# Selected Solutions to Artin's Algebra, Second Ed.

Takumi Murayama

July 22, 2014

These solutions are the result of taking MAT323 Algebra in the Spring of 2012, and also TA-ing for MAT346 Algebra II in the Spring of 2014, both at Princeton University. This is not a *complete* set of solutions; see the List of Solved Exercises at the end. Please e-mail `takumim@umich.edu` with any corrections.

## Contents

# 2 Groups

## 2.1 Laws of Composition

**Exercise 2.1.2.** *Prove the properties of inverses that are listed near the end of the section.*

*Remark.* The properties are listed on p. 40 as the following:

(*a*) If an element $a$ has both a left inverse $l$ and a right inverse $r$, i.e., if $la = 1$ and $ar = 1$, then $l = r$, $a$ is invertible, $r$ is its inverse.
(*b*) If $a$ is invertible, its inverse is unique.
(*c*) Inverses multiply in the opposite order: If $a$ and $b$ are invertible, so is the product $ab$, and $(ab)^{-1} = b^{-1}a^{-1}$.
(*d*) An element $a$ may have a left inverse or a right inverse, though it is not invertible.

*Proof of* (*a*). We see $l = lar = r$. □

*Proof of* (*b*). Let $b, b'$ be inverses of $a$. Then, $b = bab' = b'$, by (*a*). □

*Proof of* (*c*). Consider $ab$. We see that $b^{-1}a^{-1}$ is the inverse of $ab$ since $(b^{-1}a^{-1})(ab) = b^{-1}a^{-1}ab = b^{-1}b = 1$ by associativity. Uniqueness follows by (*b*). □

*Proof of* (*d*). Consider Exercise 2.1.3 below. $s$ is not invertible since it does not have a two-sided inverse, but it does have a left inverse. □

**Exercise 2.1.3.** *Let* $\mathbb{N}$ *denote the set* $\{1, 2, 3, \ldots\}$ *of natural numbers, and let* $s\colon \mathbb{N} \to \mathbb{N}$ *be the* shift *map, defined by* $s(n) = n + 1$. *Prove that* $s$ *has no right inverse, but that it has infinitely many left inverses.*

*Proof.* $s$ does not have a right inverse since $s$ does not map any element of $\mathbb{N}$ back to 1; however, we can define a left inverse $r_k(n) = n - 1$ for $n > 1$, and $r_k(1) = k$ for some $k \in \mathbb{N}$; we see that this is a left inverse of $s$, i.e., that $r_k \circ s = \mathrm{id}_{\mathbb{N}}$. Since $k$ is arbitrary this implies that there is an infinite number of $r_k$'s. □

## 2.2 Groups and Subgroups

**Exercise 2.2.3.** *Let* $x$, $y$, $z$, *and* $w$ *be elements of a group* $G$.

(*a*) *Solve for* $y$, *given that* $xyz^{-1}w = 1$.
(*b*) *Suppose that* $xyz = 1$. *Does it follow that* $yzx = 1$? *Does it follow that* $yxz = 1$?

*Solution for* $(a)$. We claim that $y = x^{-1}w^{-1}z$. This follows since

$$x(x^{-1}w^{-1}z)z^{-1}w = xx^{-1}w^{-1}zz^{-1}w = 1. \qquad \square$$

*Solution for* $(b)$. Suppose $xyz = 1$. This implies $x^{-1} = yz$, and by Exercise 2.1.2$(a)$, this left inverse is a right inverse, and so $1 = xyz = x(yz) = (yz)x = yzx$.

Now consider $yxz$; the example

$$x = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad z = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}, \quad xyz = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad yxz = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$$

in $GL_2(\mathbb{R})$ shows that $xyz = 1$ does not imply $yxz = 1$. $\square$

**Exercise 2.2.4.** *In which of the following cases is $H$ a subgroup of $G$?*

$(a)$ $G = GL_n(\mathbb{C})$ *and* $H = GL_n(\mathbb{R})$.

$(b)$ $G = \mathbb{R}^\times$ *and* $H = \{1, -1\}$.

$(c)$ $G = \mathbb{Z}^+$ *and $H$ is the set of positive integers.*

$(d)$ $G = \mathbb{R}^\times$ *and $H$ is the set of positive reals.*

$(e)$ $G = GL_2(\mathbb{R})$ *and $H$ is the set of matrices* $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, *with* $a \neq 0$.

*Solution for* $(a)$. $H$ is a subset since $\mathbb{R} \subset \mathbb{C}$ implies $H \subset GL_n(\mathbb{R})$. $H$ is a subgroup since $GL_n(\mathbb{R})$ is a group, hence contains an identity and is closed under multiplication and inversion. $\square$

*Solution for* $(b)$. $H$ is a subgroup since it is clearly a subset, contains the identity 1, and $-1 \times -1 = 1$ implies $H$ is closed under multiplication and inversion. $\square$

*Solution for* $(c)$. $H$ is not a subgroup since $-1 \notin H$, though it is the inverse of 1. $\square$

*Solution for* $(d)$. $H$ is a subgroup since it is clearly a subset, contains 1, is closed under multiplication since the product of two positive real numbers is a positive real number, and since $x \in H$ has inverse $1/x \in H$, which is still positive and real. $\square$

*Solution for* $(e)$. $H$ is not a subgroup since it is not even a subset of $G$. $\square$

## 2.4 Cyclic Groups

**Exercise 2.4.1.** *Let $a$ and $b$ be elements of a group $G$. Assume that $a$ has order 7 and that $a^3b = ba^3$. Prove that $ab = ba$.*

*Proof.* $ab = aba^7 = a(ba^3)a^4 = a(a^3b)a^4 = a^4(ba^3)a = a^4(a^3b)a = ba$. $\square$

**Exercise 2.4.3.** *Let $a$ and $b$ be elements of a group $G$. Prove that $ab$ and $ba$ have the same order.*

*Proof.* Suppose $(ab)^n = 1$. We note that $b = b(ab)^n = (ba)^n b$, but this implies $(ba)^n = 1$, and so both have order $n$. □

**Exercise 2.4.6.**

(a) *Let $G$ be a cyclic group of order 6. How many of its elements generate $G$? Answer the same question for cyclic groups of order 5 and 8.*

(b) *Describe the number of elements that generate a cyclic group of arbitrary orders $n$.*

*Solution for (b).* By Prop. 2.4.3, if $x$ generates $G$ a cyclic group of order $n$, another element $x^i \in G$ generates $G$ if and only if $\gcd(i, n) = 1$ for $1 \leq i \leq n$, since then $|x^i| = n$. Thus, the number of elements that generate $G$ is equal to the number of numbers less than $n$ that are coprime to $n$. □

*Solution for (a).* By (b), it suffices to count the number of numbers less than $n$ that are coprime to $n$. For 6, $\{1, 5\}$ are coprime to 6, hence two elements generate the cyclic group of order 6. For 5, $\{1, 2, 3, 4\}$ are coprime to 5, hence four elements generate the cyclic group of order 5. For 8, $\{1, 3, 5, 7\}$ are coprime to 8, hence four elements generate the cyclic group of order 8. □

**Exercise 2.4.9.** *How many elements of order 2 does the symmetric group $S_4$ contain?*

*Solution.* The order 2 elements of $S_4$ consist of $\binom{4}{2} = 6$ two-cycles, and $\binom{4}{2} \times \frac{1}{2} = 3$ products of disjoint two-cycles, and so there are 9 elements of order 2. □

**Exercise 2.4.10.** *Show by example that the product of elements of finite order in a group need not have finite order. What if the group is abelian?*

*Solution.* Consider $GL_2(\mathbb{R})$, and the following matrices in $GL_2(\mathbb{R})$:

$$A = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

We see that $A^2 = B^2 = 1$, and so they are of order 2, whereas

$$AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \implies (AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix},$$

and so $AB$ has infinite order.

Now suppose the group is abelian. Suppose $a, b$ are our elements of finite order, of order $n, m$ respectively. Then, $(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = 1$, and so $ab$ is necessarily of finite order. □

## 2.6 Isomorphisms

**Exercise 2.6.2.** *Describe all homomorphisms $\varphi\colon \mathbb{Z}^+ \to \mathbb{Z}^+$. Determine which are injective, which are surjective, and which are isomorphisms.*

*Solution.* By the definition of homomorphism, for all positive $n \in \mathbb{Z}^+$, we have

$$\varphi(n) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n \text{ times}}, \quad \varphi(-n) = -\varphi(n), \quad \varphi(0) = \varphi(n) + \varphi(-n) = 0.$$

Thus, $\varphi$ is fully determined by what 1 maps to. By the above, we then have that $\varphi_n : z \rightsquigarrow nz$ for $n \in \mathbb{Z}^+$ are all the homomorphisms of $\mathbb{Z}^+$. The injective homomorphisms consist of those $\varphi_n$ for $n \neq 0$. The surjective homomorphisms consist of those $\varphi_n$ for $n = \pm 1$; these are also the isomorphisms of $\mathbb{Z}^+$ since they are injective. □

**Exercise 2.6.3.** *Show that the functions $f = 1/x$, $g = (x-1)/x$ generate a group of functions, the law of composition being composition of functions, that is isomorphic to the symmetric group $S_3$.*

*Solution.* We define

$$f_1 = x, \quad f_2 = \frac{1}{x}, \quad f_3 = 1 - x, \quad f_4 = \frac{1}{1-x}, \quad f_5 = \frac{x}{x-1}, \quad f_6 = \frac{x-1}{x}.$$

Then, we can construct the multiplication table:

| | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
|---|---|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
| $f_2$ | $f_2$ | $f_1$ | $f_4$ | $f_3$ | $f_6$ | $f_5$ |
| $f_3$ | $f_3$ | $f_6$ | $f_1$ | $f_5$ | $f_4$ | $f_2$ |
| $f_4$ | $f_4$ | $f_5$ | $f_2$ | $f_6$ | $f_3$ | $f_1$ |
| $f_5$ | $f_5$ | $f_4$ | $f_6$ | $f_2$ | $f_1$ | $f_3$ |
| $f_6$ | $f_6$ | $f_3$ | $f_5$ | $f_1$ | $f_2$ | $f_4$ |

This proves closure since every combination of factors is accounted for, identity since every row/column contains $e = f_1$, and associativity since associativity holds for composition of rational functions. We claim that this is isomorphic to $S_3$. This follows since if we let $f_1 \rightsquigarrow e$, $f_2 \rightsquigarrow (12)$, $f_6 \rightsquigarrow (123)$, we get the following table:

| | $e$ | (12) | (13) | (132) | (23) | (123) |
|---|---|---|---|---|---|---|
| $e$ | $e$ | (12) | (13) | (132) | (23) | (123) |
| (12) | (12) | $e$ | (132) | (13) | (123) | (23) |
| (13) | (13) | (123) | $e$ | (23) | (132) | (12) |
| (132) | (132) | (23) | (12) | (123) | (13) | $e$ |
| (23) | (23) | (132) | (123) | (12) | $e$ | (13) |
| (123) | (123) | (13) | (23) | $e$ | (12) | (132) |

This proves it is a homomorphism since all of the multiplications are accurate, and is an isomorphism since every element in $S_3$ is mapped to, with inverse defined by matching entries. This shows $f_2, f_6$ generate the group of functions since $(12), (123)$ generate $S_3$ as on p. 42. □

**Exercise 2.6.6.** *Are the matrices* $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}$ *conjugate elements of the group* $GL_2(\mathbb{R})$*? Are they conjugate elements of* $SL_2(\mathbb{R})$*?*

*Solution.* We explicitly calculate the conjugation for the conjugation matrix $A$:

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$
$$\begin{bmatrix} a_{11} & a_{11} + a_{12} \\ a_{21} & a_{21} + a_{22} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{11} + a_{21} & a_{12} + a_{22} \end{bmatrix}$$

This equality requires $a_{11} = 0$, $a_{12} = a_{21}$; however, we see that then $\det A < 0$ in this case, so the matrices are not conjugate in $SL_2(\mathbb{R})$.

We see that they are, however, conjugate elements of the group $GL_2(\mathbb{R})$, since

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$ □

## 2.8 Cosets

**Exercise 2.8.4.** *Does a group of order* 35 *contain an element of order* 5*? of order* 7*?*

*Solution.* Any element in $G$ has order in $\{1, 5, 7, 35\}$ by Cor. 2.8.10. Suppose $G$ had no elements of order 5; then, all non-identity elements must have order 7, for if $|x| = 35$, then $|x^7| = 5$. Let $h$ have order 7, and $H = \langle h \rangle$; since $|H| = 7$, pick $g \notin H$. Then, $g \neq e$ and has order 7. The left cosets $H, gH, g^2H, \ldots, g^6H$ must be disjoint, for, if $g^a h^i = g^b h^j$, then $g^{a-b} = h^{i-j}$, and so picking $r$ such that $r(a-b) \equiv 1 \bmod 7$, we have that $g = g^{r(a-b)} = h^{r(i-j)} \in H$, a contradiction. But this contradicts the counting formula (2.8.8), since $|G| = 35 \neq 49 = 7 \cdot 7 = |H|[G : H]$, and so $G$ contains an element of order 5.

Now suppose $G$ had no elements of order 7; then all non-identity elements have order 5 as before. Letting $h$ have order 5 and $H, g$ as before, the same argument gives that $H, gH, g^2H, \ldots, g^4H$ are disjoint left cosets in $G$. This contradicts the counting formula (2.8.8) again, since $|G| = 35 \neq 25 = 5 \cdot 5 = |H|[G : H]$, hence $G$ contains an element of order 7. □

**Exercise 2.8.8.** *Let $G$ be a group of order 25. Prove that $G$ has at least one subgroup of order 5, and that if it contains only one subgroup of order 5, then it is a cyclic group.*

*Proof.* Any element in $G$ has order in $\{1, 5, 25\}$ by Cor. 2.8.10. If $G$ had no elements of order 5, it must have an element $x$ of order 25, but then $|x^5| = 5$, hence $\langle x^5 \rangle$ is a subgroup of order 5.

Now suppose $H$ is the only subgroup of order 5 in $G$, and pick $x \notin H$. $x$ has order 5 or 25 by Cor. 2.8.10 again, and since $e \in H$. But $|x| = 5$ implies $H = \langle x \rangle$, hence $x \in H$, and so we know $|x| = 25$, i.e., $G = \langle x \rangle$ is cyclic. □

**Exercise 2.8.10.** *Prove that every subgroup of index 2 is a normal subgroup, and show by example that a subgroup of index 3 need not be normal.*

*Proof.* If $H \leqslant G$ with $[G : H] = 2$, we see that, picking $a \notin H$, $G = H \amalg aH = H \amalg Ha$, since this is the only we can form cosets of $a$ in $G$. Thus, $aH = Ha$, hence $H \lhd G$ by Prop. 2.8.17.

Now we consider $S_3$; the 2-cycle $y = (12)$ generates a subgroup $H$ of order 2, and therefore of index 3 by the counting formula (2.8.8). However, by the multiplication table constructed last week, we see that, from (2.8.4) and (2.8.16),

$$xH = \{x, xy\} \neq \{x, x^2y\} = Hx.$$ □

## 2.10 The Correspondence Theorem

**Exercise 2.10.3.** *Let $G$ and $G'$ be cyclic groups of orders 12 and 6, generated by elements $x$ and $y$, respectively, and let $\varphi\colon G \to G'$ be the map defined by $\varphi(x^i) = y^i$. Exhibit the correspondence referred to in the Correspondence Theorem explicitly.*

*Solution.* We note that $K = \ker \varphi = \{e, x^6\}$. The subgroups of $G$ that contain these are $\langle x \rangle, \langle x^2 \rangle, \langle x^3 \rangle, \langle x^6 \rangle$, and each correspond to $\langle y \rangle, \langle y^2 \rangle, \langle y^3 \rangle, e$ respectively, which are all the subgroups of $G'$. □

## 2.11 Product Groups

**Exercise 2.11.1.** *Let $x$ be an element of order $r$ of a group $G$, and let $y$ be an element of $G'$ of order $s$. What is the order of $(x, y)$ in the product group $G \times G'$?*

*Solution.* The order is $\operatorname{lcm}(r, s)$, since $(x, y)^n = (x^n, y^n) = (e, e)$ implies $r, s \mid n$. □

**Exercise 2.11.3.** *Prove that the product of two infinite cyclic groups is not infinite cyclic.*

*Proof.* Recall that a cyclic group must be generated by a single element; since all infinite cyclic groups are isomorphic to $\mathbb{Z}$, we can consider $\mathbb{Z} \times \mathbb{Z}$. Suppose that $(a, b)$ is this single element. But then, we see that $(2a, b)$ cannot be obtained from adding $(a, b)$ to itself, which implies that $\mathbb{Z} \times \mathbb{Z}$ is not infinite cyclic. □

## 2.12 Quotient Groups

**Exercise 2.12.2.** *In the general linear group $GL_3(\mathbb{R})$, consider the subsets*

$$H = \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}, \text{ and } K = \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

*where $*$ represents an arbitrary real number. Show that $H$ is a subgroup of $GL_3$, that $K$ is a normal subgroup of $H$, and identify the quotient group $H/K$. Determine the center of $H$.*

*Proof.* $H \leqslant GL_3$ since clearly $I \in H$,

$$\begin{bmatrix} 1 & a_{11} & a_{21} \\ 0 & 1 & a_{22} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b_{11} & b_{21} \\ 0 & 1 & b_{22} \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_{11} + b_{11} & a_{21} + b_{21} + a_{11}b_{22} \\ 0 & 1 & a_{22} + b_{22} \\ 0 & 0 & 1 \end{bmatrix} \in H,$$

and since

$$\begin{bmatrix} 1 & a_{11} & a_{21} \\ 0 & 1 & a_{22} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -a_{11} & -a_{21} + a_{11}a_{22} \\ 0 & 1 & -a_{22} \\ 0 & 0 & 1 \end{bmatrix} = I.$$

We now show that $K$ is a normal subgroup of $H$. Define $k_a$ as the matrix in $K$ that has the parameter $a$; we see $k_0 = I \in K$, $k_a k_b = k_{a+b}$, $k_a k_{-a} = I$, and so it only remains to show normality by showing $hk = kh$ for $h \in H, k \in K$, which is equivalent to $hkh^{-1} = k$:

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b_{11} & b_{21} \\ 0 & 1 & b_{22} \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b_{11} & a + b_{21} \\ 0 & 1 & b_{22} \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b_{11} & b_{21} \\ 0 & 1 & b_{22} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

By the additive nature of the $k_a$ relations, we see that $K \approx \mathbb{R}^+$.

The quotient group $H/K$ is then represented by matrices of the form

$$\begin{bmatrix} 1 & b & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix},$$

i.e., the cosets are these times $K$, since multiplying by $k_a$ only alters the top-right entry, and so multiplying by $k_a$ will keep $b, c$ constant, and therefore remain in the same coset. Moreover, this generates the entire space since we can multiply arbitrary $k_a$ to a coset with arbitrary parameters $b, c$.

The center of $H$ contains $K$, since $K$ commutes with elements of $H$ as shown above; we claim the center is solely $K$. If $A, B \in H$, then by the above $AB = BA$ is

$$\begin{bmatrix} 1 & a_{11}+b_{11} & a_{21}+b_{21}+a_{11}b_{22} \\ 0 & 1 & a_{22}+b_{22} \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_{11}+b_{11} & a_{21}+b_{21}+a_{22}b_{11} \\ 0 & 1 & a_{22}+b_{22} \\ 0 & 0 & 1 \end{bmatrix}.$$

This implies $a_{11}b_{22} = a_{22}b_{11}$. But if $A$ is fixed and $B$ is an arbitrary matrix in $H$, then $a_{11}b_{22} = a_{22}b_{11}$ must hold for all matrices $B$, and so $a_{11} = a_{22} = 0$, hence $A \in K$. Thus, the center of $H$ is $K \approx \mathbb{R}^+$. □

**Exercise 2.12.4.** *Let $H = \{\pm 1, \pm i\}$ be the subgroup of $G = \mathbb{C}^\times$ of fourth roots of unity. Describe the cosets of $H$ in $G$ explicitly. Is $G/H$ isomorphic to $G$?*

*Solution.* By (2.8.5), cosets $aH, bH$ are equal if and only if $b = ah$ for some $h \in H$, and so if $a = re^{2\pi i\theta}, b = se^{2\pi i\eta}$ for $r, s \in \mathbb{R}_{>0}$, $\theta, \eta \in [0, 1)$, then $aH = bH$ if and only if $r = s$ and $\theta - \eta \in \{0, 1/4, 1/2, 3/4\}$. Hence the cosets of $H$ are $\{re^{2\pi\theta}H \mid r \in \mathbb{R}_{>0},\ \theta \in [0, 1/4)\}$.

Now consider the map $\varphi\colon G \to G, x \rightsquigarrow x^4$. Then, this is trivially a homomorphism of $G$; it is moreover surjective since any nonzero complex number has a fourth root. We see that $\ker\varphi = H$, and so $G/H \approx G$ by the isomorphism theorem. □

**Exercise 2.12.5.** *Let $G$ be the group of upper triangular real matrices $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, with $a$ and $d$ different from zero. For each of the following subsets, determine whether or not $S$ is a subgroup, and whether or not $S$ is a normal subgroup. If $S$ is a normal subgroup, identify the quotient group $G/S$.*

(*i*) *$S$ is the subset defined by $b = 0$.*
(*ii*) *$S$ is the subset defined by $d = 1$.*
(*iii*) *$S$ is the subset defined by $a = d$.*

*Solution for* $(i)$. $S \leqslant G$ since the diagonal entries would multiply with each other and not affect the other entries of the matrices, $I \in S$, and the inverse can be found by letting the inverse have entries $a^{-1}, d^{-1}$. $S$ is not a normal subgroup since

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}a & 0\\ 0 & d\end{bmatrix} = \begin{bmatrix}a & d\\ 0 & d\end{bmatrix} \neq \begin{bmatrix}a & a\\ 0 & d\end{bmatrix} = \begin{bmatrix}a & 0\\ 0 & d\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}. \qquad \square$$

*Solution for* $(ii)$. This forms a subgroup since

$$\begin{bmatrix}a & b\\ 0 & 1\end{bmatrix}^{-1} = \begin{bmatrix}1/a & -b/a\\ 0 & 1\end{bmatrix},$$

implies it is closed under inversion, and

$$\begin{bmatrix}a & b\\ 0 & 1\end{bmatrix}\begin{bmatrix}a' & b'\\ 0 & 1\end{bmatrix} = \begin{bmatrix}aa' & ab'+b\\ 0 & 1\end{bmatrix},$$

implies it is closed under multiplication; the identity is trivially in $S$.

We now see that it is a normal subgroup:

$$\begin{bmatrix}a & b\\ 0 & d\end{bmatrix}\begin{bmatrix}a' & b'\\ 0 & 1\end{bmatrix}\begin{bmatrix}1/a & -b/ad\\ 0 & 1/d\end{bmatrix} = \begin{bmatrix}a' & (b+ab'-a'b)/d\\ 0 & 1\end{bmatrix} \in S.$$

We see that the quotient group $G/S$ would be represented by matrices of the form

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

for $d \in \mathbb{R}^\times$ since this would cover all of $G$:

$$\begin{bmatrix}1 & 0\\ 0 & d\end{bmatrix}\begin{bmatrix}a & b\\ 0 & 1\end{bmatrix} = \begin{bmatrix}a & b\\ 0 & d\end{bmatrix},$$

and since each matrix of the form above gives a different coset because multiplying by elements in $S$ keep $d$ constant. $\square$

*Solution for* $(iii)$. This is a subgroup since it satisfies closure:

$$\begin{bmatrix}a & b\\ 0 & a\end{bmatrix}\begin{bmatrix}c & d\\ 0 & c\end{bmatrix} = \begin{bmatrix}ac & bc+ad\\ 0 & ac\end{bmatrix} \in S,$$

inverse:

$$\begin{bmatrix}a & b\\ 0 & a\end{bmatrix}^{-1} = \begin{bmatrix}1/a & -b/a^2\\ 0 & 1/a\end{bmatrix} \in S,$$

and clearly the identity is in $S$.

