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 \\ \Phi_{15} &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \\ \Phi_{16} &= x^8 + 1 \\ \Phi_{18} &= x^6 - x^3 + 1\end{aligned}$$

Missing in the above list, when n is prime, Φ_n is given by the next theorem.

Theorem 11.3. If p is a prime then $\Phi_p = 1 + x + x^2 + \cdots + x^{p-1}$.

Proof. Since $x^p - 1 = \Phi_1\Phi_p$ then we have $\Phi_p = (x^p - 1)/(x - 1)$. ▽

You might think that the coefficients of Φ_n are only ± 1 . That is false, but you will not see any counterexample until Φ_{105} . What is not hard to demonstrate, next, is the fact that the coefficients are always integer.

Theorem 11.4. The cyclotomic polynomials Φ_n belong to $\mathbb{Z}[x]$ for all $n \geq 1$.

Proof. We use induction based on $x^n - 1 = \prod_{d|n} \Phi_d$, which allows us to assume $x^n - 1 = f\Phi_n$ for some monic polynomial $f \in \mathbb{Z}[x]$. This shows that $\Phi_n \in \mathbb{Q}[x]$ by the division algorithm there. Then by Gauss' lemma, $\Phi_n \in \mathbb{Z}[x]$ since it is monic. ▽

Definition. We name the extension $\mathbb{Q}(z)$ the n th *cyclotomic field* over \mathbb{Q} if z is a primitive n th root of unity in \mathbb{C} . Note that $\mathbb{Q}(z) = \mathbb{Q}(z^k)$ if and only if $\gcd(k, n) = 1$, hence the notation $\mathbb{Q}(z)$ is not dependent on which primitive root we choose.

Theorem 11.5. The n th cyclotomic field $\mathbb{Q}(z)$ is isomorphic to $\mathbb{Q}[x]/(\Phi_n)$.

Proof. This follows from the next theorem, which asserts that Φ_n is irreducible, thus establishing it as the minimal polynomial of z over \mathbb{Q} . ▽

Theorem 11.6. The cyclotomic polynomial Φ_n is irreducible over \mathbb{Q} .

Proof. Assume that $\Phi_n = fg \in \mathbb{Z}[x]$, both monic and f is chosen irreducible. Let z be a primitive n th root of unity for which $f(z) = 0$, hence f is the minimal polynomial of z over \mathbb{Q} . Choose a prime p as long as $p \nmid n$, so that z^p is another primitive root. Then z^p is a zero of either f or g . We will first show that $g(z^p) = 0$ is impossible.

If $g(z^p) = 0$ then z is a zero of $g(x^p)$ and $f \mid g(x^p)$. We may write $fh = g(x^p) \in \mathbb{Z}[x]$. Reducing mod p , we have $f'h' = g'(x^p) \in \mathbb{Z}_p[x]$, degrees unchanged. But by Lemma 9.7 $g'(x^p) = g'(x)^p$ in $\mathbb{Z}_p[x]$, where unique factorization applies. Here any irreducible factor of f' divides g' as well. Thus $f'g' = \Phi_n'$ implies that Φ_n' has multiple zeros, hence $x^n - 1$

does as well, over \mathbb{Z}_p . This is banned by Theorem 8.9: the derivative is $nx^{n-1} \neq 0$; only 0 is zero, and 0 is never a root of unity.

So we have $f(z^p) = 0$. Now a typical primitive n th root of unity is z^k with $\gcd(k, n) = 1$. In that case $k = p_1 \cdots p_r$, not assumed distinct, such that $p_i \nmid n$. Writing $z^k = (z^{p_1})^{p_2 \cdots p_r}$ we see by induction that $f(z^k) = 0$ —for all $\phi(n)$ values of k . This can happen only if $f = \Phi_n$, irreducible over \mathbb{Z} , and over \mathbb{Q} by Gauss’ lemma. ∇

Exercise 11

- 1) Compute Φ_n for each value of $n = 20, \dots, 30$.
- 2) Verify the following identities.
 - a) $\Phi_n(0) = 1$ for all $n \geq 2$
 - b) $\Phi_{2^n}(x) = x^{2^{n-1}} + 1$ for all $n \geq 1$
 - c) $\Phi_{2n}(x) = \Phi_n(-x)$ for all odd $n \geq 3$
 - d) $\Phi_{n^2}(x) = \Phi_n(x^n)$ for all $n \geq 1$
- 3) Prove that Φ_p is irreducible over \mathbb{Q} , where p is prime, using Eisenstein’s criterion and the substitution $x = y + 1$.
- 4) Show that $\gcd(x^m - 1, x^n - 1) = x^{\gcd(m,n)} - 1$ in $\mathbb{Q}[x]$ by factoring both of them into cyclotomic polynomials.

12 Algebraic Extensions

Definition. Let K be an extension field over F . The *degree* $[K:F]$ of K over F is the dimension of K as a vector space over F . If this degree is a finite number, we say that the field K is a *finite extension* over F ; or an *infinite extension* otherwise.

Theorem 12.1. Let $F \subseteq K \subseteq L$ be extensions of fields. Then $[L:F] = [L:K] \times [K:F]$ if finite, and in particular, $[K:F] \mid [L:F]$. Hence, a finite extension over another finite extension is finite over the bottom field.

Proof. The proof can be found in a linear algebra text. ∇

Definition. An element $a \in K$ which is not algebraic over F is called a *transcendental* element. For examples, the real numbers π and e are both transcendental over \mathbb{Q} , but this fact is not easy to demonstrate.

Theorem 12.2. The element $a \in K$ is algebraic of degree n over F if and only if $[F(a):F] = n$. Hence a is transcendental if and only if $F(a)$ is an infinite extension over F .

Proof. We have seen that $F[x]/(f) = \{(f) + a_0 + a_1x + \dots + a_{n-1}x^{n-1} \mid a_i \in F\}$, where $n = \deg f$. In this case $\{1, x, \dots, x^{n-1}\}$ is a basis of $F[x]/(f)$ over F . Hence if a is algebraic then $\{1, a, \dots, a^{n-1}\}$ is a basis of $F(a)$ over F and $[F(a):F] = n$. Conversely if $[F(a):F] = n$ then the set $\{1, a, \dots, a^n\}$ is linearly dependent, that is, there exists $g \in F[x]$ such that $g(a) = 0$ and so a is algebraic. By Theorem 8.3, $[F[x]/(f):F] = n$, where f is the minimal polynomial of a over F . Hence $\deg f = n$. ∇

Example. The n th cyclotomic field $\mathbb{Q}(z)$ is an extension of degree $\phi(n)$ over \mathbb{Q} , because the minimal polynomial of z is given by Φ_n , whose degree is $\phi(n)$. On the other hand, the extension \mathbb{R} over \mathbb{Q} is infinite. To see it, simply consider the intermediate subfield $\mathbb{Q}(\pi)$, trusting that π is transcendental.

Lemma 12.3. If $a, b \neq 0$ are algebraic over F then $a \pm b, ab, ab^{-1}$ are algebraic over F .

Proof. We have field extensions $F \subseteq F(a) \subseteq (F(a))(b) = F(a, b)$, where each is finite over the one below it, according to Theorem 12.2. By Theorem 12.1 $F(a, b)$ is finite over F and, being a field, it contains $a \pm b, ab, ab^{-1}$. Hence by Theorem 12.2 again, all these elements are also algebraic over F . ∇

Theorem 12.4. Let K be an extension field over F . The set of all elements in K which are algebraic over F is a subfield of K containing F .

Proof. This follows directly from the lemma. ∇

Theorem 12.5. Let K be the field of all real numbers which are algebraic over \mathbb{Q} . Then the degree $[K:\mathbb{Q}]$ is infinite.

Proof. The polynomial $x^n - 2$ is irreducible according to Eisenstein's criterion. Hence the real number $\sqrt[n]{2}$ is algebraic of degree n over \mathbb{Q} . It follows that $[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}] = n$ and $[K:\mathbb{Q}] \geq n$. Since n is arbitrary, K must be an infinite extension. ∇

Definition. The extension field K over F is called an *algebraic extension* if every element $a \in K$ is algebraic over F .

Theorem 12.6. The extension field K over F is finite if and only if K is an algebraic extension over F in the form $K = F(a_1, \dots, a_n)$ for some elements $a_1, \dots, a_n \in K$.