We now check this subgroup is normal:

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} a' & b' \\ 0 & a' \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}^{-1} = \begin{bmatrix} a' & ab'/d \\ 0 & a' \end{bmatrix} \in S.$$

The quotient group $G/S$ would be represented by matrices of the form

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

for $d \in \mathbb{R}^\times$ since this would cover all of $G$:

$$\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & ad \end{bmatrix},$$

and since each matrix of the form above gives a different coset since multiplying by elements in $S$ cannot give another matrix of the same form unless $d$ is the same. □

# 6 Symmetry

## 6.3 Isometries of the Plane

**Exercise 6.3.2.** *Let $m$ be an orientation-reversing isometry. Prove algebraically that $m^2$ is a translation.*

*Proof.* By Thm. 6.3.2 and (6.3.3), $m^2 = t_v \rho_\theta r t_v \rho_\theta r = t_v \rho_\theta r t_v r \rho_{-\theta} = t_v \rho_\theta t_{v'} \rho_{-\theta} = t_{v+v''}$, where $v'' = \rho_\theta(r(v))$. □

**Exercise 6.3.6.**

(a) *Let $s$ be the rotation of the plane with angle $\pi/2$ about about the point $(1,1)^t$. Write the formula for $s$ as a product $t_a \rho_\theta$.*

(b) *Let $s$ denote reflection of the plane about the vertical axis $x = 1$. Find an isometry $g$ such that $grg^{-1} = s$, and write $s$ in the form $t_a \rho_\theta r$.*

*Solution for (a).* By (6.3.3),

$$s = t_{(1,1)} \rho_{\pi/2} t_{(-1,-1)} = t_{(1,1)} t_{\rho_{\pi/2}(-1,-1)} \rho_{\pi/2} = t_{(2,0)} \rho_{\pi/2}.$$ □

*Solution for (b).* By (6.3.3), letting $g = t_{1,0} \rho_{\pi/2}$,

$$s = grg^{-1} = t_{(1,0)} \rho_{\pi/2} r \rho_{-\pi/2} t_{(-1,0)} = t_{(1,0)} \rho_\pi r t_{(-1,0)} = t_{(1,0)} \rho_\pi t_{(-1,0)} r = t_{(2,0)} \rho_\pi r.$$ □

## 6.4 Finite Groups of Orthogonal Operators on the Plane

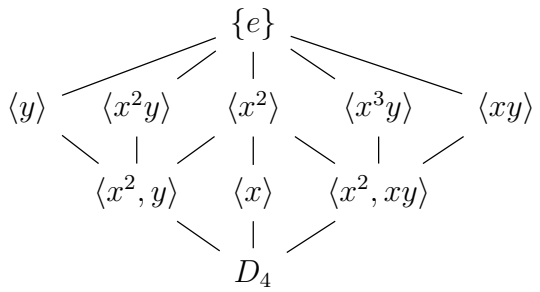
**Exercise 6.4.2.**

(a) *List all subgroups of the dihedral group $D_4$, and decide which ones are normal.*

(b) *List the proper normal subgroups $N$ of the dihedral group $D_{15}$, and identify the quotient groups $D_{15}/N$.*

(c) *List the subgroups of $D_6$ that do not contain $x^3$.*

*Solution for (a).* We claim the subgroups of $D_4$ form the lattice diagram




By Lagrange's theorem (Thm. 2.8.9), any subgroup $H \leqslant D_4$ must have $|H| \in \{1, 2, 4, 8\}$. $\{e\}$ is the unique order 1 subgroup. The order 2 subgroups are generated by one order 2 element, hence are given by the second row above. The order 4 subgroups are either generated by an order 4 element or by two order 2 elements; these give the third row. Finally, $D_4$ is the unique order 8 subgroup.

We claim the normal subgroups of $D_4$ are

$$\{e\}, \langle x\rangle, \langle x^2\rangle, \langle x^2, y\rangle, \langle x^2, xy\rangle, D_4.$$

$\langle x^2\rangle$ is normal since $x^2$ commutes with all other elements of $D_4$; the other proper subgroups are normal because they are of index 2 by the counting formula (2.8.8), and by Exercise 2.8.10. Lastly, the other four subgroups in the second row of the diagram above are not normal since they are not closed under conjugation by $x$. □

*Solution for (b).* Any proper subgroup $H \leqslant D_{15}$ must have $|H| \in \{2, 3, 5, 15\}$ by Lagrange's theorem (Thm. 2.8.9). The order 2 subgroups are of the form $\langle x^i y\rangle$; these are not normal since they are not closed under conjugation by $x$. Since $2 \nmid 3, 5, 15$, we know no other subgroup contains an element of the form $x^i y$. Thus, every normal subgroup of $D_{15}$ must be of the form $\langle x^i\rangle$ for $i = 1, 3, 5$, since any other $i$ gives a subgroup equal to one of these three. These are all in fact normal subgroups since they are kernels of homomorphisms $D_{15} \to D_i$ for $i = 1, 3, 5$ mapping $x \rightsquigarrow x, y \rightsquigarrow y$.

By the first isomorphism theorem (Thm. 2.12.10), this implies the quotient groups for each nontrivial $N$ are isomorphic to

$$D_{15}/\langle x\rangle \approx D_1, \quad D_{15}/\langle x^3\rangle \approx D_3, \quad D_{15}/\langle x^5\rangle \approx D_5. \qquad \square$$

*Solution for* $(c)$. By Lagrange's theorem (Thm. 2.8.9), any subgroup $H \leqslant D_6$ must have $|H| \in \{1, 2, 3, 4, 6, 12\}$. $\{e\}$ is the unique order 1 subgroup, and does not contain $x^3$. The order 2 subgroups are $\langle x^3\rangle$ and $\langle x^i y\rangle$ for $0 \leq i \leq 5$; only the first contains $x^3$. The unique order 3 subgroup is $\langle x^2\rangle$, which does not contain $x^3$. The order 4 subgroups not containing $x^3$ are of the form $\langle x^i y, x^j y\rangle$ for $i \neq j$ since $D_6$ contains no elements of order 4, but this subgroup is of order 4 if and only if $x^{j-i} = x^3 = x^{i-j}$, hence there are no order 4 subgroups not containing $x^3$. The order 6 subgroups must be generated by an order 2 and an order 3 element, hence those not containing $x^3$ are of the form $\langle x^2, x^i y\rangle$. But different choices $i, j$ for $i$ give the same subgroup if and only if $i \equiv j \bmod 2$, hence the only subgroups of order 6 not containing $x^3$ are $\langle x^2, y\rangle$ and $\langle x^2, xy\rangle$. The unique order 12 subgroup $D_{16}$ contains $x^3$. In summary, the subgroups that do not contain $x^3$ are

$$\{e\}, \langle y\rangle, \langle xy\rangle, \langle x^2 y\rangle, \langle x^3 y\rangle, \langle x^4 y\rangle, \langle x^5 y\rangle, \langle x^2\rangle, \langle x^2, y\rangle, \langle x^2, xy\rangle. \qquad \square$$

**Exercise 6.4.3.**

$(a)$ *Compute the left cosets of the subgroup* $H = \{1, x^5\}$ *in the dihedral group* $D_{10}$.
$(b)$ *Prove that* $H$ *is normal and that* $D_{10}/H$ *is isomorphic to* $D_5$.
$(c)$ *Is* $D_{10}$ *isomorphic to* $D_5 \times H$*?*

*Solution for* $(a)$. The cosets are represented by $e, x, x^2, x^3, x^4, y, xy, x^2 y, x^3 y, x^4 y$. $\square$

*Solution for* $(b)$. To show that $H$ is normal, it suffices to show $x^5$ commutes with every element of $D_{10}$: it trivially commutes with $x$, and with $y$ since $yx^5 y = yyx^5 = x^5$. Thus $H \lhd D_{10}$.

Now the surjective homomorphism $D_{10} \to D_5$ sending $x \rightsquigarrow x, y \rightsquigarrow y$ has kernel $H$, hence $D_{10}/H \approx D_5$ by the first isomorphism theorem (Thm. 2.12.10). $\square$

*Solution for* $(c)$. Note $D_5 \hookrightarrow D_{10}$ by having $x \rightsquigarrow x^2$, hence to show $D_{10} \approx D_5 \times H$, it suffices by Prop. 2.11.4$(d)$ to show $H \bigcap D_5 = \{e\}$, $HD_5 = G$, and $H, D_5 \lhd G$ with this embedding of $D_5$. The normality of both groups follows by $(b)$ and since $D_5$ is of index 2 in $G$ (Exercise 2.8.10). Their intersection is $e$ since $x^5 \notin D_5$. $HD_5 = G$ since $x^5$ commutes with every element of $D_5 \subset D_{10}$ by $(b)$, and so we can get any element of the form $x^i, x^i y$ for $0 \leq i \leq 9$. $\square$

## 6.5 Discrete Groups of Isometries

**Exercise 6.5.5.** *Prove that the group of symmetries of the frieze pattern* $\lhd \lhd \lhd \lhd \lhd \lhd \lhd \lhd$ *is isomorphic to the direct product* $C_2 \times C_\infty$ *of a cyclic group of order* 2 *and an infinite cyclic group.*

*Proof.* Let $G \leqslant M$ be the group of symmetries. By Thm. 6.3.2, any symmetry arises as $t_v\rho_\theta$ or $t_v\rho_\theta r$ where $t_v$ are translations, $\rho_\theta$ are rotations, and $r$ are reflections across the $x$-axis. In both cases, $\theta$ must be zero to be a symmetry, and $v$ must be an integer multiple of the length of $\lhd$. Hence the group $C_2$ of reflections across the $x$-axis and the group $C_\infty$ of translations by integer multiples of lengths of $\lhd$ generate $G$.

We claim $C_2 \times C_\infty \approx G$. Since clearly $C_2 \cap C_\infty = \{e\}$, by Prop. 2.11.4$(d)$ it only remains to show $C_2, C_\infty \lhd G$. $C_\infty \lhd G$ since it has index 2 in $G$ by the classification of symmetries above, and then by Exercise 2.8.10. $C_2 \lhd G$ since our translations all lie on the $x$-axis, and then by using (6.3.3). □

**Exercise 6.5.9.** *Let* $G$ *be a discrete subgroup of* $M$ *whose translation group is not trivial. Prove that there is a point* $p_0$ *in the plane that is not fixed by any element of* $G$ *except the identity.*

*Proof.* We first claim that the set of points fixed by any nontrivial isometry $m \in G$ has Lebesgue measure zero. We proceed by considering each kind of isometry in Thm. 6.3.4. If $m$ is a nontrivial translation, then there are no fixed points. If $m$ is a nontrivial rotation around a point $p$, then $p$ is a fixed point. If $m$ is a nontrivial reflection about a line $\ell$, then any point on $\ell$ is a fixed point. If $m$ is a nontrivial glide, then $m$ has no fixed points. Thus, in all cases the set of fixed points has Lebesgue measure zero in $\mathbb{R}^2$.

Now for each $m \neq e$, let $F_m$ be the set of fixed points of $m$; by the above, it has Lebesgue measure zero. We claim there are only countably many $m \in G$. By Thm. 6.3.2, any $m$ is of the form $t_v\rho_\theta$ or $t_v\rho_\theta$. By Thm. 6.5.5, there are only countably many $t_v$. By Prop. 6.5.10, there are only finitely many $\rho_\theta$ and $\rho_\theta r$. Thus, there are only countably many $m \in G$.

Finally, the set of all points fixed by some nontrivial element of $G$ has Lebesgue measure

$$\mu\left(\bigcup_{e\neq m\in G} F_m\right) \leq \sum_{e\neq m\in G} \mu(F_m) = 0,$$

hence almost all points in $\mathbb{R}^2$ are not fixed by any nontrivial element of $G$. □

## 6.6 Plane Crystallographic Groups

**Exercise 6.6.2.** *Let $G$ be the group of symmetries of an equilateral triangular lattice $L$. Determine the index in $G$ of the subgroup of translations in $G$.*

*Proof.* The index of translations is given by $[G : T]$. By Theorem 6.3.2, we see that every isometry should be given by $t_v \rho_\theta r$; we therefore want the cardinality of the set of $\rho_\theta r$'s. But this is exactly the set $D_3$, and so $[G : T] = |D_3| = 6$. □

## 6.7 Abstract Symmetry: Group Operations

**Exercise 6.7.1.** *Let $G = D_4$ be the dihedral group of symmetries of the square.*

(*a*) *What is the stabilizer of a vertex? of an edge?*

(*b*) *$G$ operates on the set of two elements consisting of the diagonal lines. What is the stabilizer of a diagonal?*

*Solution for* (*a*). If the vertex lies along the axis of reflection for $y$, $\{e, y\}$ is the stabilizer. If it does not, $\{e, x^2y\}$ is the stabilizer. If the given edge lies immediately to the $+\theta$ direction of the line of reflection, the stabilizer is $\{e, xy\}$. If it does not, $\{e, x^3y\}$ is the stabilizer. □

*Solution for* (*b*). The stabilizer of the diagonal is $\{e, x^2, y, x^2y\}$. □

**Exercise 6.7.2.** *The group $M$ of isometries of the plane operates on the set of lines in the plane. Determine the stabilizer of a line.*

*Solution.* It suffices to consider the classes of isometries in Thm. 6.3.4. The stabilizer of a line $\ell$ consists of translations along $\ell$, rotations of an angle $\pi$ about a point $p \in \ell$, reflections about $\ell$, and glide reflections about $\ell$. □

**Exercise 6.7.8.** *Decompose the set $\mathbb{C}^{2\times2}$ of $2\times2$ matrices into orbits for the following operations of $GL_2(\mathbb{C})$:*

(*a*) *left multiplication,*

(*b*) *conjugation.*

*Solution* (*a*). Left multiplication by elements of $GL_2(\mathbb{C})$ corresponds to products of elementary row operations on matrices in $\mathbb{C}^{2\times2}$. By row reduction, we know that applying elementary row operations on a given matrix in $\mathbb{C}^{2\times2}$ gives a unique matrix of one of the following forms:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & a \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Thus, $\mathbb{C}^{2\times 2}$ decomposes as

$$\left(GL_2(\mathbb{C})\cdot\begin{bmatrix}1&0\\0&1\end{bmatrix}\right)\amalg\left(\coprod_{a\in\mathbb{C}}GL_2(\mathbb{C})\cdot\begin{bmatrix}1&a\\0&0\end{bmatrix}\right)\amalg\left(GL_2(\mathbb{C})\cdot\begin{bmatrix}0&1\\0&0\end{bmatrix}\right)\amalg\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix}\right\}.\ \square$$

*Solution* $(b)$. Since every matrix is conjugate (similar) to a unique Jordan form (up to ordering of Jordan blocks), we have that the orbits are generated by the different Jordan forms, i.e., $\mathbb{C}^{2\times 2}$ decomposes as

$$\left(\coprod_{\lambda\in\mathbb{C}}GL_2(\mathbb{C})*\begin{bmatrix}\lambda&1\\0&\lambda\end{bmatrix}\right)\amalg\left(\coprod_{\lambda_1\geq\lambda_2,\lambda_i\in\mathbb{C}}GL_2(\mathbb{C})*\begin{bmatrix}\lambda_1&0\\0&\lambda_2\end{bmatrix}\right).\qquad\square$$

**Exercise 6.7.11.** *Prove that the only subgroup of order* 12 *of the symmetric group* $S_4$ *is the alternating group* $A_4$.

*Proof.* We first prove a lemma: If $H$ is a subgroup of $G$, then $H$ is normal if and only if $H$ is the union of conjugacy classes in $G$. But $H$ is normal if and only if it is closed under conjugation if and only if $H=\bigcup_{h\in H}G*h$.

Now suppose $H\leqslant S_4$ has order 12. Then, by the counting formula (2.8.8), $|S_4|=24=12\cdot[S_4:H]=|H|[S_4:H]$ implies $[S_4:H]=2$, and so $H\lhd S_4$ by Exercise 2.8.10. So, we use the classification of conjugacy classes in $S_4$ from p. 201, following Prop. 7.5.1:

| Partition | Element | No. in Conj. Class |
|---|---|---|
| $1+1+1+1$ | $e$ | $1$ |
| $2+1+1$ | $(ab)$ | $\binom{4}{2}=6$ |
| $2+2$ | $(ab)(cd)$ | $\frac{1}{2}\binom{4}{2}=3$ |
| $3+1$ | $(abc)$ | $2\cdot\binom{4}{3}=8$ |
| $4$ | $(abcd)$ | $3!=6$ |

Now if $H\lhd S_4$ has order 12, it must arise from a union of conjugacy classes above including $\{e\}$ (since it is a subgroup), but the only way this is possible is the sum $1+3+8=12$. The conjugacy classes associated with these terms are exactly the even permutations in $S_4$, which form the subgroup $A_4$, and so $A_4$ is the only subgroup of order 12 in $S_4$. $\square$

## 6.8 The Operation on Cosets

**Exercise 6.8.4.** *Let* $H$ *be the stabilizer of the index* $\mathbf{1}$ *for the operation of the symmetric group* $G=S_n$ *on the set of indices* $\{\mathbf{1},\dots,\mathbf{n}\}$. *Describe the left cosets of* $H$ *in* $G$ *and the map* (6.8.4) *in this case.*

*Solution.* We see that $H$ consists of all cycles that hold $\mathbf{1}$ fixed, i.e., permutations of the remaining $n-1$ elements, hence is isomorphic to $S_{n-1}$. We claim

$$G/H = \{(\mathbf{1i})H \mid \mathbf{i} \in \{\mathbf{1}, \dots, \mathbf{n}\}\}$$

Each $(\mathbf{1i})$ gives a different coset since no $(\mathbf{1i})H$ contains $(\mathbf{1j})$ for $\mathbf{i} \neq \mathbf{j}$, and then by (2.8.5). These are all the cosets since by Pop. 6.8.4, $|G/H| = |O_{\mathbf{1}}| = n$. Thus, the map $\epsilon\colon G/H \to O_{\mathbf{1}}$ is the map $(\mathbf{1i}) \rightsquigarrow \mathbf{i}$. □

## 6.9 The Counting Formula

**Exercise 6.9.4.** *Identify the group $T'$ of all symmetries of a regular tetrahedron, including orientation-reversing symmetries.*

*Solution.* $T' \leqslant O_3(\mathbb{R})$ operates transitively on the set $F$ of faces of order 4, hence is given by a permutation of the set $\{f_1, f_2, f_3, f_4\}$, and so there is a homomorphism $T' \to S_4$ by Prop. 6.11.2. This is injective since if $t \in T'$ fixes three faces, then it fixes the three vectors defining the centers of each face, hence is the identity matrix in $O_3(\mathbb{R})$. We claim this homomorphism $T' \to S_4$ is surjective, hence an isomorphism; it suffices to show $|T'| = 24$. But the stabilizer $G_f$ of a given face $f$ is the group $D_3$ generated by a rotation by $2\pi/3$ about the center of $f$ and a reflection about an axis in $f$; $|D_3| = 6$, and so the counting formula (6.9.2) gives $|T'| = 6 \cdot 4 = 24$, hence $T' \approx S_4$. □

## 6.10 Operations on Subsets

**Exercise 6.10.1.** *Determine the orders of the orbits for left multiplication on the set of subsets of order 3 of $D_3$.*

*Solution.* We know that there are $\binom{6}{3} = 20$ subsets of order 3 of $D_3$; we also know by the counting formula (6.9.2) that there can only be orbits of order $1, 2, 3, 6$ since only these divide $|D_3|$. We see that only the subset $\{e, x, x^2\}$ is a subgroup, which produces the orbit $\{e, x, x^2\}, \{y, yx, yx^2\}$. The other 18 subsets form 3 orbits of order 6 of $D_3$. Letting $H_1 = \{e, x, y\}$, we have

$$\begin{aligned} H_1 &= \{e, x, y\}, & xH_1 &= \{x, x^2, yx^2\}, & x^2H_1 &= \{x^2, e, yx\}, \\ yH_1 &= \{y, yx, e\}, & yxH_1 &= \{yx, yx^2, x^2\}, & yx^2H_1 &= \{y, yx^2, x\}. \end{aligned}$$

Letting $H_2 = \{e, x, yx\}$, we have

$$\begin{aligned} H_2 &= \{e, x, yx\}, & xH_2 &= \{x, x^2, y\}, & x^2H_2 &= \{x^2, e, yx^2\}, \\ yH_2 &= \{y, yx, x\}, & yxH_2 &= \{yx, yx^2, e\}, & yx^2H_2 &= \{y, yx^2, x^2\}. \end{aligned}$$

Letting $H_3 = \{e, x, yx^2\}$, we have

$$\begin{aligned} H_3 &= \{e, x, yx^2\}, & xH_3 &= \{x, x^2, yx\}, & x^2H_3 &= \{x^2, e, y\}, \\ yH_3 &= \{y, yx, x^2\}, & yxH_3 &= \{yx, yx^2, x\}, & yx^2H_3 &= \{y, yx^2, e\}. \end{aligned}$$

We therefore have one orbit of order 2 and three orbits of order 6; this means we have $1 \times 2 + 3 \times 6 = 20$ subsets in these orbits, and so we have found all of them. □

## 6.11 Permutation Representations

**Exercise 6.11.1.** *Describe all the ways in which $S_3$ can operate on a set of four elements.*

*Solution.* By Cor. 6.11.3, it suffices to find all homomorphisms $f\colon S_3 \to S_4$. Recall from p. 42 that $S_3$ is generated by $x = (123), y = (12)$; a homomorphism $f$ is then fully determined by specifying $f(x), f(y)$. We moreover note that $x^3 = e, y^2 = e$ implies $f(x)^3 = f(y)^2 = e$, hence $f(x) = e$ or is one of the eight 3-cycles in $S_4$ by the classification in Exercise 6.7.11; similarly, $f(y) = e$ or is one of the nine elements of order 2 in the table from Exercise 6.7.11.

If $f(x) = e$, then there is no restriction on $f(y)$, thus there are ten homomorphisms $f$ of this kind.

If $f(x) = (abc)$, then since $yx$ has order 2, $f(yx)^2 = f(y)^2 f(x)^2 = e$. Thus $f(y) \neq e$. Now suppose $f(y)$ acts nontrivially on the fourth element $d$ unaffected by $f(x)$; then without loss of generality, $f(y)$ interchanges $a, d$, and so $f(yx) \cdot d = a$. Hence $f(yx)$ must map $a \rightsquigarrow d$ as well, and so $f(y) \cdot b = d$. But then $f(y)^2 \cdot b = a \neq b$, contradicting that $f(y)$ has order 2. Hence $f(y)$ is a permutation of order 2 of the subset $\{a, b, c\}$, which are 2-cycles; assume without loss of generality that $f(y) = (ab)$. In the argument above, there are 4 choices for the fixed point $d$ of $f(x)$, 3 choices for the fixed point of $f(y)$, and two choices for $a = f(x) \cdot c$. Each choice gives a homomorphism $f$ by just renaming $a, b, c$ as $1, 2, 3$, hence realizing $f$ as the canonical operation of $S_3$ on the subset $\{1, 2, 3\} \subset \{1, 2, 3, 4\}$. Thus, there are 24 homomorphisms $f$ such that $f(x) \neq e$. □

**Exercise 6.11.5.** *A group $G$ operates faithfully on a set $S$ of five elements, and there are two orbits, one of order 3 and one of order 2. What are the possible groups?*
Hint: *Map $G$ to a product of symmetric groups.*

*Solution.* Let $S = \{1, 2, 3, 4, 5\}$ such that the two orbits are $O_3 = \{1, 2, 3\}$, $O_2 = \{4, 5\}$, respectively. $G$ operates on $O_3, O_2$ separately, hence the action of $G$ on $O_3, O_2$ respectively correspond to group homomorphisms $f_3\colon G \to S_3$ and $f_2\colon G \to$

$S_2$. This defines a group homomorphism $f = (f_3, f_2)\colon G \to S_3 \times S_2$ defined by $g \rightsquigarrow (f_3(g), f_2(g))$. Since $G$ acts faithfully on $S$, $g$ is injective, hence $G \approx f(G)$ by Cor. 2.12.11. Now the only group that acts transitively on $O_2$ is $S_2$ itself, and so $f_2(G) \approx S_2$. On the other hand, there are two groups that act transitively on $O_3$: $C_3$ and $S_3$. Hence $G \approx C_3 \times S_2$ or $S_3 \times S_2$. □

**Exercise 6.11.6.** *Let $F = \mathbb{F}_3$. There are four one-dimensional subspaces of the space of column vectors $F^2$. List them. Left multiplication by an invertible matrix permutes these subspaces. Prove that this operation defines a homomorphism $\varphi\colon GL_2(F) \to S_4$. Determine the kernel and the image of this homomorphism.*

*Proof.* We have the following one-dimensional subspaces, denoting $F = \{0, 1, 2\}$:

$$V_1 = \left\{ \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}2\\0\end{bmatrix} \right\}, \quad V_2 = \left\{ \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}0\\2\end{bmatrix} \right\}, \quad V_3 = \left\{ \begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}2\\2\end{bmatrix} \right\}, \quad V_4 = \left\{ \begin{bmatrix}2\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix} \right\}.$$

Call $e_i$ the first listed vector in $V_i$; note that $V_i = \{e_i, 2e_i\}$. These are all the subspaces in $F^2$ since there are only $3 \cdot 3 - 1 = 8$ nontrivial vectors in $F^2$.