Proof. If $[K:F]$ is finite then so is $[F(a):F]$ for any $a \in K$ by Theorem 12.1, hence by Theorem 12.2, K is an algebraic extension. The elements a_1, \dots, a_n can be chosen from any basis of K over F as a vector space. Conversely suppose $K = F(a_1, \dots, a_n)$ is algebraic over F . Since $F \subseteq F(a_1) \subseteq (F(a_1))(a_2) \subseteq \dots \subseteq K$ and each step is finite, then $[K:F]$ is finite by Theorem 12.1. ∇

Theorem 12.7. Algebraic extension over an algebraic extension is again algebraic. That is, if K is algebraic over F and L is algebraic over K then L is algebraic over F .

Proof. Let $a \in L$. Since a is algebraic over K , we have $b_0 + b_1a + \dots + b_na^n = 0$ for some elements $b_i \in K$. These b_i 's are algebraic over F , hence by Theorem 12.6, $[M:F]$ is finite where $M = F(b_0, \dots, b_n)$. Also a is algebraic over M , hence by Theorem 12.2 $[M(a):M]$ is finite. By Theorem 12.1 then $M(a)$ is finite over F . But $M(a) = F(a, b_0, \dots, b_n)$, hence by Theorem 12.6 again, a is algebraic over F . ∇

Exercise 12

- 1) Find the degree and a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over \mathbb{Q} .
- 2) Given that π is transcendental over \mathbb{Q} , show that $\pi^{2/3}$ is also transcendental.
- 3) Suppose that a, b are algebraic over F of degrees m, n respectively. If $\gcd(m, n) = 1$, prove that $[F(a, b):F] = mn$.
- 4) The extension field K over F is called *simple* if $K = F(a)$ for some $a \in K$.
 - a) Prove that any extension field of prime degree is simple.
 - b) Prove that any finite extension over a finite field is simple.
 - c) If $\text{char}(F) = 0$, it is known that $F(a, b)$ is simple for all algebraic elements $a, b \in K$. Use this fact to prove that any finite extension over \mathbb{Q} is simple.
 - d) Illustrate (c) by finding $a \in \mathbb{R}$ such that $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(a)$.

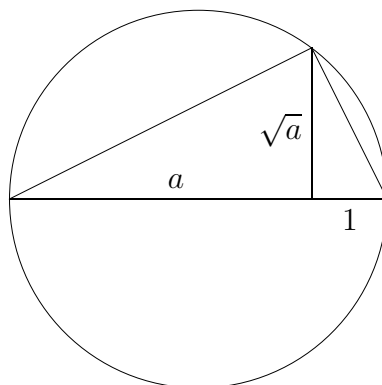
13 Applications in Classical Geometry

Consider the xy -plane of the usual cartesian coordinate system. A point on the plane is *constructible* if it can be traced out using only an unmarked ruler and a compass. The unit length is assumed, so that at least we are able construct all points with integer coordinates. By dropping perpendicular lines against the x and y -axes, we see that a point (a, b) is constructible if and only if the real number lengths a and b are constructible.

Theorem 13.1. The real numbers which are constructible form a subfield of \mathbb{R} .

Proof. Let $a, b \in \mathbb{R}$ be constructible. It is intuitively clear how to get the lengths $a \pm b$ using a ruler and a compass. It is also known how to construct two similar right-angle triangles $ABC \sim A'B'C'$. To construct ab we let $AB = 1$, $BC = a$, and $A'B' = b$. Then by the properties of similar triangles, we have $B'C' = ab$. To make $B'C' = 1/a$, simply let $AB = a$, $BC = 1$, and $A'B' = 1$. ∇

Example. The theorem implies that all rational numbers are constructible. To see an irrational number example, recall in grade school geometry how to construct \sqrt{a} from a given length a , pictured below.



Theorem 13.2. The number $a \in \mathbb{R}$ is constructible only if a is algebraic over \mathbb{Q} of degree a power of 2.

Proof. Consider equations of lines and circles with coefficients in $F = \mathbb{Q}$. We omit details, but any two such graphs only intersect at constructible coordinates belonging to F or to some quadratic extension $F(\sqrt{a_0})$. Constructible numbers are all obtained in this way, perhaps successively replacing F by $F_1 = F(\sqrt{a_0})$, then F_1 by $F_2 = F_1(\sqrt{a_1})$, and on. In each step we have $[F_n : \mathbb{Q}] = 2^n$. ∇

Remark. The proof actually gives a stronger statement: a is constructible only if $a \in F_n$ in some tower of extension fields $\mathbb{Q} \subset F_1 \subset \cdots \subset F_n \subset \mathbb{R}$, such that $F_{i+1} = F_i(\sqrt{a_i})$, of degree 2 over F_i . In fact, this is a necessary and sufficient condition to be constructible since, as seen in the previous example, square root numbers are constructible.

Example. A classical geometry challenge posed by the Greeks was to construct a square whose area equals that of a given circle. This is the famous *squaring the circle* problem. To construct such a square requires the length $\sqrt{\pi}$, which is not algebraic. With the theorem, we know why this challenge is impossible to answer.

Corollary 13.3. An arbitrary angle cannot be trisected.

Proof. We show as a counterexample that $\alpha = 60^\circ$ cannot be trisected because the number $a = \cos 20^\circ$ is not constructible. We use the trigonometric identity $\cos 3\alpha = 4 \cos^3 \alpha - 3 \cos \alpha$ to see that $8a^3 - 6a - 1 = 0$. Now the polynomial $8x^3 - 6x - 1$ is irreducible over \mathbb{Q} because it has no zero mod 5, for instance. Hence $[\mathbb{Q}(a):\mathbb{Q}] = 3$, not a power of 2. ∇

Corollary 13.4. The regular septagon is not constructible.

Proof. Let $\alpha = 2\pi/7$. To construct the septagon it is necessary that both $\sin \alpha$ and $\cos \alpha$ be constructible, say they belong to some extension K of degree 2^n over \mathbb{Q} . Then the primitive seventh root of unity $z = \cos \alpha + i \sin \alpha$ belongs to $K(i)$, of degree 2 over K . Hence $[K(i):\mathbb{Q}] = 2^{n+1}$. But note that $\mathbb{Q}(z)$ is an intermediate subfield of degree $\phi(7) = 6$. Since $6 \nmid 2^{n+1}$, this whole thing is impossible. ∇

Definition. The *Fermat numbers* are given by $F_n = 2^{2^n} + 1$ for integers $n \geq 0$. A *Fermat prime* is a Fermat number which is also a prime number. The first five Fermat numbers are Fermat primes: 3, 5, 17, 257, 65537. However, it is not yet known if there is any more Fermat prime.

Lemma 13.5. Any prime of the form $2^m + 1$ is a Fermat prime.

Proof. Exercise. ∇

Theorem 13.6. The regular polygon with n vertices is constructible only if n is a product of some power of 2 and distinct Fermat primes.

Proof. Generalizing from the case $n = 7$, the previous proof shows it necessary that $\phi(n)$ be a power of 2. If $n = 2^k \prod p_i^{e_i}$ then $\phi(n) = 2^{k-1} \prod p_i^{e_i-1} (p_i - 1)$. Hence $e_i = 1$ for each i , and p_i is a power of 2 plus one. By the lemma each p_i is a Fermat prime. ∇

Remark. The converse of the theorem is good as well. In particular Gauss, who first proved it, actually constructed a regular 17-gon in his teen. But for us to prove it, we will have to wait for Galois theory.

Exercise 13

- 1) Another ancient Greek problem is called *doubling the cube*. Can we construct a cube double the volume of another constructible cube?
- 2) Which of the angles $8^\circ, 9^\circ, 15^\circ, 40^\circ$ are constructible?
- 3) Suppose that there are no more Fermat primes. How many regular polygons can be constructed with an odd number of vertices?
- 4) Using ruler and compass only, show how to construct a regular pentagon.

To Learn More

Any one of the following textbooks is recommended for further reading and self-study.

1. Michael F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley 1969, Westview Press 1994.
2. Daniel A. Marcus, *Number Fields*, Springer 1977, 1995.
3. Gary L. Mullen and Carl Mummert, *Finite Fields and Applications*, American Mathematical Society 2007.
4. Pierre Samuel, *Algebraic Theory of Numbers*, Hermann 1970, Dover 2008.