Left multiplication by an invertible matrix defines an action on the vectors in $F^2$ since left multiplication by matrices in $F$ is associative, and since the identity matrix defines the trivial action; this descends to a well-defined action on the subspaces $V_i$ since the span of $Ae_i$ is equal to the span of $2Ae_i$ for any $A \in GL_2(F)$. Hence, by Cor. 6.11.3, this action defines a homomorphism $\varphi\colon GL_2(F) \to S_4$.

Now $\ker\varphi = \{I, 2I\}$ since $\supset$ clearly holds, and for $A \in GL_2(F)$, $Ae_1 \in V_1$ implies the first column of $A$ is either $e_1$ or $2e_1$, $Ae_2 \in V_2$ implies the second column of $A$ is either $e_2$ or $2e_2$, and $Ae_3 \in V_3$ implies that the coefficients on $e_i$ in each column have to be the same, hence $A = I$ or $2I$.

We claim $\operatorname{im}\varphi = S_4$. By Cor. 2.8.13, we have $|GL_2(F)| = |\ker\varphi||\operatorname{im}\varphi|$, and since $|S_4| = 24$ and $|\ker\varphi| = 2$ from above, it suffices to show $|GL_2(F)| = 48$. Now every matrix in $GL_2(F)$ consists of a pair of linearly independent vectors in $F_2$; there are $8 \cdot 6 = 48$ of these pairs by the above decomposition of $F_2$ into subspaces, hence $|GL_2(F)| = 48$. □

## 6.12 Finite Subgroups of the Rotation Group

**Exercise 6.12.3.** *Let $O$ be the group of rotations of a cube, and let $S$ be the set of four diagonal lines connecting opposite vertices. Determine the stabilizer of one of the diagonals.*

*Solution.* $O$ acts on $S$, hence there is a homomorphism $O \to S_4$ by Prop. 6.11.2. We first show this homomorphism is injective. If $s \in O$ fixes all four diagonals, then $s$ either fixes or interchanges the two endpoints of each diagonal. If $s \neq e$, i.e., it acts nontrivially on the vertexes, then we can pick three pairs of opposite vertexes such that $s$ interchanges one of the pairs of vertexes, or such that $s$ interchanges all three pairs of vertexes. In either case, give $\mathbb{R}^3$ a basis that points along the three diagonals connecting these pairs of vertexes; then the matrix for $s$ in this basis has an odd number of $-1$'s on the diagonal, and so has determinant $-1$, contradicting that $O \leqslant SO_3(\mathbb{R})$. The homomorphism $O \to S_4$ is surjective, since looking at the faces of the cube, $O$ acts transitively on the set of faces, and each face has stabilizer $C_4$, hence $|O| = |O_f||O \cdot f| = 4 \cdot 6 = 24$ by the counting formula (6.9.2).

Now we know $O$ acts like $S_4$ on the set of diagonals, hence the stabilizer of one of the diagonals is the same as fixing one index in the set of indexes $\{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}\}$ as in Exercise 6.8.4, hence is equal to $S_3$. □

**Exercise 6.12.7.** *The* 12 *points* $(\pm 1, \pm\alpha, 0)^t$, $(0, \pm 1, \pm\alpha)^t$, $(\pm\alpha, 0, \pm 1)^t$ *form the vertices of a regular icosahedron if* $\alpha > 1$ *is chosen suitably. Verify this, and determine* $\alpha$*.*

*Proof.* We have that the 12 points form three categories of the form above. By the distance formula, if they are in the same category, we have three possibilities for square distances:

| Vertex | Change sign of 1 | Change sign of $\alpha$ | Change sign of both |
|---|---|---|---|
| Square Distance | 4 | $4\alpha^2$ | $4(\alpha^2+1)$ |

If they are in different categories, then we have two possibilities for square distances. If our coordinates are $(x_1, x_2, x_3)$ and $(y_1, y_2, y_3)$, then there is only one $i$ such that $x_i, y_i \neq 0$, and $x_i, y_i$ must have different absolute values for each $i$, giving the table

| Vertex | $x_i, y_i$ have same sign | $x_i, y_i$ have differing sign |
|---|---|---|
| Square Distance | $2(\alpha^2-\alpha+1)$ | $2(\alpha^2+\alpha+1)$ |

where for a given vertexes, there are four vertexes each with square distance of each form above.

We now find $\alpha$. There must be five vertexes of shortest distance from $v_0$; by comparing the possible distances above, this shortest square distance must be equal to both 4 and $2(\alpha^2-\alpha+1)$. This gives the equation

$$2(\alpha^2-\alpha+1) = 4 \implies \alpha^2-\alpha-1 = 0 \implies \alpha = \frac{1+\sqrt{5}}{2}$$

by choosing the root greater than 1. This shows each vertex has exactly five neighbors of distance 2 away from it; we claim that the polyhedron formed by connecting vertexes of distance 2 away from each other forms an icosahedron.

Now we show each face formed by the edges is a congruent equilateral triangle. This is true since any face is formed by neighboring vertexes, which are distance 2 away from each other by the above. Each vertex moreover has the same number of faces meeting there since every vertexes has exactly five neighbors by the above.

Finally, suppose we have two neighboring vertexes $v, v'$ forming an edge; we claim there are only two faces intersecting at that edge. It suffices to show there are only two vertexes $w$ that are of distance 2 from both. Suppose $v_i = v_i' = 0$; in the following, we consider subscripts mod 3. Then $v_{i+1} = -v_{i+1}'$ with absolute value 1, so $w_{i+1} = 0, |w_{i+2}| = 1, |w_i| = 3$ by the table above. Next $v_{i+2} = v_{i+2}'$, hence $w_{i+2}$ must have the same sign as $v_{i+2}, v_{i+2}'$. Finally, $w_i$ can have either sign since $v_i = v_i' = 0$, hence there are only two vertexes that are of distance 2 from $v, v'$. □

## 6.M Miscellaneous Problems

**Exercise 6.M.7.** *Let $G$ be a finite group operating on a finite set $S$. For each element $g$ of $G$, let $S^g$ denote the subset of elements of $S$ fixed by $g$: $S^g = \{s \in S \mid gs = s\}$, and let $G_s$ be the stabilizer of $s$.*

(a) *We may imagine a true-false table for the assertion that $gs = s$, say with rows indexed by elements of $G$ and columns indexed by elements of $S$. Construct such a table for the action of the dihedral group $D_3$ on the vertices of a triangle.*
(b) *Prove the formula $\sum_{s\in S}|G_s| = \sum_{g\in G}|S^g|$.*
(c) *Prove* Burnside's Formula: $|G| \cdot (\textit{number of orbits}) = \sum_{g\in G}|S^g|$.

*Solution for (a).* We construct the true-false table:

| | $s_1$ | $s_2$ | $s_3$ |
|---|---|---|---|
| $e$ | True | True | True |
| $x$ | False | False | False |
| $x^2$ | False | False | False |
| $y$ | True | False | False |
| $yx$ | False | True | False |
| $yx^2$ | False | False | True |

where $S = \{s_1, s_2, s_3\}$ is the set of the vertices of the triangle, $x = (s_1 s_2 s_3)$ rotations, and $y$ is the reflection with preferred vertex $s_1$. □

*Proof of* $(b)$. By summing over different sets, we have

$$\sum_{s\in S}|G_s| = |\{(g,s)\in G\times S \mid gs = s\}| = \sum_{g\in G}|S^g|. \qquad \square$$

*Proof of* $(c)$. By the orbit-stabilizer theorem (Prop. 6.8.4) we have that there is a bijection between cosets $G/G_s$ and orbits $O_s$. By the counting formula (2.8.8), we then have

$$|G_s|\cdot|O_s| = |G_s|\cdot|G/G_s| = |G|.$$

Note in particular that $|G_{s'}|$ is equal for all $s'\in O_s$ since $O_s = O_{s'}$. Thus,

$$|G|\cdot(\text{number of orbits}) = \sum_{\text{orbits } O_s}|G| = \sum_{\text{orbits } O_s}|G_s|\cdot|O_s| = \sum_{s\in S}|G_s|,$$

and so, combining $(b)$,

$$|G|\cdot(\text{number of orbits}) = \sum_{g\in G}|S^g|. \qquad \square$$

# 11 Rings

## 11.1 Definition of a Ring

**Exercise 11.1.1.** *Prove that* $7+\sqrt[3]{2}$ *and* $\sqrt{3}+\sqrt{-5}$ *are algebraic numbers.*

*Proof.* $7+\sqrt[3]{2}$ is a root of $(x-7)^3-2 = x^3-21x^2+147x-345 = 0$.
$\sqrt{3}+\sqrt{-5}$ is a root of $(x^2+2)^2+60 = x^4+4x^2+64 = 0$. $\square$

**Exercise 11.1.2.** *Prove that, for* $n\neq 0$, $\cos(2\pi/n)$ *is an algebraic number.*

*Proof.* Suppose $n>0$. Recall that the Chebyshev polynomials $T_n(x)$ are defined by the recurrence relations $T_0(x)=1$, $T_1(x)=x$, and $T_n(x) = 2x\,T_{n-1}(x)-T_{n-2}(x)$. We claim $T_n(\cos\theta)=\cos n\theta$ for any $\theta$. This is clear for $n=0,1$. For arbitrary $n$,

$$\begin{aligned} T_n(\cos\theta) &= 2\cos\theta\,T_{n-1}(\cos\theta) - T_{n-2}(\cos\theta)\\ &= 2\cos\theta\cos\left((n-1)\theta\right) - \cos\left((n-2)\theta\right)\\ &= \cos n\theta + \cos\left((n-2)\theta\right) - \cos\left((n-2)\theta\right) = \cos n\theta, \end{aligned}$$

and so $T_n(\cos\theta)=\cos n\theta$ for any $\theta$ as desired. Letting $\theta = 2\pi/n$, we have that $T_n(\cos(2\pi/n)) = \cos 2\pi = 1$, and so $\cos(2\pi/n)$ satisfies the polynomial equation $T_n(x)-1=0$.

If $n<0$, then using the fact that $\cos(2\pi/n)=\cos(-2\pi/n)$, we see $\cos(2\pi/n)$ satisfies the polynomial equation $T_{-n}(x)-1=0$ by the above. $\square$

**Exercise 11.1.3.** *Let $\mathbb{Q}[\alpha,\beta]$ denote the smallest subring of $\mathbb{C}$ containing the rational numbers $\mathbb{Q}$ and the elements $\alpha=\sqrt{2}$ and $\beta=\sqrt{3}$. Let $\gamma=\alpha+\beta$. Is $\mathbb{Q}[\alpha,\beta]=\mathbb{Q}[\gamma]$? Is $\mathbb{Z}[\alpha,\beta]=\mathbb{Z}[\gamma]$?*

*Solution.* Since $\gamma\in\mathbb{Z}[\alpha,\beta],\mathbb{Q}[\alpha,\beta]$, the reverse inclusion $\supset$ holds in both cases. We claim that the inclusion $\subset$ holds for $\mathbb{Q}$, but not $\mathbb{Z}$.

To show $\mathbb{Q}[\alpha,\beta]\subset\mathbb{Q}[\gamma]$, it suffices to show $\alpha,\beta\in\mathbb{Q}[\gamma]$. Now $\gamma^2=5+2\alpha\beta\in\mathbb{Q}[\gamma]$, hence $\alpha\beta\in\mathbb{Q}[\gamma]$, so $\alpha\beta\gamma=3\alpha+2\beta\in\mathbb{Q}[\gamma]$. Thus $\alpha=\alpha\beta\gamma-2\gamma\in\mathbb{Q}[\gamma]$, and finally $\beta=\gamma-\alpha\in\mathbb{Q}[\gamma]$ as well.

To show $\mathbb{Z}[\alpha,\beta]\not\subset\mathbb{Z}[\gamma]$, we claim $\alpha\beta\notin\mathbb{Z}[\gamma]$. It suffices to show that $\gamma^k$ only has even coefficients for $\alpha\beta$, for then, any element $\sum_{k=0}^{N}a_k\gamma^k\in\mathbb{Q}[\gamma]$ will have an even coefficient for $\alpha\beta$, hence $\alpha\beta$ cannot be expressed as such a sum.

To prove this, we claim

$$\gamma^k=\begin{cases}a\alpha+b\beta \text{ for } a,b \text{ odd} & \text{when } k \text{ odd}\\ c+d\alpha\beta \text{ for } c \text{ odd}, d \text{ even} & \text{when } k \text{ even}\end{cases}$$

This is clear for $k=0,k=1$. For arbitrary $n$, consider first when $k$ is even. Then, by inductive hypothesis

$$\gamma^k=\gamma^{k-1}\gamma=(a\alpha+b\beta)(\alpha+\beta)=2a+3b+(a+b)\alpha\beta,$$

for $a,b$ odd, hence $2a+3b$ is odd and $a+b$ is even. Likewise, when $k$ is odd,

$$\gamma^k=\gamma^{k-1}\gamma=(c+d\alpha\beta)(\alpha+\beta)=(3d+c)\alpha+(c+2d)\beta,$$

for $c$ odd, $d$ even, hence $3d+c,c+2d$ are odd, and we are done. □

## 11.2 Polynomial Rings

**Exercise 11.2.1.** *For which positive integers $n$ does $x^2+x+1$ divide $x^4+3x^3+x^2+7x+5$ in $[\mathbb{Z}/(n)][x]$?*

*Proof.* We will perform the division algorithm on $x^4+3x^3+x^2+7x+5$. We have

$$\begin{array}{r|l} & x^2+2x-2 \\ \hline x^2+x+1 & x^4+3x^3+x^2+7x+5 \\ & -x^4-x^3-x^2 \\ \hline & 2x^3+7x \\ & -2x^2-2x^2-2x \\ \hline & -2x^2+5x+5 \\ & 2x^2+2x+2 \\ \hline & 7x+7 \end{array}$$

and so $x^4 + 3x^3 + x^2 + 7x + 5 = (x^2 + 2x - 2)(x^2 + x + 1) + (7x + 7)$, where the remainder $7x + 7 \equiv 0 \bmod n$ if and only if $n \in \{1, 7\}$. Hence $x^2 + x + 1$ divides $x^4 + 3x^3 + x^2 + 7x + 5$ in $[\mathbb{Z}/(n)][x]$ if and only if $n \in \{1, 7\}$. $\square$

**Exercise 11.2.2.** *Let $F$ be a field. The set of all formal power series $p(t) = a_0 + a_1 t + a_2 t^2 + \cdots$, with $a_i$ in $F$, forms a ring that is often denoted by $F[[t]]$. By* formal *power series we mean that the coefficients form an arbitrary sequence of elements of $F$. There is no requirement of convergence. Prove that $F[[t]]$ is a ring, and determine the units in this ring.*

*Proof.* We denote $p(t) = \sum_i a_i t^i, q(t) = \sum_i b_i t^i, r(t) = \sum_i c_i t^i$. Let $+$ defined as $p(t) + q(t) = \sum_k (a_k + b_k) t^k$ and $\times$ as $p(t) \times q(t) = \sum_k \sum_{i+j=k} a_i b_j t^k$.

$+$ makes $F[[t]]$ an abelian group because associativity and commutativity follow since $+$ is defined termwise, and because having $a_i = 0$ for all $i$ defines an identity and letting $q(t)$ such that $b_i = -a_i$ for all $i$ defines an inverse for $p(t)$.

$\times$ is commutative since $\sum_{i+j=k} a_i b_j = \sum_{i+j=k} b_i a_j$, and is associative since

$$\begin{aligned}(p(t) \times q(t)) \times r(t) &= \sum_\ell \sum_{i+j=\ell} a_i b_j t^\ell \times r(t) = \sum_\ell \sum_{i+j+k=\ell} a_i b_j c_k t^\ell \\ &= p(t) \times \sum_\ell \sum_{j+k=\ell} b_j c_k t^\ell = p(t) \times (q(t) \times r(t)).\end{aligned}$$

The identity is $p(t)$ such that $a_0 = 1, a_i = 0$ for all $i > 0$.

It remains to show the distributive property:

$$\begin{aligned}(p(t) + q(t)) \times r(t) &= \sum_i (a_i + b_i) t^i \times \sum_j c_j t^j = \sum_k \sum_{i+j=k} (a_i + b_i) c_j t^k \\ &= \sum_k \sum_{i+j=k} a_i c_j t^k + \sum_k \sum_{i+j=k} b_i c_j t^k \\ &= p(t) \times r(t) + q(t) \times r(t).\end{aligned}$$

Finally, we claim that the $p(t)$ such that $a_0 \neq 0$ are the units. Any unit must have $a_0 \neq 0$, for $p(t) \times q(t) = 1 \implies a_0 b_0 = 1$. In the other direction, suppose $p(t)$ is such that $a_0 \neq 0$. Define $q(t)$ such that

$$b_0 = a_0^{-1}, \quad b_i = -a_0^{-1} \sum_{j=1}^{i} a_j b_{i-j}.$$

Then, $a_0 b_0 = 1$ but

$$\sum_{i=0}^{k} a_{k-i} b_i = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_k b_0 = 0,$$

and so $p(t) \times q(t) = 1$. □

## 11.3 Homomorphisms and Ideals

**Exercise 11.3.3.** *Find generators for the kernels of the following maps:*
(a) $\mathbb{R}[x, y] \to \mathbb{R}$ *defined by* $f(x, y) \rightsquigarrow f(0, 0)$,
(b) $\mathbb{R}[x] \to \mathbb{C}$ *defined by* $f(x) \rightsquigarrow f(2 + i)$,
(c) $\mathbb{Z}[x] \to \mathbb{R}$ *defined by* $f(x) \rightsquigarrow f(1 + \sqrt{2})$,
(d) $\mathbb{Z}[x] \to \mathbb{C}$ *defined by* $x \rightsquigarrow \sqrt{2} + \sqrt{3}$,
(e) $\mathbb{C}[x, y, z] \to \mathbb{C}[t]$ *defined by* $x \rightsquigarrow t$, $y \rightsquigarrow t^2$, $z \rightsquigarrow t^3$.

*Remark.* We will denote each map as $\varphi$.

*Solution for* (a). We claim that $(x, y) = \ker \varphi$. By the division algorithm, any polynomial $f \in \mathbb{R}[x, y]$ can be written $g + a_0$ for $g \in (x, y)$, and so $\varphi(f) = a_0 = 0$ if and only if $a_0 = 0$ if and only if $f = g \in (x, y)$. □

*Solution for* (b). We claim that $(x^2 - 4x + 5) = \ker \varphi$. $x^2 - 4x + 5 = (x - (2 + i))(x - (2 - i))$, hence $(x^2 - 4x + 5) \subset \ker \varphi$. Conversely, let $f \in \ker \varphi$. By the division algorithm, we can write $f = g + r$ for $g \in (x^2 - 4x + 5)$, where $r = a_1 x + a_0$ for $a_i \in \mathbb{R}$ has degree less than 2. Then, $\varphi(f) = \varphi(g) + \varphi(r) = a_1(2 + i) + a_0$, which is zero only if $a_1 = a_0 = 0$, i.e., only if $f = g \in (x^2 - 4x + 5)$. □

*Solution for* (c). We claim that $(x^2 - 2x - 1) = \ker \varphi$. $x^2 - 2x - 1 = (x - (1 + \sqrt{2}))(x - (1 - \sqrt{2}))$, hence $(x^2 - 2x - 1) \subset \ker \varphi$. Conversely, let $f \in \ker \varphi$. By the division algorithm, we can write $f = g + r$ for $g \in (x^2 - 4x + 5)$, where $r = a_1 x + a_0$ for $a_i \in \mathbb{Z}$ has degree less than 2, since $x^2 - 2x - 1$ is monic. Then, $\varphi(f) = \varphi(g) + \varphi(r) = a_1(1 + \sqrt{2}) + a_0$, which is zero only if $a_1 = a_0 = 0$ since $1, \sqrt{2}$ are linearly independent over $\mathbb{Z}$, i.e., only if $f = g \in (x^2 - 2x - 1)$. □

*Solution for* (d). We claim that $(x^4 - 10x^2 + 1) = \ker \varphi$. We have $(x^4 - 10x^2 + 1) \subset \ker \varphi$, since $\varphi(x^4 - 10x^2 + 1) = (\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 1 = 0$. Conversely,

let $f \in \ker \varphi$. By the division algorithm, we can write $f = g + r$, where $r = a_3x^3 + a_2x^2 + a_1x + a_0$ for $a_i \in \mathbb{Z}$ has degree less than 4. Then,

$$\begin{aligned}\varphi(f) = \varphi(g + r) &= r(\sqrt{2} + \sqrt{3}) \\ &= a_3(\sqrt{2} + \sqrt{3})^3 + a_2(\sqrt{2} + \sqrt{3})^2 + a_1(\sqrt{2} + \sqrt{3}) + a_0 \\ &= (11a_3 + a_1)\sqrt{2} + (9a_3 + a_1)\sqrt{3} + (2a_2)\sqrt{6} + (5a_2 + a_0).\end{aligned}$$

This gives rise to the system of equations represented by the matrices

$$\begin{bmatrix} 1 & 0 & 5 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 9 \\ 0 & 1 & 0 & 11 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

since $\sqrt{2}, \sqrt{3}, \sqrt{6}, 1$ are linearly independent over $\mathbb{Z}$. But, this only has the trivial solution $a_0 = a_1 = a_2 = a_3 = 0$, since

$$\begin{vmatrix} 1 & 0 & 5 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 9 \\ 0 & 1 & 0 & 11 \end{vmatrix} = -2 \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 9 \\ 0 & 1 & 11 \end{vmatrix} = -2 \begin{vmatrix} 1 & 9 \\ 1 & 11 \end{vmatrix} = -2(11 - 9) = -4 \neq 0,$$

which implies $f = g \in (x^4 - 10x^2 + 1)$. □

*Solution for* $(e)$. We claim that $(x^2 - y, x^3 - z, y^3 - z^2) = \ker \varphi$. Clearly, $(x^2 - y, x^3 - z, y^3 - z^2) \subset \ker \varphi$, since

$$\varphi(x^2 - y) = t^2 - t^2 = 0, \quad \varphi(x^3 - z) = t^3 - t^3 = 0, \quad \varphi(y^3 - z^2) = t^6 - t^6 = 0.$$

Conversely, we first regard $f$ as a polynomial in $z$ whose coefficients are in $x, y$, as in Corollary 11.3.8. We can apply the division algorithm to get $f = g_1 + r_1$ for $g_1 \in (y^3 - z^2)$, where $r_1$ is of degree less than 2 in $z$. If $r_1 = 0$, then $f \in (y^3 - z^2)$, and so we are done. If not, then we can apply the division algorithm again with $x^2 - y$, this time in $y$, on $r_1$ to have $r_1 = g_2 + r_2$ for $g_2 \in (x^2 - y)$, where $r_2$ is of degree 0 in $y$, and degree less than 2 in $z$. If $r_2 = 0$, then $f = g_1 + g_2 \in (y^3 - z^2, x^2 - y)$, and so we are done. If not, then we can apply the division algorithm again with $x^3 - z$, this time in $x$, on $r_2$ to have $r_2 = g_3 + r_3$ for $g_3 \in (x^3 - z)$, where $r_3$ is of degree less than 2 in $x$, degree 0 in $y$, and degree less than 2 in $z$. This means that we have

$$\varphi(r_3) = \varphi(a_{101}xz + a_{001}z + a_{100}x + a_{000}) = a_{101}t^4 + a_{001}t^3 + a_{100}t + a_{000} = 0,$$

and the linear independence of $t^k$ over $\mathbb{C}$ implies that $r_3 = 0$, and so $f = g_1 + g_2 + g_3 \in (y^3 - z^2, x^2 - y, x^3 - z)$. □

**Exercise 11.3.5.** *The derivative of a polynomial $f$ with coefficients in a field $F$ is defined by the calculus formula $(a_nx^n + \cdots + a_1x + a_0)' = na_nx^{n-1} + \cdots + 1a_1$. The integer coefficients are interpreted in $F$ using the unique homomorphism $\mathbb{Z} \to F$.*

(a) *Prove the product rule $(fg)' = f'g + fg'$ and the chain rule $(f \circ g)' = (f' \circ g)g'$.*

(b) *Let $\alpha$ be an element of $F$. Prove that $\alpha$ is a multiple root of a polynomial $f$ if and only if it is a common root of $f$ and of its derivative $f'$.*

*Proof of* (a). Let $f = \sum a_ix^i$, $g = \sum b_jx^j$. Then by (11.2.7), $fg = \sum c_kx^k$, where $c_k = \sum_{i+j=k} a_ic_j$, and so

$$f'g = \left(\sum_{i\geq 0}(i+1)a_{i+1}x^i\right)\left(\sum_{j\geq 0} b_jx^j\right) = \sum_{k\geq 0}\sum_{i+j=k}(i+1)a_{i+1}b_jx^k,$$

and similarly

$$fg' = \left(\sum_{i\geq 0} a_ix^i\right)\left(\sum_{j\geq 0}(j+1)b_{j+1}x^j\right) = \sum_{k\geq 0}\sum_{i+j=k}(j+1)a_ib_{j+1}x^k.$$

Thus,

$$\begin{aligned} f'g + fg' &= \sum_{k\geq 0}\left(\sum_{i+j=k}(i+1)a_{i+1}b_j + (j+1)a_ib_{j+1}\right)x^k \\ &= \sum_{k\geq 0}\left(\sum_{i+j=k+1} ia_ib_j + ja_ib_j\right)x^k \\ &= \sum_{k\geq 0}(k+1)\sum_{i+j=k+1} a_ib_jx^k = \sum_{k\geq 0}(k+1)c_{k+1}x^k = (fg)'. \end{aligned}$$ □

*Proof of* (b). Suppose $f \in F[x]$. Then, $f = (x-\alpha)^k g$ for some $k \geq 0$ and $g \in F[x]$ such that $g(\alpha) \neq 0$. By (a), $f' = k(x-\alpha)^{k-1}g + (x-\alpha)^k g'$ if $k \geq 1$, and $f' = g'$ if $k = 0$. Hence $f(\alpha) = f'(\alpha) = 0$ if and only if $k \geq 2$, i.e., $\alpha$ is a multiple root of $f$ if and only if $\alpha$ is a common root of $f, f'$. □

**Exercise 11.3.7.** *Determine the automorphisms of the polynomial ring $\mathbb{Z}[x]$.*

*Proof.* Suppose $\varphi \in \mathrm{Aut}(\mathbb{Z}[x])$. Then $\varphi(1) = 1$, hence

$$n = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n \text{ times}} = \varphi(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \varphi(n).$$

Thus, if $f = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$, then $\varphi(f) = \sum_{j=0}^{n} b_j \varphi(x)^j$, and so $\varphi$ is uniquely determined by $\varphi(x)$.

So let $\varphi(x) = \sum_{i=0}^{d} a_i x^i$. Then,

$$\varphi(f) = \sum_{i=0}^{d} a_i \left( \sum_{j=0}^{n} b_j x^j \right)^d = a_d b_n x^{nd} + \cdots + \sum_{i=0}^{d} a_i b_j^d. \tag{1}$$

hence $\deg(\varphi(f)) = nd$. Suppose $f \in \mathbb{Z}[x]$ is the unique element such that $\varphi(f) = x$. Then, $nd = 1$ and $a_d b_n = 1$ imply that $d = 1$ and $a_1 \in \{\pm 1\}$. Thus $\varphi(x) = \pm x + a$ for $a \in \mathbb{Z}$, i.e., every $\varphi \in \mathrm{Aut}(\mathbb{Z}[x])$ must map $x \rightsquigarrow \pm x + a$ for $a \in \mathbb{Z}$. Finally, all such $\varphi$ give automorphisms of $\mathbb{Z}$ since they define ring homomorphisms by the equation (1), and since $\mathbb{Z}[\pm x + a] = \mathbb{Z}[x]$. □

**Exercise 11.3.8.** *Let $R$ be a ring of prime characteristic $p$. Prove that the map $R \to R$ defined by $x \rightsquigarrow x^p$ is a ring homomorphism. (It is called the* Frobenius map*).*

*Proof.* We first claim that for $p$ prime, $p \mid \binom{p}{i}$ if $1 \leq i \leq p-1$. By definition,

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdots 2 \cdot 1}.$$

$1 \geq i$ implies $p$ appears in the numerator, and $i \leq p-1$ implies $p$ does not appear in the denominator. Since $\binom{p}{i} \in \mathbb{Z}$, this implies $p \mid \binom{p}{i}$, hence $\binom{p}{i} = 0 \in R$.

Now if $x, y \in R$, the binomial theorem gives

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} = x^p + y^p$$

Thus $x \rightsquigarrow x^p$ respects addition. Since trivially $1 \rightsquigarrow 1$ and $(xy)^p = x^p y^p$, we therefore have that $x \rightsquigarrow x^p$ defines a ring homomorphism $R \to R$. □

**Exercise 11.3.9.**

(a) *An element $x$ of a ring $R$ is called* nilpotent *if some power is zero. Prove that if $x$ is nilpotent, then $1 + x$ is a unit.*

(b) *Suppose that $R$ has prime characteristic $p \neq 0$. Prove that if $a$ is nilpotent then $1 + a$ is* unipotent*, that is, some power of $1 + a$ is equal to 1.*

*Proof of (a).* Suppose $x^N = 0$. Then

$$(1+x)(1 - x + x^2 - \cdots + (-1)^{N-1} x^{N-1}) = 1 - x^N = 1,$$

hence $1 + x$ is a unit. □

*Proof of (b).* Suppose $a^N = 0$. By Exercise 11.3.8, $x \rightsquigarrow x^p$ is a homomorphism $R \to R$, so $(1+a)^p = 1 + a^p$. Iterating this map $n$ times such that $p^n \geq N$ gives $(1+a)^{p^n} = 1 + a^{p^n} = 1 + a^N a^{p^n - N} = 1$. □

**Exercise 11.3.10.** *Determine all ideals of the ring $F[[t]]$ of formal power series with coefficients in a field $F$ (see Exercise* 11.2.2*).*

*Solution.* We claim all nonzero ideals are of the form $(t^n)$ for some $n$. Let $I$ be an ideal and $p \in I$ such the number $n \coloneqq \min\{i \mid a_i \neq 0\}$ is minimal. We claim $I = (t^n)$. First, $p = t^n q$ for some unit $q$, hence $(t^n) \subset I$. Conversely, any $r \in I$ has first nonzero coefficient at degree $\geq n$, hence $t^n s$ for some $s \in F[[t]]$, and so $r \in (t^n)$. □

**Exercise 11.3.11.** *Let $R$ be a ring, and let $I$ be an ideal of the polynomial ring $R[x]$. Let $n$ be the lowest degree among nonzero elements of $I$. Prove or disprove: $I$ contains a monic polynomial of degree $n$ if and only if it is a principal ideal.*

*Proof of $\Rightarrow$.* If $I = 0$, then it is principal so suppose not. Let $f$ be a monic polynomial of lowest degree $n$. We claim $(f) = I$. $f \in I$ hence $(f) \subset I$. Now suppose $g \in I$; then, by division with remainder we can write $g = fq + r$, where if $r \neq 0$, it has degree lower than $f$. But then, $f, g \in I$, hence $g - fq = r \in I$, so $r = 0$, and $g \in (f)$. □

*Counterexample for $\Leftarrow$.* Consider $I = (2x) \subset \mathbb{Z}[x]$. Any element in $I$ is obtained by multiplying $2x$ by a polynomial of degree $\geq 1$, in which case we get an element of degree $\geq 2$, or by multiplying by an element of $\mathbb{Z}$. But then, $2 \notin \mathbb{Z}^\times$, hence there is no monic polynomial of degree 1 in $I$. □

**Exercise 11.3.12.** *Let $I$ and $J$ be ideals of a ring $R$. Prove that the set $I + J$ of elements of the form $x + y$, with $x$ in $I$ and $y$ in $J$, is an ideal. This ideal is called the* sum *of the ideals $I$ and $J$.*

*Proof.* Let $(x+y), (x'+y') \in I + J$ and $s \in R$, where $x, x' \in I$, $y, y' \in J$. Then, $s(x+y) + (x'+y') = (sx + x') + (sy + y') \in I + J$, hence $I + J$ is an ideal. □

**Exercise 11.3.13.** *Let $I$ and $J$ be ideals of a ring $R$. Prove that the intersection $I \cap J$ is an ideal. Show by example that the set of products $\{xy \mid x \in I, y \in J\}$ need not be an ideal, but that the set of finite sums $\sum x_\nu y_\nu$ of products of elements of $I$ and $J$ is an ideal. This ideal is called the* product ideal*, and is denoted by $IJ$. Is there a relation between $IJ$ and $I \cap J$?*

*Proof.* Let $x, y \in I \cap J$ and $s \in R$. Then, $sx + y \in I$ and $sx + y \in J$ since $I, J$ are ideals, hence $sx + y \in I \cap J$ and so $I \cap J$ is an ideal.

Now let $R = \mathbb{Z}[x], I = (2, x), J = (3, x)$. Then, $3x, 2x$ are in the set of products, but their difference $3x - 2x = x$ is not, and so the set of products is not an ideal.

Let $\sum x_i y_i, \sum x_i' y_i' \in IJ$ and $s \in R$, where $x_i, x_i' \in I$, $y_i, y_i' \in J$. Then, $s \sum x_i y_i + \sum x_i' y_i' = \sum s x_i y_i + \sum x_i' y_i' \in IJ$, hence $IJ$ is an ideal.

We have in general $IJ \subset I \cap J$ since $\sum x_i y_i$ for $x_i \in I, y_i \in J$ has $x_i y_i \in I \cap J$. $IJ = I \cap J$ if $I + J = (1)$ by Exercise 11.6.8$(a)$.

$I \cap J \subset IJ$ does not hold in general, for if $R = \mathbb{Z}, I = (m), J = (n)$, then $I \cap J = (\text{lcm}(m, n))$ but $IJ = (mn)$. □

## 11.4 Quotient Rings

**Exercise 11.4.2.** *What does the Correspondence Theorem tell us about ideals of* $\mathbb{Z}[x]$ *that contain* $x^2 + 1$*?*

*Solution.* By the Correspondence Theorem (Thm. 11.4.3), there is a bijective correspondence between the ideals of $\mathbb{Z}[x]$ that contain $x^2 + 1$ and the ideals of $\mathbb{Z}[x]/(x^2 + 1) \approx \mathbb{Z}[i]$, where these two rings are isomorphic as in Ex. 11.4.5. By Prop. 12.2.5$(c)$, $\mathbb{Z}[i]$ is a Euclidean domain, hence a principal ideal domain by Prop. 12.2.7. Thus, every ideal in $\mathbb{Z}[i]$ is of the form $(a + bi)$ for $a, b \in \mathbb{Z}$. These correspond to ideals $(a + bx)$ in $\mathbb{Z}[x]/(x^2 + 1)$ by the isomorphism $i \rightsquigarrow x$ from above, hence the ideals in $\mathbb{Z}[x]$ containing $x^2 + 1$ are of the form $(a + bx, x^2 + 1)$. □

**Exercise 11.4.3.** *Identify the following rings:* $(a)$ $\mathbb{Z}[x]/(x^2 - 3, 2x + 4)$*,* $(b)$ $\mathbb{Z}[i]/(2 + i)$*,* $(c)$ $\mathbb{Z}[x]/(6, 2x - 1)$*,* $(d)$ $\mathbb{Z}[x]/(2x^2 - 4, 4x - 5)$*,* $(e)$ $\mathbb{Z}[x]/(x^2 + 3, 5)$*.*

*Solution for* $(a)$*.* We see that $2(x^2 - 3) - (x - 2)(2x + 4) = 2 \in (x^2 - 3, 2x + 4)$, and so $(x^2 - 3, 2x + 4) = (x^2 - 3, 2x + 4, 2) = (x^2 - 3, 2)$, since $2(x + 2) = 2x + 4$. Then, $\mathbb{Z}[x]/(x^2 - 3, 2x + 4) = \mathbb{Z}[x]/(x^2 - 3, 2)$. But then, $\mathbb{Z}[x]/(x^2 - 3, 2) \approx \mathbb{F}_2[x]/(x^2 - 3) = \mathbb{F}_2[x]/(x^2 + 1) = \mathbb{F}_2[x]/(x + 1)^2$ since $x^2 + 1 = (x + 1)^2$ in $\mathbb{F}_2$. □

*Solution for* $(b)$*.* First recall $\mathbb{Z}[i] \approx \mathbb{Z}[x]/(x^2 + 1)$. Thus, $\mathbb{Z}[i]/(2 + i) \approx \mathbb{Z}[x]/(x^2 + 1, 2 + x)$. We first consider the quotient $\mathbb{Z}[x]/(2 + x)$. Since $(2 + x)$ is the kernel of the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}[-2]$, $f(x) \rightsquigarrow f(-2)$, we see that this is isomorphic to $\mathbb{Z}$, as in Example 11.4.5. Then, we have that the residue of $g = x^2 + 1$ is 5, and so we have $\mathbb{Z}[i]/(2 + i) \approx \mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$. □

*Solution for* $(c)$*.* We first note $6x - 3(2x - 1) = 3 \in (6, 2x - 1)$, and so $(6, 2x - 1) = (3, 2x - 1)$. Also, $3x - (2x - 1) = x + 1 \in (3, 2x - 1)$, and so $(3, 2x - 1) = (3, x + 1)$. Thus, $\mathbb{Z}[x]/(6, 2x - 1) = \mathbb{Z}[x]/(3, x + 1) \approx \mathbb{F}_3[x]/(x + 1) = \mathbb{F}_3$. □

*Solution for (d).* Since $(4x+5)(4x-5)-8(2x^2-4)=7\in(2x^2-4,4x-5)$, hence $(2x^2-4,4x-5)=(7,2x^2-4,4x-5)$. Hence $\mathbb{Z}[x]/(2x^2-4,4x-5)=\mathbb{Z}[x]/(7,2x^2-4,4x-5)=\mathbb{F}_7[x]/(2x^2-4,4x-5)$. In $\mathbb{F}_7[x]$, $4(2x^2-4)=x^2+5$ and $2(4x-5)=x+4$, hence $(2x^2-4,4x-5)=(x^2+5,x+4)$. But $x+4\mid x^2+5$, hence $(x^2+5,x+4)=(x+4)$. Finally, $\mathbb{F}_7[x]/(2x^2-4,4x-5)=\mathbb{F}_7[x]/(x^2+5,x+4)=\mathbb{F}_7[x]/(x+4)\approx\mathbb{F}_7$. □

*Solution for (e).* We see $\mathbb{Z}[x]/(x^2+3,5)\approx\mathbb{F}_5[x]/(x^2+3)$. But since $x^2+3\neq 0$ for any $x\in\mathbb{F}_5$, we see that we cannot reduce $x^2+3$. But in $\mathbb{F}_5$, $x^2+3=x^2-2$, and so we have $\mathbb{F}_5[\sqrt{2}]$. □

**Exercise 11.4.4.** *Are the rings $\mathbb{Z}[x]/(x^2+7)$ and $\mathbb{Z}[x]/(2x^2+7)$ isomorphic?*

*Solution.* We claim they are not. Let $R=\mathbb{Z}[x]/(x^2+7)$ and $S=\mathbb{Z}[x]/(2x^2+7)$. Asume $\alpha\colon R\to S$ is an isomorphism. $\alpha(1)=1$, hence $\alpha(2)=2$, and so if $\alpha$ is an isomorphism, then $R/(2)\approx S/(2)$. We claim this is a contradiction. For, $R/(2)\approx F_2[x]/(x^2+1)\neq 0$, whereas $S/(2)\approx F_2[x]/(1)=0$. □

## 11.5 Adjoining Elements

**Exercise 11.5.1.** *Let $f=x^4+x^3+x^2+x+1$ and let $\alpha$ denote the residue of $x$ in the ring $R=\mathbb{Z}[x]/(f)$. Express $(\alpha^3+\alpha^2+\alpha)(\alpha^5+1)$ in terms of the basis $(1,\alpha,\alpha^2,\alpha^3)$ of $R$.*

*Proof.* We first have $(x^3+x^2+x)(x^5+1)=x^8+x^7+x^6+x^3+x^2+x$. We then perform the division algorithm:

$$\begin{array}{rr|l}
 & & x^4 - x \\
\hline
x^4+x^3+x^2+x+1 & x^8+x^7+x^6 + x^3 + x^2 + x & \\
 & -x^8-x^7-x^6-x^5-x^4 & \\
\hline
 & -x^5-x^4+x^3+x^2+x & \\
 & x^5+x^4+x^3+x^2+x & \\
\hline
 & 2x^3+2x^2+2x &
\end{array}$$

and so $(\alpha^3+\alpha^2+\alpha)(\alpha^5+1)=2\alpha^3+2\alpha^2+2\alpha\in\mathbb{Z}[x]/(f)$. □

**Exercise 11.5.3.** *Describe the ring obtained from $\mathbb{Z}/12\mathbb{Z}$ by adjoining an inverse of 2.*

*Solution.* Let $R=(\mathbb{Z}/12\mathbb{Z})[x]/(2x-1)$ be our ring; it is isomorphic to $\mathbb{Z}[x]/(12,2x-1)$. $(12,2x-1)=(3,2x-1)$ since $\subset$ clearly holds and $12x^2-(3+6x)(2x-1)=3\in(12,2x-1)$. Thus $R\approx\mathbb{Z}[x]/(3,2x-1)\approx\mathbb{F}_3[x]/(2x-1)$. But $2\in\mathbb{F}_3^\times$, hence $\mathbb{F}_3[x]/(2x-1)\approx\mathbb{F}_3$, so $R\approx\mathbb{F}_3$. □

**Exercise 11.5.4.** *Determine the structure of the ring $R'$ obtained from $\mathbb{Z}$ by adjoining an element $\alpha$ satisfying each set of relations.*
*(a)* $2\alpha = 6, 6\alpha = 15$, *(b)* $2\alpha - 6 = 0, \alpha - 10 = 0$, *(c)* $\alpha^3 + \alpha^2 + 1 = 0, \alpha^2 + \alpha = 0$.

*Solution for (a).* $\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(2x-6, 6x-15)$. But $(6x-15)-3(2x-6) = 3 \in (2x-6, 6x-15)$, and $3(x-2)-(2x-6) = x \in (2x-6, 6x-15)$ imply $(2x-6, 6x-15) = (x, 3)$. Thus, $\mathbb{Z}[\alpha] \approx \mathbb{Z}[x]/(3, x) \approx \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$. □

*Solution for (b).* $\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(2x-6, x-10)$. But $(2x-6)-2(x-10) = 14 \in (2x-6, x-10)$ and $(x-10)+14 = x+4 \in (2x-6, x-10)$ imply $(2x-6, x-10) = (x+4, 14)$, since $2x - 6 = 2x(x + 4) - 14$. Thus, $\mathbb{Z}[\alpha] \approx \mathbb{Z}[x]/(x + 4, 14) \approx \mathbb{Z}/14\mathbb{Z}$. □

*Solution for (c).* $\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(x^3 + x^2 + 1, x^2 + x)$. But $x^3 + x^2 + 1 - x(x^2 + x) = 1 \in (x^3 + x^2 + 1, x^2 + x)$, and so $\mathbb{Z}[\alpha] \approx \mathbb{Z}[x]/(1) = 0$, the zero ring. □

**Exercise 11.5.6.** *Let $a$ be an element of a ring $R$, and let $R'$ be the ring $R[x]/(ax-1)$ obtained by adjoining an inverse of $a$ to $R$. Let $\alpha$ denote the residue of $x$ (the inverse of $a$ in $R'$).*

- *(a) Show that every element $\beta$ of $R'$ can be written in the form $\beta = \alpha^k b$, with $b$ in $R$.*
- *(b) Prove that the kernel of the map $R \to R'$ is the set of elements $b$ of $R$ such that $a^n b = 0$ for some $n > 0$.*
- *(c) Prove that $R'$ is the zero ring if and only if $a$ is nilpotent (see Exercise 11.3.9).*

*Proof of (a).* Any element $\beta \in R'$ can be written as a finite sum $\sum b_k \alpha^k$. Letting $K$ be the largest $k$ such that $b_k \neq 0$, we see that defining $b = \sum a^{K-k} b_k$, $\alpha^K b = \beta$. □

*Proof of (b).* Let $\Gamma_a(R) = \{b \in R \mid a^n b = 0 \text{ for some } n > 0\}$, and call the map defined $\varphi$; it suffices to show $\Gamma_a(R) = \varphi^{-1}((ax - 1))$, where $(ax - 1) \subset R[x]$. But $b \in R$ has $\varphi(b) \in (ax - 1)$ if and only if $(ax - 1)g = b$ for some $g = \sum g_i x^i \in R[x]$. Solving recursively, we must have $g_i = -a^i b$ for all $i$. Such a $g$ exists if and only if $b \in \Gamma_a(R)$, for otherwise $g$ would be an infinite sum. □

*Proof of (c).* $a$ is nilpotent if and only if $1 \in \Gamma_a(R)$. By the proof of $(b)$, this holds if and only if $1 \in (ax - 1)$, and since $R[x] \to R'$ is surjective, this holds if and only if $R' = 0$ by the first isomorphism theorem (Thm. 11.4.2$(b)$). □

## 11.6 Product Rings

**Exercise 11.6.1.** *Let $\varphi\colon \mathbb{R}[x] \to \mathbb{C}\times\mathbb{C}$ be the homomorphism defined by $\varphi(x) = (1, i)$ and $\varphi(r) = (r, r)$ for $r \in \mathbb{R}$. Determine the kernel and the image of $\varphi$.*

*Solution.* $\varphi$ is the evaluation map $f \rightsquigarrow (f(1), f(i))$. So $f \in \ker\varphi \iff f(1) = f(i) = 0 \iff f \in ((x-1)(x^2+1))$, i.e., $\ker\varphi = ((x-1)(x^2+1))$.

We now claim $\operatorname{im}\varphi = \mathbb{R}\times\mathbb{C}$. $\subset$ clearly holds. Now let $(c, a+bi) \in \mathbb{R}\times\mathbb{C}$. Then, if $f = a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{R}[x]$ is of degree 3,

$$\begin{aligned}\varphi(f) &= (a_3 + a_2 + a_1 + a_0, -ia_3 - a_2 + a_1 i + a_0)\\ &= (a_3 + a_2 + a_1 + a_0, (a_0 - a_2) + (a_1 - a_3)i),\end{aligned}$$

and the condition $f \rightsquigarrow (c, a+bi)$ gives the system of equations

$$\begin{cases} a_0 + a_1 + a_2 + a_3 = c \\ a_0 \quad - a_2 \quad = a \\ \quad a_1 \quad - a_3 = b \end{cases}$$

which has a solution by linear algebra, hence $\supset$ also holds, and $\operatorname{im}\varphi = \mathbb{R}\times\mathbb{C}$. □

**Exercise 11.6.2.** *Is $\mathbb{Z}/(6)$ isomorphic to the product ring $\mathbb{Z}/(2)\times\mathbb{Z}/(3)$? Is $\mathbb{Z}/(8)$ isomorphic to $\mathbb{Z}/(2)\times\mathbb{Z}/(4)$?*

*Solution.* Letting $R = \mathbb{Z}/(6), I = (2), J = (3)$ in Exercise 11.6.8(*c*), we have $\mathbb{Z}/(6) \approx \mathbb{Z}/(2)\times\mathbb{Z}/(3)$, since $IJ = 0$ in $R$.

$\mathbb{Z}/(8) \not\approx \mathbb{Z}/(2)\times\mathbb{Z}/(4)$, for $\mathbb{Z}/(8)$ has an additive element of order 8 while $\mathbb{Z}/(2)\times\mathbb{Z}/(4)$ does not. □

**Exercise 11.6.3.** *Classify rings of order* 10.

*Proof.* Let $R$ be a ring of order 10. By the Sylow Theorems (Thms. 7.7.2, 7.7.4, 7.7.6), the abelian group $(R, +)$ contains exactly one normal subgroup each of orders 2 and 5, with trivial intersection, hence by Prop. 2.11.4(*d*), $(R, +) \approx \mathbb{Z}/(2)\times\mathbb{Z}/(5) \approx \mathbb{Z}/(10)$. It remains to show $R \approx \mathbb{Z}/(10)$ also as a ring. Let $a \in R$ be an element of order 10; $a$ then generates $R$, and so $1 \in R$ implies $na = 1$ for some $1 \le n \le 9$. If $n = 2$, then $5a = 2a \cdot 5a = 10a^2 = 0$, contradicting that $a$ has order 10; similarly, $n \neq 5$. Thus, $na = 1$ has order 10, and generates $R$, hence $R \approx \mathbb{Z}/(10)$. □

**Exercise 11.6.4.** *In each case, describe the ring obtained from the field $\mathbb{F}_2$ by adjoining an element $\alpha$ satisfying the given relation:*
(*a*) $\alpha^2 + \alpha + 1 = 0$, (*b*) $\alpha^2 + 1 = 0$, (*c*) $\alpha^2 + \alpha = 0$.

*Remark.* Since each equation is of degree 2, we can write $\mathbb{F}_2[\alpha] = \{0, 1, \alpha, \alpha+1\}$ by Prop. 11.5.5$(a)$ in each case.

*Solution for* $(a)$. Since $\alpha(\alpha+1) = \alpha^2+\alpha = 1$, every element of $\mathbb{F}_2[\alpha]$ has an inverse. Thus, we have a field of order 4, i.e., $\mathbb{F}_2[\alpha] = \mathbb{F}_4$. □

*Solution for* $(b)$. $\mathbb{F}_2[\alpha] = \mathbb{F}_2[x]/(x^2+1) = \mathbb{F}_2[i]$, the ring of Gauss integers mod 2. We see $(\alpha+1)^2 = \alpha^2+1 = 0$, and so $\alpha^2 = 1$, $\alpha(\alpha+1) = \alpha^2+\alpha = \alpha+1$. This is not a field, or even an integral domain, since $(\alpha+1)^2 = 0$. □

*Solution for* $(c)$. We have $\alpha^2 = \alpha$, and so by Prop. 11.6.2 we have $\mathbb{F}_2[\alpha] \approx \alpha\mathbb{F}_2[\alpha] \times (\alpha+1)\mathbb{F}_2[\alpha]$. Since $\alpha\mathbb{F}_2[\alpha] = \{0, \alpha\}$ and $(\alpha+1)\mathbb{F}_2[\alpha] = \{0, \alpha+1\}$ are both isomorphic to $\mathbb{F}_2$, we see that $\mathbb{F}_2[\alpha] \approx \mathbb{F}_2 \times \mathbb{F}_2$. □

**Exercise 11.6.5.** *Suppose we adjoin an element $\alpha$ satisfying the relation $\alpha^2 = 1$ to the real numbers $\mathbb{R}$. Prove that the resulting ring is isomorphic to the product $\mathbb{R} \times \mathbb{R}$.*

*Proof.* The resulting ring is $R = \mathbb{R}[x]/(x^2-1)$. Let $\varphi\colon \mathbb{R}[x] \to \mathbb{R} \times \mathbb{R}$ be defined by $f \rightsquigarrow (f(1), f(-1))$. $\ker\varphi = (x^2-1) = ((x+1)(x-1))$, and so by the first isomorphism theorem (Thm. 11.4.2$(b)$) it suffices to show $\varphi$ is surjective, inducing an isomorphism $R \to \mathbb{R} \times \mathbb{R}$. Letting $f = ax+b \in \mathbb{R}[x]$ of degree 1, we have

$$\varphi(ax+b) = (a+b, a-b),$$

which can be solved for arbitrary $(a+b, a-b) = (x, y)$ by linear algebra. □

**Exercise 11.6.6.** *Describe the ring obtained from the product ring $\mathbb{R}\times\mathbb{R}$ by inverting the element $(2, 0)$.*

*Solution.* Using the isomorphism in Exercise 11.6.5, since $x+1 \rightsquigarrow (2, 0)$, the ring is

$$\frac{\mathbb{R}[x,y]}{(x^2-1, (x+1)y-1)} \approx \frac{\mathbb{R}[x,(x+1)^{-1}]}{(x^2-1)} = \frac{\mathbb{R}[x,(x+1)^{-1}]}{((x+1)(x-1))} = \frac{\mathbb{R}[x,(x+1)^{-1}]}{(x-1)} \approx \mathbb{R},$$

since $x+1$ has residue 2 in $\mathbb{R}[x]/(x-1)$, which already has an inverse in $\mathbb{R}$. □

**Exercise 11.6.7.** *Prove that in the ring $\mathbb{Z}[x]$, the intersection $(2) \cap (x)$ of the principal ideals $(2)$ and $(x)$ is the principal ideal $(2x)$, and that the quotient ring $R = \mathbb{Z}[x]/(2x)$ is isomorphic to the subring of the product ring $\mathbb{F}_2[x] \times \mathbb{Z}$ of pairs $(f(x), n)$ such that $f(0) \equiv n$ modulo 2.*

*Proof.* Clearly $(2x) \subset (2) \cap (x)$. Conversely, if $f \in (2) \cap (x)$, then $f = 2g = xh$ for some $g, h \in \mathbb{Z}[x]$. But this implies $g \in (x)$, hence $f \in (2x)$.

Now consider the ring homomorphism $\varphi\colon \mathbb{Z}[x] \to \mathbb{F}_2[x] \times \mathbb{Z}$ where $\sum a_i x^i \rightsquigarrow \sum(\overline{a}_i x^i, a_0)$, where $\overline{a}_i$ is the residue of $a_i$ in $\mathbb{F}_2$. We claim $\varphi(\mathbb{Z}[x]) = S \coloneqq \{(f(x), n) \in \mathbb{F}_2[x] \times \mathbb{Z} \mid f(0) \equiv n \bmod 2\}$. By construction, $\varphi(\mathbb{Z}[x]) \subset S$; conversely, any $(f(x), n) \in S$ must have $f(x) = \sum \overline{a}_i x^i$ where $\overline{a}_0 = \overline{n}$, and so choosing representatives $a_i$ of $\overline{a}_i$ in $\mathbb{Z}$ such that $a_0 = n$, we see that $\sum a_i x^i \mapsto (f(x), n)$, hence $\varphi(\mathbb{Z}[x]) \supset S$.

Finally we show $\ker \varphi = (2x)$. $(2x) \subset \ker \varphi$ by construction. Conversely, $\varphi(f) = (0,0) \implies a_0 = 0$ and $2 \mid a_i$ for $i \neq 0$, hence $f \in (2) \cap (x) = (2x)$ by the above. Thus, $R \approx S$ by the first isomorphism theorem (Thm. 11.4.2($b$)). □

**Exercise 11.6.8.** *Let $I$ and $J$ be ideals of a ring $R$ such that $I + J = R$.*

($a$) *Prove that $IJ = I \cap J$ (see Exercise* 11.3.13*).*

($b$) *Prove the* Chinese Remainder Theorem: *For any pair $a, b$ of elements of $R$, there is an element $x$ such that $x \equiv a$ modulo $I$ and $x \equiv b$ modulo $J$. (The notation $x \equiv a$ modulo $I$ means that $x - a \in I$.)*

($c$) *Prove that if $IJ = 0$, then $R$ is isomorphic to the product ring $(R/I) \times (R/J)$.*

($d$) *Describe the idempotents corresponding to the product decomposition in ($c$).*

*Proof of ($a$).* Clearly $IJ \subset I \cap J$. In the other direction, let $u + v = 1$ for $u \in I, v \in J$. Then, if $x \in I \cap J$, $x = x(u + v) = xu + xv \in IJ$. □

*Proof of ($b$).* It suffices to show the ring homomorphism $\varphi\colon R \to R/I \times R/J$ defined by $x \mapsto (x+I, x+J)$ is surjective. Let $(a+I, b+J) \in R/I \times R/J$. Since $I + J = R$, we have $u + v = 1$ for some $u \in I, v \in J$. Let $x = bu + av$. Then, $\varphi(x) = (x+I, x+J) = (av + I, bu + J) = (a(1-u) + I, b(1-v) + J) = (a + I, b + J)$. □

*Proof of ($c$).* By definition in ($b$) $\ker \varphi = I \cap J$, and by ($a$), $\ker \varphi = IJ = 0$, and so we are done by the first isomorphism theorem (Thm. 11.4.2($b$)). □

*Solution for ($d$).* By ($b$), if $u + v = 1$ for $u \in I, v \in J$, then $\varphi(v) = (1, 0)$ and $\varphi(u) = (0, 1)$. Hence the idempotents corresponding to the product decomposition in ($c$) are the images of $u, v$ from partitions of unity $u + v = 1$ for $u \in I, v \in J$. □

## 11.7 Fractions

**Exercise 11.7.1.** *Prove that a domain of finite order is a field.*

*Proof.* Suppose $R$ is a finite domain, and consider $R^\times \coloneqq R \setminus \{0\}$. It suffices to show any $r \in R^\times$ is a unit. If $|R^\times| = n$, then $r \cdot R^\times \subset R^\times$ since $R$ is a domain, and $|r \cdot R^\times| = n$ by the cancellation law (11.7.1). Hence $1 \in r \cdot R^\times$, and so $rr' = 1$ for some $r' \in R^\times$. □

**Exercise 11.7.2.** *Let $R$ be a domain. Prove that the polynomial ring $R[x]$ is a domain, and identify the units in $R[x]$.*

*Proof.* Let $f, g \in R[x]$ be nonzero, and suppose $fg = 0$. If $\deg f = d$, $\deg g = d'$, then $\deg fg = d + d'$ since the product $a_d b_{d'}$ of their leading coefficients is nonzero, contradicting that $\deg fg$ is undefined. Hence $R[x]$ is a domain.

If $fg = 1$ then $\deg fg = d + d' = 0$, so $f$ and $g$ are constant polynomials. Viewing constant polynomials as elements of $R$, the units of $R[x]$ are then the units of $R$. □

**Exercise 11.7.3.** *Is there a domain that contains exactly* 15 *elements?*

*Solution.* Suppose $R$ is such a domain; it is a field by Exercise 11.7.1. It suffices to show any finite field $F$ has order $p^n$ for some prime power $p^n$, since 15 cannot be written in this way. By Lem. 3.2.10, $F$ has characteristic $p$ for some prime $p$, and so contains $\mathbb{F}_p$. Then, $F$ is of finite dimension $n$ as a vector space over $\mathbb{F}_p$, and so contains $p^n$ elements. □

**Exercise 11.7.4.** *Prove that the field of fractions of the formal power series $F[[x]]$ over a field $F$ can be obtained by inverting the element $x$. Find a neat description of the elements of that field (see Exercise* 11.2.2*).*

*Proof.* Take an element $\frac{f}{g}$ in the field of fractions of $F[[x]]$ and suppose $g = \sum_{i=n}^{\infty} a_i x^i$ with $n \geq 0$ and $a_n \neq 0$. Then, $g = x^n g_0$, where $g_0$ is a unit of $F[[x]]$ by Exercise 11.2.2, and so $\frac{f}{g} = \frac{f g_0^{-1}}{x^n}$. Thus, the field of fractions of $F[[x]]$ is contained in $F[[x]][x^{-1}]$, and the reverse inclusion is clear, and so the field of fractions of $F[[x]]$ is $F[[x]][x^{-1}]$.

This is the ring of infinite series of the form $h = \sum_{i \geq n} a_i x^i$ for $n \in \mathbb{Z}$, which is called the ring of formal Laurent series $F((x))$. □

## 11.8 Maximal Ideals

**Exercise 11.8.1.** *Which principal ideals in $\mathbb{Z}[x]$ are maximal ideals?*

*Solution.* We claim that none are. Suppose $(f) \subset \mathbb{Z}[x]$ is maximal. Then, $\deg f > 0$, for otherwise $(f) \subsetneq (f, x) \subsetneq \mathbb{Z}[x]$, contradicting maximality of $(f)$. Now choose $p$ such that $p \nmid a_i$ for any coefficient $a_i$ of $f$. Then, $(f) \subsetneq (p, f)$ since $p \notin (f)$, and $(p, f) \subsetneq \mathbb{Z}[x]$ since $\mathbb{Z}[x]/(p, f) = \mathbb{F}_p[x]/(f) \neq 0$. Thus, $(f)$ cannot be maximal. □

**Exercise 11.8.2.** *Determine the maximal ideals of each of the following rings:* (*a*) $\mathbb{R} \times \mathbb{R}$, (*b*) $\mathbb{R}[x]/(x^2)$, (*c*) $\mathbb{R}[x]/(x^2 - 3x + 2)$, (*d*) $\mathbb{R}[x]/(x^2 + x + 1)$.

*Solution for* (*a*). The units in $\mathbb{R} \times \mathbb{R}$ are elements $(a, b)$ for $a, b \neq 0$, and so any maximal ideal in $\mathbb{R} \times \mathbb{R}$ cannot contain a pair $(a, 0)$ and $(0, b)$ for $a, b \neq 0$. Hence every element in a maximal ideal of $\mathbb{R} \times \mathbb{R}$ must have the same coordinate equal to zero, and so it is of the form $\mathbb{R} \times 0$ or $0 \times \mathbb{R}$ since $0 \times 0$ is not maximal; these are maximal by Prop. 11.8.2(*b*) since taking quotients gives $\mathbb{R}$, a field. □

*Solution for* (*b*). The ideals in $\mathbb{R}[x]/(x^2)$ are the ideals in $\mathbb{R}[x]$ containing $(x^2)$ by the correspondence theorem (Thm. 11.4.3). Since $\mathbb{R}[x]$ is a PID by Props. 12.2.5, 12.2.7, the only proper ideals containing $(x^2)$ are $(x)$ and $(x^2)$, since if $x^2 \in (f)$, then $x^2 = fg$ implies $f \mid x^2$. We have $(x^2) \subsetneq (x)$, and so $(x)$ is the only maximal ideal. □

*Solution for* (*c*). $x^2 - 3x + 2 = (x - 2)(x - 1)$ and $(x - 2) + (x - 1) = \mathbb{R}[x]$ implies $\mathbb{R}[x]/(x^2 - 3x + 2) \approx \mathbb{R}[x]/(x - 1) \times \mathbb{R}[x]/(x - 2) \approx \mathbb{R} \times \mathbb{R}$ by Exercise 11.6.8(*c*). The maximal ideals of $\mathbb{R} \times \mathbb{R}$ are $\mathbb{R} \times 0$ and $0 \times \mathbb{R}$ as in (*a*), which correspond to $(x - 2), (x - 1)$, respectively, in $\mathbb{R}[x]/(x^2 - 3x + 2)$. □

*Solution for* (*d*). We note that $x^2 + x + 1$ has no real roots, and so is irreducible in $\mathbb{R}[x]$. Thus, $(x^2+x+1)$ maximal and $\mathbb{R}[x]/(x^2+x+1)$ is a field with unique maximal ideal (0) by Prop. 11.8.2. □

**Exercise 11.8.3.** *Prove that the ring* $\mathbb{F}_2[x]/(x^3+x+1)$ *is a field, but that* $\mathbb{F}_3[x]/(x^3+x+1)$ *is not a field.*

*Proof.* By Prop. 11.8.2(*b*), it suffices to show $(x^3+x+1)$ is maximal in $\mathbb{F}_2[x]$ but not in $\mathbb{F}_3[x]$. But this is true since $x^3+x+1$ has no roots in $\mathbb{F}_2$ ($0^3+0+1 = 1 = 1^3+1+1$), while $x^3+x+1$ has the root 1 in $\mathbb{F}_3$ ($1^3+1+1 = 0$), hence $(x^3+x+1) \subsetneq (x-1)$. □

**Exercise 11.8.4.** *Establish a bijective correspondence between maximal ideals of* $\mathbb{R}[x]$ *and points in the upper half plane.*

*Proof.* $\mathbb{R}[x]$ is a PID by Props. 12.2.5, 12.2.7, and so any maximal ideal is of the form $(f)$. But $(f)$ is maximal if and only if $f$ is an irreducible nonunit in $\mathbb{R}[x]$. Every polynomial in $\mathbb{R}[x]$ of degree at least 3 has a real root, and therefore is not irreducible. So, every maximal ideal is of the form $(f)$ for $f$ a linear polynomial or an irreducible quadratic polynomial.

Now recall we can identify the upper half plane with the subset of $\mathbb{C}$ of elements $z$ with $\mathrm{Im}(z) \geq 0$. Therefore, we can define the function $H$ that sends every maximal ideal $(f)$ to the root of $f$ in the upper half plane. Notice that the function is

well-defined: if $f$ is linear, then it has only one solution, a real number, and if $f$ is an irreducible quadratic polynomial, then $z$ and $\overline{z}$ are the roots of $f$, for some $z \in \mathbb{C} \setminus \mathbb{R}$, so only one of the roots is in the upper half-plane.

We need to show $H$ is a bijection. We define the inverse $H^{-1}$ sending $z$ to the ideal generated by $x - z$ if $z \in \mathbb{R}$, and $(x - z)(x - \overline{z})$ otherwise. $H^{-1}$ is clearly a two-sided inverse of $H$ since $(f) = (cf)$ for any $c \in \mathbb{R}$, and so we are done. □

## 11.9 Algebraic Geometry

**Exercise 11.9.4.** *Let $U$ and $V$ be varieties in $\mathbb{C}^n$. Prove that the union $U \cup V$ and the intersection $U \cap V$ are varieties. What does the statement $U \cap V = \emptyset$ mean algebraically? What about the statement $U \cup V = \mathbb{C}^n$?*

*Proof.* Let $U$ be defined by $\{f_1, \ldots, f_r\}$, and $V$ by $\{g_1, \ldots, g_s\}$. $U \cap V$ is defined by $\{f_1, \ldots, f_r, g_1, \ldots, g_s\}$ since $x \in U \cap V$ if and only if $f_i(x) = 0$ for all $i$ and $g_j(x) = 0$ for all $j$. We claim $U \cup V$ is equal to the variety $W$ defined by $\{f_i g_j\}_{i,j}$. $U \cup V \subset W$ since if $x \in U$ (resp. $V$), then $f_i = 0$ for all $i$ (resp. $g_j = 0$ for all $j$), hence $f_i g_j = 0$ for all $i, j$. Conversely, suppose $x \in W \setminus U \cup V$. Then, there exists $i_0, j_0$ such that $f_{i_0}(x), g_{j_0}(x) \neq 0$, and so $f_{i_0} g_{j_0} \neq 0$, a contradiction.

Now by Thm. 11.9.1 and Cor. 11.9.3, $U \cap V = \emptyset$ if and only if the quotient ring $\mathbb{C}[x_1, \ldots, x_n]/(f_1, \ldots, f_r, g_1, \ldots, g_s) = 0$, i.e., $(f_1, \ldots, f_r, g_1, \ldots, g_s) = (1)$.

Now $U \cup V = \mathbb{C}^n$ if and only if any point $x \in \mathbb{C}^n$ is a common zero of all $f_i g_j$. But there are only finitely many $f_i g_j$ with finitely many zeros each, and so this holds if and only if all the $f_i g_j$ are equal to 0, which is true if and only if all the $f_i$ or all the $g_j$ are 0, if and only if $U$ or $V$ equals $\mathbb{C}^n$. □

**Exercise 11.9.5.** *Prove that the variety of zeros of a set $\{f_1, \ldots, f_r\}$ of polynomials depends only on the ideal they generate.*

*Proof.* For sets of polynomials $\{f_1, \ldots, f_r\}$ and $\{g_1, \ldots, g_s\}$, let $V, W$ be the varieties formed by their zero sets and let $I, J$ be the ideals they generate, respectively. We claim $I \supset J$ implies $V \subset W$. Every $g_j$ can then be written as a linear combination of the $f_i$, hence if $x \in V$, $f_i(x) = 0$ for all $i$, and so $g_j(x) = \sum a_i f_i(x) = 0$ for all $j$ as well, i.e., $V \subset W$.

Finally, if $I = J$, then $V \subset W$ and $W \subset V$, and so $V = W$. Thus, the variety defined by a set $\{f_1, \ldots, f_r\}$ depends only on the ideal $(f_1, \ldots, f_r)$. □

**Exercise 11.9.6.** *Prove that every variety in $\mathbb{C}^2$ is the union of finitely many points and algebraic curves.*

*Proof.* Let $U$ be defined by $\{f_1, \ldots, f_r\}$, and let $g = \gcd(f_1, \ldots, f_r)$; $g$ exists since $\mathbb{C}[x, y]$ is a UFD (Thm. 12.3.10). Then, $U = V \cup W$, where $V$ is defined by $g$ and $W$ by $\{f_1/g, \ldots, f_r/g\}$ as in Exercise 11.9.4. $W$ is the union of finitely many points by Thm. 11.9.10 since $\gcd(\gcd(f_1/g, \ldots, f_{r-1}/g), f_r/g) = \gcd(f_1/g, \ldots, f_r/g) = 1$. $V$ is the union of finitely many algebraic curves since $g = \prod g_i$ for some irreducible polynomials $g_i$, hence $V$ is the union of curves defined by $g_i$ as in Exercise 11.9.4. □

**Exercise 11.9.11.** *Let $C_1$ and $C_2$ be the zeros of quadratic polynomials $f_1$ and $f_2$ respectively that don't have a common linear factor.*

(*a*) *Let $p$ and $q$ be distinct points of intersection of $C_1$ and $C_2$, and let $L$ be the (complex) line through $p$ and $q$. Prove that there are constants $c_1$ and $c_2$, not both zero, so that $g = c_1 f_1 + c_2 f_2$ vanishes identically on $L$. Prove also that $g$ is the product of linear polynomials.*

(*b*) *Prove that $C_1$ and $C_2$ have at most 4 points in common.*

*Proof of* (*a*). Let $\lambda(t) = (1-t)p + tq$ parametrize $L \subset \mathbb{C}^2$. Then, $f_1(\lambda(t)), f_2(\lambda(t))$ are quadratic in $t$, and so $c_1 f_1(\lambda(t)) + c_2 f_2(\lambda(t))$ is at most quadratic in $t$ for any $c_i \in \mathbb{C}$. Let $t_0 \in \mathbb{C} \setminus \{0, 1\}$, and choose $c_i$ such that $c_1 f_1(\lambda(t_0)) + c_2 f_2(\lambda(t_0)) = 0$; we can moreover choose $c_i$ to be nonzero. Then, $h(t) = c_1 f_1(\lambda(t)) + c_2 f_2(\lambda(t))$ is at most quadratic in $t$ hence has at most two zeros if $h \neq 0$ by the fundamental theorem of algebra (Thm. 15.10.1); but $h(0) = h(1) = h(t_0) = 0$ implies $h(t) = 0$. Hence $g = c_1 f_1 + c_2 f_2$ vanishes identically on $L$.

Now since $g$ vanishes on $L$, by unique factorization (Thm. 12.3.10) $g = g_L g'$ for some linear polynomial $g_L$ that defines $L$. $g$ is at most quadratic, hence $g'$ is either linear or constant. In either case, $g$ is then a product of linear polynomials. □

*Proof of* (*b*). Suppose $C_1 \cap C_2$ contains more than four points. Let $g$ as in (*a*). Then, $g = c_1 f_1 + c_2 f_2$ implies that $C_1 \cap C_2 \subset \{g = 0\}$. $g$ is either the product of one or two linear polynomials as in (*a*), and so $C_1 \cap C_2$ is contained in either one or two lines. In either case, this implies at least three points in $C_1 \cap C_2$ lie on one line parametrized by $\eta(t)$. Then, $f_1(\eta(t)), f_2(\eta(t))$ are quadratic and both vanish at three values of $t$, and so $f_1(\eta(t)) = f_2(\eta(t)) = 0$ by the fundamental theorem of algebra (Thm. 15.10.1). Thus, $f_1, f_2$ have infinitely many common zeros in $\mathbb{C}^2$, hence have a common linear factor by Thm. 11.9.10, a contradiction. □

**Exercise 11.9.12.** *Prove in two ways that the three polynomials $f_1 = t^2 + x^2 - 2$, $f_2 = tx - 1$, $f_3 = t^3 + 5tx^2 + 1$ generate the unit ideal in $\mathbb{C}[x, t]$ in two ways: by showing that they have no common zeros, and also by writing 1 as a linear combination of $f_1$, $f_2$, and $f_3$ with polynomial coefficients.*

*Proof.* We first show that there are no common zeros. If $f_2(x,t) = 0$, then $x, t \neq 0$ and $t = x^{-1}$. Thus,

$$f_1(x, x^{-1}) = x^2 - 2 + x^{-2} = x^{-2}(x^4 - 2x^2 + 1) = x^{-2}(x^2 - 1)^2,$$

hence if $f(x,t) = 0$ as well, then $(x,t) = \pm(1,1)$. But $f_3(1,1) = 7, f_3(-1,-1) = -5$, hence $f_1, f_2, f_3$ have no common zeros, and $(f_1, f_2, f_3) = (1)$ by Exercise 11.9.4.

Now we write 1 as a linear combination of $f_1, f_2, f_3$. 1 can be expressed as

$$\frac{1}{1225}\begin{pmatrix} (-6t^2x - 24tx^2 & - 142t^2 - 352tx & + 53t & - 36x & )f_1 \\ + (\ 12t^2x - 24tx^2 - 36x^3 + 284t^2 - 568tx + 12x^2 & & + 36t + 140x - 1278)f_2 \\ + (\ & 6tx + 12x^2 + 142t & + 68x & - 53)f_3 \end{pmatrix}$$

which we found by using Macaulay2. □

**Exercise 11.9.13.** *Let $\varphi\colon \mathbb{C}[x,y] \to \mathbb{C}[t]$ be a homomorphism that is the identity on $\mathbb{C}$ and sends $x \rightsquigarrow x(t)$, $y \rightsquigarrow y(t)$ and such that $x(t)$ and $y(t)$ are not both constant. Prove that the kernel of $\varphi$ is a principal ideal.*

*Proof.* We claim $\ker\varphi$ is principal. If not, then $\ker\varphi$ contains two elements $f, g$ that do not have a common factor. We claim they do not have a common factor in $\mathbb{C}(x)[y]$. For, suppose $h \in \mathbb{C}(x)[y]$ is a common factor; then, $h = a^{-1}h_0$ for some $a \in \mathbb{C}[x]$, $h_0 \in \mathbb{C}[x,y]$ by clearing denominator. Assuming without loss of generality that nothing of the form $x - \alpha$ divides $h_0$, then $h_0$ divides $f, g$ in $\mathbb{C}(x)[y]$, hence also does in $\mathbb{C}[x,y]$ by Prop. 11.9.9, contradicting that $f, g$ do not have a common factor.

Therefore, there exist $r_0, s_0 \in \mathbb{C}(x)[y]$ such that $r_0 f + s_0 g = 1$, and clearing denominators we get $rf + sg = q \in \mathbb{C}[x]$ for some $r, s \in \mathbb{C}[x]$. This implies $\ker\varphi \cap \mathbb{C}[x]$ is nontrivial, but this is a contradiction for any $g \in \ker\varphi \cap \mathbb{C}[x]$ must satisfy $g(x(t)) = 0$ for all $t$, hence $g = 0$. □

## 11.M Miscellaneous Problems

**Exercise 11.M.3.** *Let $R$ denote the set of sequences $a = (a_1, a_2, a_3, \ldots)$ of real numbers that are eventually constant: $a_n = a_{n+1} = \ldots$ for sufficiently large $n$. Addition and multiplication are componentwise, that is, addition is vector addition and multiplication is defined by $ab = (a_1b_1, a_2b_2, \ldots)$. Prove that $R$ is a ring, and determine its maximal ideals.*

*Proof.* Denote $\overline{a}$ to be the real number $a$ converges to. $R$ is a ring since sums and products of eventually constant sequences are eventually constant, commutativity

and associativity of $+, \times$ and the distributive property follow since addition and multiplication are defined componentwise, and $R$ has additive identity $(0, 0, \ldots)$, additive inverses $-a = (-a_1, -a_2, \ldots)$ for $a$, and multiplicative identity $(1, 1, \ldots)$.

We now want to find its maximal ideals. Consider for each $i \in \mathbb{Z}_{>0}$ the map $\varphi_i \colon R \to \mathbb{R}$ defined by $a \rightsquigarrow a_i$; since $+, \times$ are defined termwise, and $0 \rightsquigarrow 0$, this defines a ring homomorphism. It is moreover surjective, hence $\mathfrak{m}_i \coloneqq \ker \varphi_i = \{a \mid a_i = 0\}$ is maximal by Prop. 11.8.2$(a)$. Now consider the map $\varphi_\infty \colon R \to \mathbb{R}$ defined by mapping $a$ to the real number it converges to; since $0 \rightsquigarrow 0$ and $\overline{a+b} = \overline{a} + \overline{b}, \overline{ab} = \overline{a}\overline{b}$, this defines a ring homomorphism. It is moreover surjective, hence $\mathfrak{m}_\infty \coloneqq \ker \varphi_\infty = \{a \mid \overline{a} = 0\}$ is maximal by Prop. 11.8.2$(a)$.

We claim these are all the maximal ideals. It suffices to show if $\mathfrak{m} \subset R$ is maximal and not equal to $\mathfrak{m}_i$, it is equal to $\mathfrak{m}_\infty$. So suppose not; then, there exists $a \in \mathfrak{m}$ such that $\overline{a} \neq 0$. There are therefore finitely many $i$ such that $a_i = 0$. Since $\mathfrak{m} \neq \mathfrak{m}_i$, for each $i$ there exists a sequence $a^i$ with $a^i_i \neq 0$; we can moreover assume $a^i_j = 0$ for all $j \neq i$ by multiplying by the sequence in $R$ with 1 in the $i$th index and 0 otherwise.

$$b = a + \sum_{\{i \mid a_i = 0\}} a^i \in \mathfrak{m}$$

is then a unit in $\mathfrak{m}$, since $b_i \neq 0$ for all $i$, contradicting maximality of $\mathfrak{m}$. □

**Exercise 11.M.4.**

$(a)$ *Classify rings $R$ that contain $\mathbb{C}$ and have dimension 2 as a vector space over $\mathbb{C}$.*

$(b)$ *Do the same for rings that have dimension 3.*

*Solution for $(a)$.* Let $\{1, r\}$ be a basis for $R$, and let $\varphi \colon \mathbb{C}[x] \to R$ be defined by $1 \rightsquigarrow 1, x \rightsquigarrow r$. $\varphi$ is then surjective, and $\ker \varphi = (f)$ for some $f \in \mathbb{C}[x]$ since $\mathbb{C}[x]$ is a PID (Props. 12.2.5, 12.2.7), giving $R \approx \mathbb{C}[x]/(f)$ by the first isomorphism theorem (Thm. 11.4.2$(b)$). $\deg f > 1$ since otherwise $\{1, r\}$ would be linearly dependent; since $r^2 = ar + b \in R$ for some $a, b \in \mathbb{C}$, we then have $f = x^2 - ax - b = (x - \zeta_1)(x - \zeta_2)$ for some $\zeta_1, \zeta_2 \in \mathbb{C}$. If $\zeta_1 = \zeta_2 =: \zeta$, then

$$R \approx \mathbb{C}[x]/(f) \approx \mathbb{C}[x]/(x^2)$$

by composing with the isomorphism defined by $x \rightsquigarrow x + \zeta$. If $\zeta_1 \neq \zeta_2$, then $(x - \zeta_1) + (x - \zeta_2) = R$ as ideals, hence

$$R \approx \mathbb{C}[x]/(f) \approx \mathbb{C}[x]/(x - \zeta_1) \times \mathbb{C}[x]/(x - \zeta_2) \approx \mathbb{C} \times \mathbb{C}$$

by Exercise 11.6.8$(c)$. Hence the two possibilities are $R \approx \mathbb{C}[x]/(x^2)$ or $\mathbb{C} \times \mathbb{C}$. □

*Solution for* $(b)$. Suppose there exists $r \in R$ such that $\{1, r, r^2\}$ is a basis for $R$. Then, defining the map $\varphi\colon \mathbb{C}[x] \to R$ by $x \rightsquigarrow r$, we again have that $\ker \varphi = (f)$ for $\deg f > 2$, since if $\deg f \leq 2$ then $\{1, r, r^2\}$ would not be linearly independent. Also, $r^3 = ar^2 + br + c$ for some $a, b, c \in \mathbb{C}$, and so $f = x^3 - ax^2 - bx - c$. If $f$ has one triple root $\zeta$, then

$$R \approx \mathbb{C}[x]/((x-\zeta)^3) \approx \mathbb{C}[x]/(x^3).$$

If $f$ has a double root $\zeta$ and a simple root $\zeta'$, then since $((x-\zeta)^2) + (x - \zeta') = R$ as ideals,

$$\begin{aligned} R &\approx \mathbb{C}[x]/((x-\zeta)^2)(x-\zeta')) \\ &\approx \mathbb{C}[x]/((x-\zeta)^2) \times \mathbb{C}[x]/(x-\zeta') \\ &\approx \mathbb{C}[x]/(x^2) \times \mathbb{C} \end{aligned}$$

by the same argument as before. Finally, if $f$ has three distinct roots, then

$$\begin{aligned} R &\approx \mathbb{C}[x]/((x-\zeta_1)(x-\zeta_2)(x-\zeta_3)) \\ &\approx \mathbb{C}[x]/(x-\zeta_1) \times \mathbb{C}[x]/(x-\zeta_2) \times \mathbb{C}[x]/(x-\zeta_3) \\ &\approx \mathbb{C} \times \mathbb{C} \times \mathbb{C} \end{aligned}$$

by repeated applications of Exercise 11.6.8$(c)$ since, for example, $((x-\zeta_1)(x-\zeta_2)) + (x-\zeta_3) = R$ as ideals.

Now suppose no $r \in R$ exists such that $\{1, r, r^2\}$ is a basis for $R$. Thus, if $\{1, r, s\}$ is a basis for $R$, then

$$r^2 = a_1 r + c_1, \quad s^2 = b_2 s + c_2, \quad rs = a_3 r + b_3 s + c_3$$

for some $a_i, b_i, c_i \in \mathbb{C}$. We claim we can assume $c_1 = c_2 = 0$. For, changing coordinates $r \rightsquigarrow r + \alpha$ gives

$$(r+\alpha)^2 = a_1(r+\alpha) + c_1 \implies r^2 = (a_1 - 2\alpha)r - (\alpha^2 + a_1\alpha - c_1),$$

and so letting $\alpha$ be such that $\alpha^2 + a_1\alpha - c_1 = 0$, we have $r^2 = a_1 r$. Similarly for $s$, we have $s^2 = b_2 s$. We then have

$$\begin{aligned} (r+zs)^2 &= r^2 + 2zrs + z^2 s^2 \\ &= (a_1 + 2a_3 z)r + (b_2 z^2 + 2b_3 z)s + 2c_3 z \\ &= A_z(r+s) + B_z \end{aligned}$$

for some $A_z, B_z \in \mathbb{C}$ since $\{1, r+zs, (r+zs)^2\}$ is linearly dependent. Thus,

$$A_z = a_1 + 2a_3 z = b_2 z^2 + 2b_3 z, \quad B_z = 2c_3 z.$$

Since the first equation must hold for all $z$, we have $a_1 = b_2 = 0$, hence $r^2 = s^2 = 0$, and also $a_3 = b_3$. This implies $(rs)^2 = r^2 s^2 = 0$, but since also

$$\begin{aligned}(rs)^2 &= (a_3 r + a_3 s + c_3)^2 \\ &= 2a_3^2 rs + 2a_3 c_3 r + 2a_3 c_3 s + c_3^2 \\ &= 2a_3(a_3^2 + c_3)r + 2a_3(a_3^2 + c_3)s + c_3(2a_3^2 + c_3),\end{aligned}$$

we have $a_3(a_3^2 + c_3) = c_3(2a_3^2 + c_3) = 0$. If one of $a_3, c_3$ is nonzero, then the other is also. But this is impossible, and so we have $a_3 = b_3 = c_3 = 0$.

Finally, let $\varphi\colon \mathbb{C}[x,y] \to R$ be defined by $1 \rightsquigarrow 1, x \rightsquigarrow r, y \rightsquigarrow s$. $\varphi$ is then surjective, giving $R \approx \mathbb{C}[x,y]/\ker\varphi$ by the first isomorphism theorem (Thm. 11.4.2($b$)). We know $I \coloneqq (x^2, y^2, xy) \subset \ker\varphi$, and the reverse inclusion holds since for any $f \in \mathbb{C}[x,y]$, $f \equiv \alpha r + \beta s + \gamma \bmod I$ for some $\alpha, \beta, \gamma \in \mathbb{C}$, and $f \rightsquigarrow 0$ in the composition $\mathbb{C}[x,y]/I \to \mathbb{C}[x,y]/\ker\varphi \to R$ if and only if $\alpha = \beta = \gamma = 0$ since $\{1, r, s\}$ is a basis for $R$, i.e., if and only if $f \in I$. Thus, in this case $R \approx \mathbb{C}[x,y]/(x^2, y^2, xy)$.

In summary, there are four possibilities for $R$:

$$\mathbb{C}[x,y]/(x^2, y^2, xy), \quad \mathbb{C}[x]/(x^3), \quad \mathbb{C}[x]/(x^2) \times \mathbb{C}, \quad \mathbb{C} \times \mathbb{C} \times \mathbb{C}. \qquad \square$$

# 12 Factoring

## 12.1 Factoring Integers

**Exercise 12.1.4.** *Solve the following simultaneous congruences:*
($a$) $x \equiv 3$ *modulo* 8, $x \equiv 2$ *modulo* 5,
($b$) $x \equiv 3$ *modulo* 15, $x \equiv 5$ *modulo* 8, $x \equiv 2$ *modulo* 7,
($c$) $x \equiv 13$ *modulo* 43, $x \equiv 7$ *modulo* 71.

*Solution for* ($a$). $x = 27 = 8 \cdot 3 + 3 = 5 \cdot 5 + 2$. $\square$

*Solution for* ($b$). $x = 93 = 15 \cdot 6 + 3 = 8 \cdot 11 + 5 = 7 \cdot 13 + 2$. $\square$

*Solution for* ($c$). $x = 2421 = 56 \cdot 34 + 13 = 34 \cdot 71 + 7$. $\square$

**Exercise 12.1.5.** *Let $a$ and $b$ be relatively prime integers. Prove that there are integers $m$ and $n$ such that $a^m + b^n = 1$ modulo $ab$.*

*Proof.* Since $a, b$ are relatively prime, $a^m + b^n = 1 \bmod ab$ if and only if $a^m + b^n = 1 \bmod a$ and $a^m + b^n = 1 \bmod b$. Note $a^m + b^n = b^n \bmod a$, and $a^m + b^n = a^m \bmod b$.

Now consider $a, a^2, a^3, \ldots \bmod b$. There are only $b$ equivalence classes $0, 1, \ldots, b-1 \bmod b$, hence for some $i < j$ we have $a^i \equiv a^j \bmod b$. Then, $a^i(a^{j-i} - 1) \equiv 0 \bmod b$, and so $b \mid a^i(a^{j-i} - 1)$. But $a, b$ are relatively prime, hence $b \mid a^{j-i} - 1$. Thus, letting $m \coloneqq j - i$, we have $a^m \equiv 1 \bmod b$.

By the same argument working mod $a$, there exists $n$ such that $b^n \equiv 1 \bmod a$, and so $a^m + b^n \equiv 1 \bmod a$ and $\bmod b$, hence $a^m + b^n \equiv 1 \bmod ab$. □

## 12.2 Unique Factorization Domains

**Exercise 12.2.1.** *Factor the following polynomials into irreducible factors in* $\mathbb{F}_p[x]$. *(a)* $x^3 + x^2 + x + 1, p = 2$, *(b)* $x^2 - 3x - 3, p = 5$, *(c)* $x^2 + 1, p = 7$

*Solution for (a).* Let $f(x) = x^3 + x^2 + x + 1$. Since $f(1) = 0$, we can then factor out $x + 1$ to get $f(x) = (x + 1)(x^2 + 1)$. Now since $1^2 + 1 = 0$, $x^2 + 1$ can be factored into $(x + 1)(x + 1)$, and so we have $f(x) = (x + 1)^3$. □

*Solution for (b).* Let $f(x) = x^2 - 3x - 3$. Since $f(1) = f(2) = 0$, we claim $f(x) = (x-1)(x-2)$; this follows since $(x-1)(x-2) = x^2-3x+2 \equiv x^2-3x-3 \mod 5$. □

*Solution for (c).* Since $f(x) = x^2 + 1 \neq 0$ for all $x \in \mathbb{F}_7$ ($f(0) = 1, f(1) = 2, f(2) = 5, f(3) = 3, f(4) = 3, f(5) = 5, f(6) = 2$), we know it is irreducible in $\mathbb{F}_7[x]$. □

**Exercise 12.2.2.** *Compute the greatest common divisor of the polynomials* $x^6+x^4+x^3+x^2+x+1$ *and* $x^5 + 2x^3 + x^2 + x + 1$ *in* $\mathbb{Q}[x]$.

*Solution.* We perform the Euclidean algorithm (p. 45):

$$\begin{aligned}
x^6 + x^4 + x^3 + x^2 + x + 1 &= x(x^5 + 2x^3 + x^2 + x + 1) + (-x^4 + 1) \\
x^5 + 2x^3 + x^2 + x + 1 &= -x(-x^4 + 1) + (2x^3 + x^2 + 2x + 1) \\
-x^4 + 1 &= \left(-\frac{x}{2} + \frac{1}{4}\right)(2x^3 + x^2 + 2x + 1) + \left(\frac{3}{4}x^2 + \frac{3}{4}\right) \\
2x^3 + x^2 + 2x + 1 &= \left(\frac{3}{4}x^2 + \frac{3}{4}\right)\frac{8}{3}x + 0
\end{aligned}$$

Since the last nonzero remainder is $\frac{3}{4}x^2+\frac{3}{4}$, the greatest common divisor is $x^2+1$. □

**Exercise 12.2.5** (partial fractions for polynomials)**.**

(a) *Prove that every element of* $\mathbb{C}(x)$ *can be written as a sum of a polynomial and a linear combination of functions of the form* $1/(x - a)^i$.

(b) *Exhibit a basis for the field* $\mathbb{C}(x)$ *of rational functions as vector space over* $\mathbb{C}$.

*Proof of* $(a)$. We first show that $f(x)/(x-a)^i \in \mathbb{C}(x)$ can be so written, where $(x-a)^i \nmid f(x) \in \mathbb{C}[x]$. We apply the Euclidean algorithm (p. 45) considering $f(x)$ as an element in $\mathbb{C}[x]$ $i$ times to obtain

$$\begin{aligned} f(x) &= q_1(x)(x-a) + r_1 \\ &= (q_2(x)(x-a) + r_2)(x-a) + r_1 \\ &\vdots \\ &= q_i(x)(x-a)^i + r_{i-1}(x-a)^{i-1} + \cdots + r_2(x-a) + r_1, \end{aligned}$$

for some $r_j \in \mathbb{C}$, and $q_i(x) \in \mathbb{C}(x)$. Dividing this out by $(x-a)^i$, we have

$$\frac{f(x)}{(x-a)^i} = q_i(x) + \frac{r_{i-1}}{(x-a)} + \cdots + \frac{r_2}{(x-a)^{i-1}} + \frac{r_1}{(x-a)^i}.$$

Now suppose we have arbitrary $f(x)/g(x) \in \mathbb{C}(x)$, where we can assume without loss of generality that $\gcd(f,g) = 1$. We can first write $g(x) = \prod_{i=1}^{n}(x-a_i)^{\alpha_i}$ for $a_i \in \mathbb{C}$, $\alpha_i \in \mathbb{N}$, by the fundamental theorem of algebra (Thm. 15.10.1) (and moving any unit factor into $f(x)$). If $n = 1$, we are done by the above, and so we proceed by induction on $n$. If $g(x)$ has $n$ distinct roots, we can write $g(x) = (x-a)^j h(x)$ for some $a \in \mathbb{C}$, $j \in \mathbb{N}$, $h(x) \in \mathbb{C}[x]$ where $h(x)$ has $n-1$ distinct roots. Since $(x-a)^j, h(x)$ share no roots, they are relatively prime and so $1 = r(x)(x-a)^j + s(x)h(x)$ for some $r(x), s(x) \in \mathbb{C}[x]$. Multiplying throughout by $f(x)/g(x)$ gives

$$\frac{f(x)}{g(x)} = \frac{r(x)}{h(x)} + \frac{s(x)}{(x-a)^j},$$

where the first term can be written as in the statement by inductive hypothesis, and the second by the above paragraph. □

*Proof of* $(b)$. We claim that

$$\mathcal{B} = \{x^i : i \in \mathbb{N}\} \bigcup \left\{ \frac{1}{(x-a)^i} : a \in \mathbb{C}, i \in \mathbb{N} \right\}$$

is a basis for $\mathbb{C}(x)$ over $\mathbb{C}$. We see that this set spans $\mathbb{C}(x)$ by $(a)$; it suffices to show that any finite subset of this set is linearly independent to show this is a basis. Let $S \subsetneq \mathcal{B}$ be finite, and suppose it is linearly dependent. Then,

$$\sum_{j \in J} c_j x^j + \sum_{i \in I} \frac{b_i}{(x-a_i)^{\alpha_i}} = 0,$$

where $J$ indexes the $x^j \in S$ and $I$ the $1/(x-a_i)^{\alpha_i} \in S$. Let $D(x)$ be the product of all the denominators appearing in the sum on the right; then,

$$D(x)\left(\sum_{j\in J} c_j x^j + \sum_{i\in I} \frac{b_i}{(x-a_i)^{\alpha_i}}\right) = 0,$$

and so $c_j = 0$ for all $j$ since the powers of $x$ that come from the sum over $J$ have higher degree than those that come from the sum over $I$. Thus, we have

$$D(x)\sum_{i\in I} \frac{b_i}{(x-a_i)^{\alpha_i}} = 0.$$

But then, all the $b_i$ must equal zero, for suppose not. Then, we can write

$$D(x)\sum_{\{i\in I | a_1 \neq a_i\}} \frac{b_i}{(x-a_i)^{\alpha_i}} = -D(x)\sum_{\{i\in I | a_1 = a_i\}} \frac{b_i}{(x-a_i)^{\alpha_i}}$$

Note that the left side has all terms divisible by $x-a_1$, while the right side has no terms divisible by $x-a_1$. Suppose the right side is zero; then the left side is nonzero mod $x-a'$ for any $a' \neq a_1$, while the right side is zero mod $x-a'$. If the right side is nonzero, then the left side is zero mod $x-a_1$ and the right side is nonzero mod $x-a_1$. In either case this is a contradiction, and so $c_j = b_i = 0$ for all $i, j$, and $\mathcal{B}$ is linearly independent. □

**Exercise 12.2.6.** *Prove that the following are Euclidean domains:*
*(a)* $\mathbb{Z}[\omega]$, $\omega = e^{2\pi i/3}$; *(b)* $\mathbb{Z}[\sqrt{-2}]$.

*Proof.* Let $\alpha = \omega$ or $\sqrt{-2}$. In either case $\mathbb{Z}[\alpha] = \{x + y\alpha \mid x, y \in \mathbb{Z}\}$. We claim that $\sigma(x+y\alpha) \coloneqq |x+y\alpha|^2$ is an appropriate size function. This simplifies to

$$\sigma(x+y\alpha) = |x+y\alpha|^2 = (x+y\alpha)(x+y\overline{\alpha}) = x^2 + xt(\alpha+\overline{\alpha}) + y^2|\alpha|^2. \tag{2}$$

We claim this is a nonnegative integer in both cases. If $\alpha = \omega$, then $\omega + \overline{\omega} = -1$ and $|\alpha|^2 = 1$, and so

$$\sigma(x+y\alpha) = x^2 - xy + y^2 \geq x^2 - 2xy + y^2 = (x-y)^2 \in \mathbb{Z}_{\geq 0}.$$

If $\alpha = \sqrt{-2}$, then $\sqrt{-2} + \overline{\sqrt{-2}} = 0$ and $|\sqrt{-2}|^2 = 2$, and so

$$\sigma(x+y\alpha) = x^2 + 2y^2 \in \mathbb{Z}_{\geq 0}.$$

Now suppose $a, b \in \mathbb{Z}[\alpha]$ are given; we want to show the property in (12.2.4) holds. First, we have

$$\frac{b}{a} = \frac{b\overline{a}}{|a|^2} = s + t\omega,$$

for some $p, q \in \mathbb{Q}$, since $b\overline{a} \in \mathbb{Z}[\alpha]$ and $|a|^2 \in \mathbb{Z}$ by (2). We can then find $q \in \mathbb{Z}[\alpha]$ close to $s + t\alpha$, by letting

$$q = x + y\alpha, \quad \text{where } |x - s| \leq \frac{1}{2},\ |y - t| \leq \frac{1}{2},$$

which is possible since every rational lies within $1/2$ of an integer. By (2), if $\alpha = \omega$,

$$\left|\frac{b}{a} - q\right|^2 = |(s - x) + (t - y)\omega|^2 = (s - x)^2 - (s - x)(t - y) + (t - y)^2 \leq \frac{3}{4} < 1,$$

and if $\alpha = \sqrt{-2}$,

$$\left|\frac{b}{a} - q\right|^2 = \left|(s - x) + (t - y)\sqrt{-2}\right|^2 = (s - x)^2 + 2(t - y)^2 \leq \frac{3}{4} < 1.$$

Multiplying throughout by $|a|^2$ and letting $r = b - aq$, we either get $r = 0$ or

$$\sigma(r) = |b - aq|^2 < |a|^2 = \sigma(a),$$

and so our function is an appropriate size function. □

**Exercise 12.2.9.** *Let $F$ be a field. Prove that the ring $F[x, x^{-1}]$ of Laurent polynomials (Chapter 11, Exercise 5.7) is a principal ideal domain.*

*Proof.* It suffices by Prop. 12.2.7 to show that $F[x, x^{-1}]$ is a Euclidean domain. We define the size function $\sigma(f)$ as $\deg_+(f) - \deg_-(f)$, where $\deg_+(f)$ denotes the largest power of $x$ in $f$ and $\deg_-(f)$ denotes the smallest power of $x$ in $f$, both including negative powers. $\sigma(f) \in \mathbb{Z}_{\geq 0}$ by considering possible values for the degree function. Now consider the Euclidean algorithm on $f$ where we divide by $g$. Let $p = x^{-\deg_-(f)}$ and $q = x^{-\deg_-(g)}$; note they are both units in $F[x, x^{-1}]$. Then, $fp, gq$ have all non-negative exponents and

$$\deg(gq) = \deg_+(gq) = \deg_+(g) - \deg_-(g) = \sigma(g).$$

Thus, $fp, gq \in F[x]$. We can then apply the Euclidean algorithm (p. 45) on $fp, gq$ in $F[x]$ to get $(fp) = r(gq) + s$, where $r, s \in F[x]$, and $s = 0$ or $\deg(s) < \deg(gq)$ by the Euclidean algorithm in $F[x]$. Then, dividing by $p$ throughout, we get $f = g(rqp^{-1}) + sp^{-1}$, and (12.2.4) holds since either $sp^{-1} = 0$, or

$$\sigma(sp^{-1}) = \sigma(s) = \deg(s) < \deg(gq) = \sigma(g).$$ □

## 12.3 Gauss's Lemma

**Exercise 12.3.1.** *Let $\varphi$ denote the homomorphism $\mathbb{Z}[x] \to \mathbb{R}$ defined by*
*(a) $\varphi(x) = 1 + \sqrt{2}$, (b) $\varphi(x) = \frac{1}{2} + \sqrt{2}$.*
*Is the kernel of $\varphi$ a principal ideal? If so, find a generator.*

*Solution for (a).* We want to find the polynomials $f(x)$ such that $f(1+\sqrt{2}) = 0$. Using the canonical embedding of $\mathbb{Z}[x]$ into $\mathbb{R}[x]$, we see that $(x - (1+\sqrt{2}))$ would generate the kernel of $\varphi$ in $\mathbb{R}[x]$. But then, since $(x-(1+\sqrt{2}))(x-(1-\sqrt{2})) = x^2 - 2x - 1$, and $(x^2 - 2x - 1) \subseteq \mathbb{Z}[x]$, we obtain $(x^2 - 2x - 1) \subseteq \ker\varphi$, as an ideal in $\mathbb{Z}[x]$. But since $x^2 - 2x - 1$ is primitive and irreducible in $\mathbb{Q}[x]$, since its roots are $(1 \pm \sqrt{2})$, $x^2 - 2x - 1$ is irreducible in $\mathbb{Z}[x]$ by Prop. 12.3.7$(a)$. Now suppose that $f(x) \in \ker\varphi \setminus (x^2 - 2x - 1)$. By the Euclidean algorithm dividing $f(x)$ by $x^2 - 2x - 1$, we can assume without loss of generality that $f(x) = ax + b$. But then, $\varphi(f) = a + a\sqrt{2} + b \neq 0$ unless $a = b = 0$, and so we see that $(x^2 - 2x - 1) = \ker\varphi$. □

*Solution for (b).* We proceed similarly to $(a)$. Considering the embedding of $\mathbb{Z}[x]$ into $\mathbb{R}[x]$, we first see that $(x - (\frac{1}{2} + \sqrt{2}))$ would generate the kernel in $\mathbb{R}[x]$, which contains $(x - (\frac{1}{2} + \sqrt{2}))(x - (\frac{1}{2} - \sqrt{2})) = x^2 - x - \frac{7}{4}$. $x^2 - x - \frac{7}{4}$ is in $\mathbb{Q}[x]$, and is irreducible since the roots are in the extension $\mathbb{R}[x]$ as in $(a)$. But then since $\mathbb{Q}$ is a field, $(4x^2 - 4x - 7) = \left(x^2 - x - \frac{7}{4}\right)$ as ideals. This former ideal is generated by a primitive and irreducible element in $\mathbb{Q}[x]$, which as an element of $\mathbb{Z}[x]$ is irreducible as well by Prop. 12.3.7$(a)$. We thus have $(4x^2 - 4x - 7) \subseteq \ker\varphi$. Now suppose that $f(x) \in \ker\varphi \setminus (4x^2 - 4x - 7)$. But taking the canonical embedding of $\mathbb{Z}[x]$ into $\mathbb{Q}[x]$, and seeing that the latter is a principal ideal domain since $\mathbb{Q}$ is a field, we obtain that $f(x) \in (4x^2 - 4x - 7)$ as an ideal in $\mathbb{Q}[x]$. But then, $4x^2 - 4x - 7 \mid f(x)$ in $\mathbb{Q}[x]$, and by Thm. 12.3.6, this implies $4x^2 - 4x - 7 \mid f(x)$ in $\mathbb{Z}[x]$; thus $(4x^2 - 4x - 7) = \ker\varphi$. □

**Exercise 12.3.2.** *Prove that two integer polynomials are relatively prime elements of $\mathbb{Q}[x]$ if and only if the ideal they generate in $\mathbb{Z}[x]$ contains an integer.*

*Proof.* $f, g \in \mathbb{Z}[x]$ are relatively prime in $\mathbb{Q}[x]$ if and only if $af + bg = 1$ for some $a, b \in \mathbb{Q}[x]$. By clearing denominators of $a, b$, this is true if and only if $a'f + b'g = d$ for some $a', b' \in \mathbb{Z}[x]$, $d \in \mathbb{Z}$, which is equivalent to saying $(f, g) \cap \mathbb{Z} \neq \emptyset$. □

**Exercise 12.3.4.** *Let $x, y, z, w$ be variables. Prove that $xy - zw$, the determinant of a variable $2 \times 2$ matrix, is an irreducible element of the polynomial ring $\mathbb{C}[x, y, z, w]$.*

*Proof.* Suppose $xy - zw$ factors as $pq$ for $p, q \notin \mathbb{C}$, where $p = a_0 + a_1 + a_2$ and $q = b_0 + b_1 + b_2$ for $a_i, b_i$ homogeneous of degree $i$ or zero. We claim $p, q$ are homogeneous of degree one; we proceed by comparing degrees. $a_0 b_0 = 0$ hence without loss of

generality $a_0 = 0$. $a_1 b_0 = 0$ as well; if $a_1 = 0$, then $b_1 = b_2 = 0$, contradicting that $q \notin \mathbb{C}$, hence $a_1 \neq 0, b_0 = 0$. This implies $b_2 = 0$, hence $p, q$ are homogeneous of degree one.

Thus, since $xy - zw = x^2(y/x - z/x \cdot w/x) = x^2(p/x)(q/x)$, $xy - zw$ is reducible only if $y/x - z/x \cdot w/x$ is reducible in $\mathbb{C}[y/x, z/x, w/x]$. Relabeling variables and taking the contrapositive, it suffices to show $t - rs$ is irreducible in $\mathbb{C}[r, s, t]$. But $\mathbb{C}[r, s, t]/(t - rs) \approx \mathbb{C}[r, s]$, a domain, hence $t - rs$ is prime (Prop. 13.5.1($a$)) and thus irreducible since $\mathbb{C}[r, s, t]$ is a domain (Lem. 12.2.10). □

**Exercise 12.3.6.** *Let $\alpha$ be a complex number. Prove that the kernel of the substitution map $\mathbb{Z}[x] \to \mathbb{C}$ that sends $x \rightsquigarrow \alpha$ is a principal ideal, and describe its generator.*

*Proof.* Let $\varphi$ be this map. By the mapping property of fractions (Thm. 11.7.2($c$), which is still true if $\varphi$ is not injective), we have the commutative diagram

$$\begin{array}{ccc} \mathbb{Z}[x] & \xrightarrow{\varphi} & \mathbb{C} \\ \downarrow & \nearrow_{\psi} & \\ \mathbb{Q}[x] & & \end{array}$$

Since $\mathbb{Q}[x]$ is a Euclidean domain, $\ker \psi$ is principal. We claim it is generated by the polynomial $f$ of minimal degree which has $\alpha$ as a root, or zero if $\alpha$ is transcendental. For, in the former case, if $g \in \ker \varphi$, we can write $g = fq + r$ by the Euclidean algorithm, and $r \neq 0$ implies $\deg r < \deg f$, contradicting the minimality of $f$.

We claim if $f = cf_0$ as in Lem. 12.3.5 for $f_0$ primitive, then $\ker \varphi = (f_0)$. $(f_0) \subset \ker \varphi$ by the commutativity of the diagram, so it suffices to show the opposite inclusion. Let $g \in \ker \varphi$. Then, $f \mid g$ in $\mathbb{Q}[x]$ by the above, hence $f_0 \mid g$ in $\mathbb{Z}[x]$ by Thm. 12.3.6($a$). Thus $\ker \varphi$ is generated by $f_0$, the primitive polynomial obtained from $f$ as above, or is zero if $\alpha$ is transcendental. □

## 12.4 Factoring Integer Polynomials

**Exercise 12.4.4.** *Factor the integer polynomial $x^5 + 2x^4 + 3x^3 + 3x + 5$ mod 2, mod 3, and over $\mathbb{Q}$.*

*Remark.* We denote $f(x) = x^5 + 2x^4 + 3x^3 + 3x + 5$.

*Solution for $\mathbb{F}_2$.* $f(x) = x^5 + x^3 + x + 1$ over $\mathbb{F}_2$. Then, $f(1) = 0$, hence $f(x) = (x + 1)(x^4 + x^3 + 1)$. Now $x^4 + x^3 + 1$ has no roots in $\mathbb{F}_2$ hence has no linear factors; $x^2 + x + 1$ is the only irreducible quadratic in $\mathbb{F}_2[x]$ and has $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x^3 + 1$, hence we cannot factor further. □

*Solution for* $\mathbb{F}_3$. $f(x) = x^5 + 2x^4 + 2$ over $\mathbb{F}_3$. Then, $f(2) = 0$, hence $f(x) = (x+1)(x^4 + x^3 + 2x^2 + x + 2)$. But 2 is also a root of $x^4 + x^3 + 2x^2 + x + 2$, hence $f(x) = (x+1)^2(x^3 + 2x + 2)$, and we cannot factor further since $x^3 + 2x + 2$ has no roots in $\mathbb{F}_3$. □

*Solution for* $\mathbb{Q}$. From $(a), (b)$, we suspect that $-1$ is a root. Indeed, $f(x) = (x+1)(x^4 + x^3 + 2x^2 - 2x + 5)$. The residue $x^4 + x^3 + 1$ of the second factor in $\mathbb{F}_2[x]$ is irreducible as in $(a)$, and so $x^4+x^3+2x^2-2x+5$ is irreducible in $\mathbb{Q}[x]$ by Prop. 12.4.3. Thus we cannot factor further. □

**Exercise 12.4.6.** *Factor* $x^5 + 5x + 5$ *into irreducible factors in* $\mathbb{Q}[x]$ *and in* $\mathbb{F}_2[x]$.

*Solution for* $\mathbb{Q}[x]$. $x^5 + 5x + 5$ is irreducible in $\mathbb{Q}[x]$ by the Eisenstein criterion (Prop. 12.4.6) since 5 doesn't divide the leading coefficient 1 while it divides all other coefficients, and $5^2 = 25$ does not divide the constant term 5. □

*Solution for* $\mathbb{F}_2[x]$. The residue in $\mathbb{F}_2[x]$ is $x^5+x+1$, which is reducible in $\mathbb{F}_2[x]$ since $x^5+x+1 = (x^3+x^2+1)(x^2+x+1)$; each of these factors have no roots in $\mathbb{F}_2$ hence we cannot factor further. □

**Exercise 12.4.7.** *Factor* $x^3 + x + 1$ *in* $\mathbb{F}_p[x]$, *when* $p = 2$, 3, *and* 5.

*Remark.* We denote $f(x) = x^3 + x + 1$.

*Solution for* $p = 2$. Since $f(0) = 1, f(1) = 1$, we see that there are no roots in $\mathbb{F}_2$, and so $x^3 + x + 1$ is irreducible. □

*Solution for* $p = 3$. Since $f(1) = 0$, we can factor out $(x + 2)$ to get $f(x) = (x+2)(x^2 + x + 2)$. We cannot factor further since $x^2 + x + 2$ has no roots in $\mathbb{F}_3$. □

*Solution for* $p = 5$. Since $f(0) = 1, f(1) = 3, f(2) = 1, f(3) = 1, f(4) = 4$, we see that there are no factors of $f(x)$ in $\mathbb{F}_5$ and so it is irreducible. □

**Exercise 12.4.12.** *Determine:*

(a) *the monic irreducible polynomials of degree* 3 *over* $\mathbb{F}_3$,
(b) *the monic irreducible polynomials of degree* 2 *over* $\mathbb{F}_5$,
(c) *the number of irreducible polynomials of degree* 3 *over the field* $\mathbb{F}_5$.

*Remark.* It suffices to make sure our polynomials have no roots, for any factorization of a quadratic or a cubic will produce a linear factor.

*Solution for* $(a)$. We consider all polynomials of the form $x^3 + ax^2 + bx + c$ in $\mathbb{F}_3$. $c = 1, 2$ since otherwise $x = 0$ would be a root. Moreover, $1 + a + b + c \not\equiv 0 \bmod 3$ and $2 + a + 2b + c \not\equiv 0 \bmod 3$ must be true for irreducibility. Suppose $c = 1$. Then, $1 + a + b + 1 \not\equiv 0$ implies $a + b \not\equiv 1$. Likewise, $2 + a + 2b + 1 \equiv a + 2b \not\equiv 0$, and so the only ordered triples that work for $c = 1$ are $(0, 2, 1), (1, 2, 1), (2, 0, 1), (2, 1, 1)$, i.e.,

$$x^3 + 2x + 1, \quad x^3 + x^2 + 2x + 1, \quad x^3 + 2x^2 + 1, \quad x^3 + 2x^2 + x + 1$$

are monic irreducible polynomials of degree 3 over $\mathbb{F}_3$.

Suppose $c = 2$. Then, $1 + a + b + 2 \equiv a + b \not\equiv 0$, and likewise, $2 + a + 2b + 2 \not\equiv 0$ implies $a + 2b \not\equiv 2$. Thus, the only ordered triples that work for $c = 2$ are $(0, 2, 2), (1, 0, 2), (1, 1, 2), (2, 2, 2)$, i.e.,

$$x^3 + 2x + 2, \quad x^3 + x^2 + 2, \quad x^3 + x^2 + x + 2, \quad x^3 + 2x^2 + 2x + 2$$

are monic irreducible polynomials of degree 3 over $\mathbb{F}_3$. □

*Solution for* $(b)$. We consider polynomials of the form $x^2 + ax + b$ in $\mathbb{F}_5$. $b = 1, 2, 3, 4$ since otherwise $x = 0$ would be a root. Moreover, we have the system of equations

$$\begin{cases} 1 + a + b \not\equiv 0 \\ 4 + 2a + b \not\equiv 0 \\ 4 + 3a + b \not\equiv 0 \\ 1 + 4a + b \not\equiv 0 \end{cases} \implies \begin{cases} a, 4a \not\equiv 4 - b, \\ 2a, 3a \not\equiv 1 - b. \end{cases}$$

We can consider this system for each $b$ value. For $b = 1$, we have

$$\begin{cases} a, 4a \not\equiv 3 \\ 2a, 3a \not\equiv 0 \end{cases} \implies a = 1, 4.$$

For $b = 2$, we have

$$\begin{cases} a, 4a \not\equiv 2 \\ 2a, 3a \not\equiv 4 \end{cases} \implies a = 0, 1, 4.$$

For $b = 3$, we have

$$\begin{cases} a, 4a \not\equiv 1 \\ 2a, 3a \not\equiv 3 \end{cases} \implies a = 0, 2, 3.$$

For $b = 4$, we have

$$\begin{cases} a, 4a \not\equiv 0 \\ 2a, 3a \not\equiv 2 \end{cases} \implies a = 2, 3.$$

Thus, our monic irreducible polynomials of degree 2 over $\mathbb{F}_5$ are

$$\begin{gathered} x^2 + x + 1, \quad x^2 + 4x + 1, \quad x^2 + 2, \quad x^2 + x + 2, \quad x^2 + 4x + 2, \\ x^2 + 3, \quad x^2 + 2x + 3, \quad x^2 + 3x + 3, \quad x^2 + 2x + 4, \quad x^2 + 3x + 4. \end{gathered}$$

□

*Solution for* $(c)$. There are 5 monic polynomials of degree 1, and from $(b)$ there are 10 monic irreducible polynomials of degree 2. The irreducible monic polynomials of degree 3 are those that cannot be obtained by multiplying together polynomials of lower degree. We see that any choice of factors gives a unique polynomial of degree 3 by Prop. 12.2.14$(c)$, and so it suffices to count all monic polynomials of degree 3 in $\mathbb{F}_5[x]$, and subtract those that can be obtained by multiplying together polynomials of lower degree.

We see that reducible polynomials of degree 3 must be a product of 3 polynomials of degree 1 or a product of 2 polynomials of degree 1 and 2 respectively. The number of polynomials in the former category is

$$\binom{5}{3} + \binom{5}{1}\binom{4}{1} + \binom{5}{1} = 35,$$

where the terms describe all different, 2 same, and all same factors. The number of polynomials in the latter category is $5 \times 10 = 50$. Since the number of degree 3 monic polynomials is $5^3 = 125$, we see that there are $125 - (35 + 50) = 40$ degree 3 monic irreducible polynomials in $\mathbb{F}_5$.

Since we want to find the number of (not necessarily monic) irreducible polynomials of degree 3 in $\mathbb{F}_5[x]$, we see that we can multiply our 40 monic polynomials by any element of $\mathbb{F}_5 \setminus \{0\}$; this results in 160 irreducible polynomials of degree 3. □

**Exercise 12.4.13** (Lagrange interpolation formula)**.**

- $(a)$ *Let $a_0, \ldots, a_n$ be distinct complex numbers. Determine a polynomial $p(x)$ of degree $n$, which has $a_1, \ldots, a_n$ as roots, and such that $p(a_0) = 1$.*
- $(b)$ *Let $a_0, \ldots, a_d$ and $b_0, \ldots, b_d$ be complex numbers, and suppose that the $a_i$ are distinct. There is a unique polynomial $g$ of degree $\leq d$ such that $g(a_i) = b_i$ for each $i = 0, \ldots, d$. Determine the polynomial $g$ explicitly in terms of $a_i$ and $b_i$.*

*Solution for* $(a)$. We let

$$p_i(x) = \prod_{j \neq i} \frac{x - a_j}{a_i - a_j}.$$

Any $a_j$ with $j \neq i$ is a root since $p_i(x) = 0 \iff x - a_j = 0$ for some $j$, and $p(a_i) = 1$ since each term in the product would equal 1. Letting $p(x) = p_0(x)$, we are done. $\square$

*Solution for* $(b)$. We let

$$g(x) = \sum_{i=0}^{d} b_i p_i(x) = \sum_{i=0}^{d} b_i \prod_{j \neq i} \frac{x - a_j}{a_i - a_j},$$

where $p_i(x)$ is as in $(a)$. $g(a_i) = b_i$ for all $i$ since $p_i(a_j) = \delta_{ij}$. $\deg g \leq d$ by the fact that each term in the sum has degree $d$.

We now prove uniqueness. Suppose $h(x)$ is another such polynomial. Then, $f(x) = g(x) - h(x)$ has degree $\leq d$ and therefore has $\leq d$ roots; however, $h(a_i) = g(a_i) - h(a_i) = b_i - b_i = 0$ for all $0 \leq i \leq d$. But then, $f(x)$ has $d+1$ distinct roots, which contradicts Prop. 12.2.20 unless $g(x) = h(x)$. $\square$

**Exercise 12.4.15.** *With reference to the Eisenstein criterion, what can one say when*
$(a)$ $\bar{f}$ *is constant,* $(b)$ $\bar{f} = x^n + \bar{b}x^{n-1}$*?*

**Claim** $(a)$**.** *Let* $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ *and let* $p \in \mathbb{Z}$ *be prime. Then* $f$ *is irreducible in* $\mathbb{Q}[x]$ *if* $(i)$ $p \nmid a_0$*;* $(ii)$ $p \mid a_i$ *for* $1 \leq i \leq n$*;* $(iii)$ $p^2 \nmid a_n$*. Note that* $(i)$ *and* $(ii)$ *hold if and only if* $\bar{f}$ *is a nonzero constant.*

*Proof of Claim* $(a)$. Suppose not; then $f = gh$ for $g = b_r x^r + \cdots + b_0, h = c_s x^s + \cdots + c_0, r + s = n$. Since then $\bar{f} = \bar{g}\bar{h} = \overline{a_0} \neq 0$ by $(i)$ and $(ii)$, we see that $\bar{g} = \overline{b_0}$ and $\bar{h} = \overline{c_0}$ since they must divide $\overline{a_0}$. But then $p \mid b_r$ and $p \mid c_s$ imply $p^2 \mid b_r c_s = a_n$. $\square$

**Claim** $(b)$**.** *Let* $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ *and let* $p \in \mathbb{Z}$ *be prime. Then* $f$ *is irreducible in* $\mathbb{Q}[x]$ *if* $(i)$ $a_n \equiv 1 \bmod p$*;* $(ii)$ $p \nmid a_{n-1}$*;* $(iii)$ $p \mid a_i$ *for* $0 \leq i \leq n-2$*;* $(iv)$ $p \nmid a_0$*. Note that* $(i)$*,* $(ii)$*, and* $(iii)$ *hold if and only if* $\bar{f} = x^n + \bar{b}x^{n-1}$*.*

*Proof of Claim* $(b)$. Suppose not; then $f = gh$ for $g = b_r x^r + \cdots + b_0, h = c_s x^s + \cdots + c_0, r + s = n$. Since then $\bar{f} = \bar{g}\bar{h} = x^n + \overline{a_{n-1}}x^{n-1} = x^{n-1}(x + \overline{a_{n-1}})$ by $(i)$, $(ii)$, and $(iii)$, without loss of generality $x + \overline{a_{n-1}} \mid \bar{g}$, and so $\bar{g} = \overline{b_r}x^{r-1}(x + \overline{a_{n-1}})$ and $\bar{h} = \overline{c_s}x^s$. But then, $p \mid c_0$ implies $p \mid b_0 c_0 = a_0$. $\square$

**Exercise 12.4.19.** *Factor* $x^5 - x^4 - x^2 - 1 \bmod 2$*,* $\bmod 16$*, and over* $\mathbb{Q}$*.*

*Remark.* We denote $f(x) = x^5 - x^4 - x^2 - 1$.

*Solution for* $\mathbb{F}_2$. $f(x) = x^5 + x^4 + x^2 + 1$ over $\mathbb{F}_2$. Then, $f(1) = 0$, and so $f(x) = (x+1)(x^4 + x + 1)$. $x^4 + x + 1$ has no roots in $\mathbb{F}_2$, and the only irreducible quadratic in $\mathbb{F}_2[x]$ is $x^2 + x + 1$ which has $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x + 1$, hence we cannot factor further. □

*Solution for* $\mathbb{Z}/16\mathbb{Z}$. $f(-5) \equiv 0 \bmod 16$, and so $f(x) = (x+5)(x^4-6x^3-2x^2+9x+3)$. This does not factor further, for a factorization of $x^4 - 6x^3 - 2x^2 + 9x + 3$ over $\mathbb{Z}/16\mathbb{Z}$ would produce a factorization of $x^4 + x + 1$ over $\mathbb{F}_2$, contradicting $(a)$. □

*Solution for* $\mathbb{Q}$. The only possible factorization is as in $(b)$. But the constant term of the linear factor in $(b)$ has constant term $5 \not\equiv \pm 1 \bmod 16$, which would be necessary for $f$ to have constant term $-1$, and so $f$ is irreducible. □

## 12.5 Gauss Primes

**Exercise 12.5.2.** *Find the greatest common divisor in* $\mathbb{Z}[i]$ *of* $(a)$ $11+7i$, $4+7i$, $(b)$ $11 + 7i$, $8 + i$, $(c)$ $3 + 4i$, $18 - i$.

*Proof of* $(a)$. First, $(11+7i)(11-7i) = 11^2+7^2 = 170 = 2\times5\times17 = (1+i)(1-i)(2+i)(2-i)(4+i)(4-i)$, and so $11 + 7i = (1 + i)(2 - i)(4 + i)$ is a prime factorization. Likewise, $(4+7i)(4-7i) = 4^2+7^2 = 65 = 5\times13 = (2+i)(2-i)(3+2i)(3-2i)$, and so $4+7i = (2+i)(3+2i)$ is a prime factorization. Thus, $\gcd(11+7i, 4+7i) = 1$. □

*Proof of* $(b)$. $11 + 7i = (1 + i)(2 - i)(4 + i)$ is a prime factorization by $(a)$. Then, $(8 + i)(8 - i) = 8^2 + 1^2 = 65 = 5 \times 13 = (2 + i)(2 - i)(3 + 2i)(3 - 2i)$, and so $8 + i = (2 - i)(3 + 2i)$. Thus, $\gcd(11 + 7i, 8 + i) = 2 - i$. □

*Proof of* $(c)$. Since $(18 - i)/(3 + 4i) = 2 - 3i$, $\gcd(3 + 4i, 18 - i) = 3 + 4i$. □

**Exercise 12.5.3.** *Find a generator for the ideal of* $\mathbb{Z}[i]$ *generated by* $3+4i$ *and* $4+7i$.

*Proof.* $\mathbb{Z}[i]$ is a PID (Props. 12.2.5$(c)$, 12.2.7), so it suffices to find $\gcd(3 + 4i, 4 + 7i)$. Since $(3 + 4i)(3 - 4i) = 25 = (2 + i)^2(2 - i)^2$, $(3 + 4i) = (2 + i)(2 + i)$ is a prime factorization, and from Exercise 12.5.2$(a)$, $4 + 7i = (2 + i)(3 + 2i)$ is a prime factorization. Thus, $2 + i$ is a generator of the ideal. □

**Exercise 12.5.5.** *Let* $\pi$ *be a Gauss prime. Prove that* $\pi$ *and* $\overline{\pi}$ *are associates if and only if* $\pi$ *is an associate of an integer prime, or* $\overline{\pi}\pi = 2$.

*Proof.* Suppose $\pi$ and $\overline{\pi}$ are associates. Then, $e(a+bi) = a - bi$ for some unit $e \in \{\pm 1, \pm i\}$. Thus, $\overline{\pi}\pi = e(a+bi)^2 = e(a^2 - b^2 + 2bi)$. First suppose $e = \pm 1$. Then, $b = 0$ since $\overline{\pi}\pi \in \mathbb{Z}$, and so $\overline{\pi}\pi = ea^2 = a^2$, since $\overline{\pi}\pi > 0$. By Theorem 12.5.2($a$), $\pi$ prime implies $a$ is an integer prime, and so $\pi$ must be an associate of $a$, an integer prime. Now suppose $e = \pm i$. Then, $\overline{\pi}\pi = \pm i(a^2 - b^2 + 2bi) = \mp 2b \pm i(a^2 - b^2)$. Then, $a^2 - b^2 = 0$ since $\overline{\pi}\pi \in \mathbb{Z}$, and so $\overline{\pi}\pi = \mp 2b$. By Theorem 12.5.2($a$), we see $b \in \{\pm 1, \pm 2\}$. But since $a^2 - b^2 = 0$ and $b = \pm 2$ imply $a = \pm 2$, we have that $2 \mid \pi$, which contradicts its primeness. Thus, $b = \pm 1$, and so $\overline{\pi}\pi = \mp 2b = 2$.

Now if $\pi$ is an associate of an integer prime, then $\pi = ep$ for some $e \in \{\pm 1, \pm i\}$, and so $\overline{\pi} = \overline{e}p$; since then $\pi/\overline{\pi} \in \{\pm 1, \pm i\}$, $\pi$ and $\overline{\pi}$ are associates. Now suppose $\overline{\pi}\pi = 2$. Then, $(a-bi)(a+bi) = a^2 + b^2 = 2 = (1+i)(1-i)$. By the fact that $\mathbb{Z}[i]$ is a UFD, this prime factorization is unique (up to a unit), and so since $1+i = i(1-i)$, we see that $\pi$ and $\overline{\pi}$ are associates. □

**Exercise 12.5.6.** *Let $R$ be the ring $\mathbb{Z}[\sqrt{-3}]$. Prove that an integer prime $p$ is a prime element of $R$ if and only if the polynomial $x^2 + 3$ is irreducible in $\mathbb{F}_p[x]$.*

*Proof.* We consider the ring $\overline{R} = \mathbb{Z}[\sqrt{-3}]/(p)$. Since $R \approx \mathbb{Z}[x]/(x^2+3)$, we can take the quotient with respect to $(p)$ and $(x^2+3)$ in different orders:

$$\begin{array}{ccc} & \overset{\text{kill}}{\underset{p}{\longrightarrow}} & \\ \mathbb{Z}[x] & & \mathbb{F}_p[x] \\ {\scriptstyle \text{kill}\atop x^2+3}\downarrow & & \downarrow{\scriptstyle \text{kill}\atop x^2+3} \\ R & \underset{\text{kill}\atop p}{\longrightarrow} & \overline{R} \end{array}$$

Now $\overline{R}$ is a domain if and only if $p$ is prime in $R$ by Prop. 13.5.1. But $\overline{R}$ is a domain if and only if $x^2+3$ is prime in $\mathbb{F}_p[x]$ as well, and since $\mathbb{F}_p[x]$ is a domain, this is true if and only if $x^2+3$ is irreducible in $\mathbb{F}_p[x]$ by Lem. 12.2.10. □

**Exercise 12.5.7.** *Describe the residue ring $\mathbb{Z}[i]/(p)$ for each prime $p$.*

*Solution.* Recall that $\mathbb{Z}[i] \approx \mathbb{Z}[x]/(x^2+1)$, and so $\mathbb{Z}[i]/(p) \approx (\mathbb{Z}[x]/(p))/(x^2+1) \approx \mathbb{F}_p[x]/(x^2+1)$.

When $p \equiv 3 \bmod 4$, $p$ is a Gauss prime and so $\mathbb{F}_p[x]/(x^2+1) \approx \mathbb{F}_p[i]$ is a field by Lem. 12.5.3, and so is isomorphic to $\mathbb{F}_{p^2}$ by Thm. 15.7.3($d$).

When $p \equiv 1 \bmod 4$ or $p = 2$, $p$ is not a Gauss prime and so $x^2+1$ is reducible in $\mathbb{F}_p[x]$ with roots $\alpha, \alpha^{-1}$ by Lem 12.5.3. Then, $(x-\alpha) + (x-\alpha^{-1}) = \mathbb{F}_p[x]$ as ideals,

and $(x-\alpha)(x-\alpha^{-1}) = (x^2+1) = 0$ as ideals in $\mathbb{F}_p[x]/(x^2+1)$, hence by Exercise 11.6.8$(c)$ we have $\mathbb{F}_p[x]/(x^2+1) \approx \mathbb{F}_p[x]/(x-\alpha) \times \mathbb{F}_p[x]/(x-\alpha^{-1}) \approx \mathbb{F}_p \times \mathbb{F}_p$. □

**Exercise 12.5.9.** *Let $R = \mathbb{Z}[\omega]$ with $\omega = e^{2\pi i/3}$. Let $p$ be a prime integer $\neq 3$. Adapt the proof of Theorem* 12.5.2 *to prove the following:*

- $(a)$ *The polynomial $x^2+x+1$ has a root in $\mathbb{F}_p$ if and only if $p = 1$ modulo* 3.
- $(b)$ *$(p)$ is a maximal ideal of $R$ if and only if $p = -1$ modulo* 3.
- $(c)$ *$p$ factors in $R$ if and only if it can be written in the form $p = a^2+ab+b^2$, for some integers $a, b$.*

*Proof of* $(a)$. $x^2+x+1$ has a root in $\mathbb{F}_p$ if and only if $x^3-1$ has a nontrivial root in $\mathbb{F}_p$, i.e., $\mathbb{F}_p^\times$ has an element of order 3. This is true if and only if $3 \mid |\mathbb{F}_p^\times| = p-1$ by corollaries to Lagrange's theorem (Cor. 2.8.10) and the first Sylow theorem (Cor. 7.7.3). This is equivalent to having $p \equiv 1 \bmod 3$. □

*Proof of* $(b)$. We consider the ring $\overline{R} = \mathbb{Z}[\omega]/(p)$. Since $R \approx \mathbb{Z}[x]/(x^2+x+1)$, we can take the quotient with respect to $(p)$ and $(x^2+x+1)$ in different orders:

$$\begin{array}{ccc} & \overset{\text{kill } p}{\longrightarrow} & \\ \mathbb{Z}[x] & & \mathbb{F}_p[x] \\ {\scriptstyle \text{kill } x^2+x+1}\downarrow & & \downarrow{\scriptstyle \text{kill } x^2+x+1} \\ R & \underset{\text{kill } p}{\longrightarrow} & \overline{R} \end{array}$$

Now $\overline{R}$ is a field if and only if $(p)$ is maximal in $R$ by Prop. 11.8.2$(b)$. But $\overline{R}$ is a field if and only if $(x^2+x+1)$ is maximal in $\mathbb{F}_p[x]$ as well, and since $\mathbb{F}_p[x]$ is a PID (Props. 12.2.5$(b)$, 12.2.7), this is true if and only if $x^2+x+1$ is irreducible in $\mathbb{F}_p[x]$ by Cor. 12.2.9$(C)$. But this holds if and only if $p \equiv -1 \bmod 3$ by $(a)$ since all prime integers $\neq 3$ are equivalent to $\pm 1 \bmod 3$. □

*Proof of* $(c)$. If $p = a^2+ab+b^2$, then $p$ factors as $(a-b\omega)(a-b\omega^2)$ in $R$.

Conversely, suppose $p$ factors in $R$. $p$ is not a unit in $R$ hence is divisible by a prime $\pi \in R$. Then, $\overline{\pi} \mid \overline{p} = p$, so $\overline{\pi}\pi \mid p^2$ in $R$ and $\mathbb{Z}$, and so $\overline{\pi}\pi = p$ or $p^2$. The latter case is impossible for otherwise $p$ would be an associate of $\pi$, hence irreducible. Thus, $p = (a-b\omega)(a-b\overline{\omega})(a-b\omega)(a-b\omega^2) = a^2+ab+b^2$ for some $a, b \in \mathbb{Z}$. □

**Exercise 12.5.10.**

- $(a)$ *Let $\alpha$ be a Gauss integer. Assume that $\alpha$ has no integer factor, and that $\overline{\alpha}\alpha$ is a square integer. Prove that $\alpha$ is a square in $\mathbb{Z}[i]$.*

(*b*) *Let $a, b, c$ be integers such that $a$ and $b$ are relatively prime and $a^2 + b^2 = c^2$. Prove that there are integers $m$ and $n$ such that $a = m^2 - n^2$, $b = 2mn$, and $c = m^2 + n^2$.*

*Proof of* (*a*). We can decompose $\alpha = u\pi_1^{k_1} \cdots \pi_n^{k_n}$ for $\pi_j$ prime and $u$ a unit, such that $\pi_i, \pi_j$ are not associates for any $i \neq j$; we want to show $2 \mid k_j$ for each $j$. Then,

$$\overline{\alpha}\alpha = u^2(\overline{\pi_1}\pi_1)^{k_1} \cdots (\overline{\pi_n}\pi_n)^{k_n} = c^2 \text{ for some } c \in \mathbb{Z}.$$

By Theorem 12.5.2(*a*), each $\overline{\pi_j}\pi_j$ is an integer prime or a square of an integer prime. For each $j$, $\overline{\pi_j}\pi_j$ integer prime implies $2 \mid k_j$, since otherwise $c^2$ would not be a square integer. Now suppose $\overline{\pi_j}\pi_j$ is a square of an integer prime for some $j$. Then, $p^2 = \overline{\pi_j}\pi_j$ implies $\pi_j$ is an associate of $p$, since this prime decomposition is unique up to units; this implies $p \mid \alpha$, which contradicts that $\alpha$ has no integer factor. Finally, $c^2 > 0$ hence $u^2 = 1$, and so $u = \pm 1$. In either case, $\alpha$ is a square since $i^2 = -1$. □

*Proof of* (*b*). Not both of $a, b$ are odd: otherwise, $c^2 = a^2 + b^2 \equiv 1 + 1 = 2 \bmod 4$, a contradiction since all even square integers must be $0 \bmod 4$. So assume without loss of generality that $a$ is odd. Let $\alpha = a + bi$. Then, $\overline{\alpha}\alpha = a^2 + b^2 = c^2$, hence by (*a*) letting $\alpha = (m + ni)^2$ we have $a = m^2 - n^2$, $b = 2mn$, and $c = m^2 + n^2$. □

## 12.M Miscellaneous Problems

**Exercise 12.M.5.** *For which integers $n$ does the circle $x^2 + y^2 = n$ contain a point with integer coordinates?*

*Solution.* We claim that $x^2 + y^2 = n$ has integer solutions if and only if every prime $\equiv 3 \bmod 4$ has even exponent in the prime factorization of $n$.

$\Leftarrow$ The prime factorization can be written $n = ab^2$, where $a$ is square free. Then, by Thm. 12.5.2(*d*), every $p$ that divides $a$ can be written $p = \overline{\pi_p}\pi_p$. Letting $x + iy = b \cdot \prod_{p|a} \pi_p$, we have $x^2 + y^2 = (x - iy)(x + iy) = ab^2 = n$.

$\Rightarrow$ Let $n = x^2 + y^2 = (x - iy)(x + iy)$. If $p \equiv 3 \bmod 4$ divides $a$, it is a Gauss prime by Thm. 12.5.2(*b*), and so $p \mid x - iy$ or $x + iy$. But then, $p \mid x, y$, hence $p \mid x \pm iy$. Thus, if $p^k$ is the power of $p$ that appears in the prime factorization for $x - iy$, then $p^{2k}$ is the power of $p$ that appears in the prime factorization for $(x - iy)(x + iy) = n$. □

**Exercise 12.M.6.** *Let $R$ be a domain and let $I$ be an ideal that is the product of distinct maximal ideals in two ways, say $I = P_1 \cdots P_r = Q_1 \cdots Q_s$. Prove that the two factorizations are the same, except for the ordering of the terms.*

*Proof.* Suppose there is an $i$ such that $Q_j \not\subset P_i$ for all $j$. Let $\varphi_i \colon R \to R/P_i$ be the canonical quotient map. Then, for each $j$ there is $q_j \in Q_j \setminus P_i$, and so

$$\prod_j \varphi_i(q_j) = \varphi_i\left(\prod_j q_j\right) \neq 0 \in R/P_i,$$

which is a contradiction since $\prod_j q_j \in Q_1 \cdots Q_s \subset P_i$. Thus, for every $i$, there is a $j$ such that $Q_j \subset P_i$; since both ideals are maximal, we moreover have $Q_j = P_i$. Thus, $\{P_1, \ldots, P_r\} \subset \{Q_1, \ldots, Q_s\}$ as sets; interchanging the role of the $P_i$ and $Q_j$ gives the opposite inclusion, so the two factorizations are equal. □

**Exercise 12.M.7.** *Let $R = \mathbb{Z}[x]$.*

(*a*) *Prove that every maximal ideal in $R$ has the form $(p, f)$, where $p$ is an integer prime and $f$ is a primitive integer polynomial that is irreducible modulo $p$.*

(*b*) *Let $I$ be an ideal of $R$ generated by two polynomials $f$ and $g$ that have no common factors other than $\pm 1$. Prove that $R/I$ is finite.*

*Proof of* (*a*). Let $M \subset R$ be a maximal ideal. It is not principal by Exercise 11.8.1, and so there exist $f_1, f_2 \in M$ that do not share a common factor. $f_1, f_2$ do not share a common factor in $\mathbb{Q}[x]$, either by Thm. 12.3.6(*b*). Thus, $r_0 f_1 + s_0 f_2 = 1$ for some $r, s \in \mathbb{Q}[x]$, and so clearing denominators, $rf_1 + sf_2 = q \in \mathbb{Q}$ for $r, s \in \mathbb{Z}[x]$, i.e., $M \cap \mathbb{Z} \neq (0)$.

Now $M \cap \mathbb{Z}$ is prime, since if $ab \in M \cap \mathbb{Z}$, then, say, $a \in M$ and moreover $a \in \mathbb{Z}$ for otherwise $ab \notin \mathbb{Z}$. Thus, $M \cap \mathbb{Z} = (0)$ or $(p)$ for some prime $p$; the former case is impossible by the above. Now consider the image $M'$ of $M$ in $\mathbb{F}_p[x]$; then, $\mathbb{Z}[x]/M \approx \mathbb{F}_p[x]/M'$ is a field, and so $M'$ is maximal by Prop. 11.8.2(*b*), and is generated by some irreducible $f_0 \in \mathbb{F}_p[x]$ by Cor. 12.2.9(*c*) since $\mathbb{F}_p[x]$ is a PID by Props. 12.2.5(*b*), 12.2.7. Now if $f \in \mathbb{Z}[x]$ is a lift of $f_0$, then $(p, f) \subset M$ since $f = 0$ in $\mathbb{F}_p[x]/M'$; $M \subset (p, f)$ since if $g \in M \setminus (p, f)$, then $g \neq 0 \in \mathbb{F}_p[x]/M' \approx \mathbb{Z}[x]/M$. □

*Proof of* (*b*). As in (*a*), if $I = (f, g)$ and $f, g$ have no common factors, then $I \cap \mathbb{Z} \neq (0)$; since $\mathbb{Z}$ is a PID, $M \cap \mathbb{Z} = (n)$ for some $n \in \mathbb{Z}$ such that $n \neq \pm 1$, for otherwise $R/I = 0$ and we are done. So, letting $n = \prod p_i^{k_i}$ be a prime factorization, we claim

$$\frac{R}{I} \approx \frac{(\mathbb{Z}/n\mathbb{Z})[x]}{(f, g)} \approx \frac{\prod_i (\mathbb{Z}/p_i^{k_i}\mathbb{Z})[x]}{(f, g)} \approx \prod_i \frac{(\mathbb{Z}/p_i^{k_i}\mathbb{Z})[x]}{(f, g)}. \tag{3}$$

The first isomorphism is clear, and the second follows by applying Exercise 11.6.8(*c*) repeatedly. For the third, consider the canonical surjection

$$\pi \colon \prod_i (\mathbb{Z}/p_i^{k_i}\mathbb{Z})[x] \to \prod_i \frac{(\mathbb{Z}/p_i^{k_i}\mathbb{Z})[x]}{(f, g)}.$$

$\ker \pi = (f, g)$ since an element on the left maps to zero on the right if and only if each direct factor is in $(f, g)$, and so (3) holds by the first isomorphism theorem (Thm. 11.4.2($b$)). Let each direct factor on the right be called $R_i$.

It suffices to show each $R_i$ is finite. Since $f, g$ do not share a common factor, without loss of generality $p_i \nmid f$. Then, separating out the terms in $f$, we can write $f = f_1 - f_2$ where $p_i \nmid f_1$ while $p_i \mid f_2$. Then, $p_i^{k_i} \mid f_2^{k_i}$, hence in $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})[x]$,

$$f_1^{k_i} = f_1^{k_i} - f_2^{k_i} = (f_1 - f_2)h = fh \in (f, g)$$

for some $h \in (\mathbb{Z}/p_i^{k_i}\mathbb{Z})[x]$. If $a$ is the leading coefficient of $f_1$, then $f_1^{k_i}$ has leading coefficient $a^{k_i}$. This is a unit since if not, then $(a^{k_i})$ is contained in a maximal ideal of $\mathbb{Z}/p_i^{k_i}\mathbb{Z}$ by Thm. 11.9.2, but $(p_i)$ is the unique maximal ideal of this ring by the correspondence theorem (Thm. 11.4.3), contradicting that $p_i \nmid a$. Thus, $m = a^{-k_i} f_1^{k_i}$ is a monic polynomial in $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})[x]$, hence each $R_i$ is finite since any polynomial with degree $\geq \deg m$ can be reduced to a polynomial of lower degree using that $m = 0$, and there are only finitely many polynomials in $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})[x]$ with degree $< \deg m$ since $\mathbb{Z}/p_i^{k_i}\mathbb{Z}$ is finite. □

**Exercise 12.M.8.** *Let $u$ and $v$ be relatively prime integers, and let $R'$ be the ring obtained from $\mathbb{Z}$ by adjoining an element $\alpha$ with the relation $v\alpha = u$. Prove that $R'$ is isomorphic to $\mathbb{Z}\left[\frac{u}{v}\right]$ and also to $\mathbb{Z}\left[\frac{1}{v}\right]$.*

*Proof.* We see that $R' = \mathbb{Z}[x]/(vx - u) \approx \mathbb{Z}[\alpha]$. Now since $v\alpha = u$ by construction, we see that having $\alpha \rightsquigarrow \frac{u}{v}$ gives an isomorphism $\mathbb{Z}[\alpha] \approx \mathbb{Z}\left[\frac{u}{v}\right]$, and so $R' \approx \mathbb{Z}\left[\frac{u}{v}\right]$. To show $R' \approx \mathbb{Z}\left[\frac{1}{v}\right]$, we first see that $\mathbb{Z}\left[\frac{1}{v}\right] \subset \mathbb{Z}\left[\frac{u}{v}\right]$ as a subring, since $u \cdot \frac{1}{v} = \frac{u}{v}$. Since $u, v$ are relatively prime, $au + bv = 1$ for some $a, b \in \mathbb{Z}$. Then, dividing out by $v$ gives $a \cdot \frac{u}{v} + b = \frac{1}{v}$. Thus, $\frac{1}{v} \in \mathbb{Z}\left[\frac{u}{v}\right]$, and so $\mathbb{Z}\left[\frac{1}{v}\right] = \mathbb{Z}\left[\frac{u}{v}\right]$. □

# 13 Quadratic Number Fields

## 13.1 Algebraic Integers

**Exercise 13.1.4.** *Let $d$ and $d'$ be integers. When are the fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d'})$ distinct?*

*Solution.* Write $d = s^2 e$ and $d' = s'^2 e'$ such that $e, e'$ are square-free. We claim $\mathbb{Q}(\sqrt{d}) \approx \mathbb{Q}(\sqrt{d'})$ if and only if $e = e'$. $\Leftarrow$ clearly holds by p. 384, so it suffices to show $\Rightarrow$. So suppose $e \neq e'$, and without loss of generality $e \neq 1$. We claim there is no $x + y\sqrt{e'}$ with $x, y \in \mathbb{Q}$ such that $e = (x + y\sqrt{e'})^2 = x^2 + 2xy\sqrt{e'} + y^2 e'$. This implies $2xy = 0$ and $x^2 + y^2 e' = e$. If $x = 0$, then $y^2 e' = e$, so if $y = a/b$ for $(a, b) = 1$,

we have $a^2e = b^2e'$; since $e, e'$ are square-free, then $a = b = 1$, so $e = e'$. On the other hand, if $y = 0$, then $x^2 = e$, contradicting that $e \neq 1$ is square-free. □

## 13.2 Factoring Algebraic Integers

**Exercise 13.2.2.** *For which negative integers $d = 2$ modulo 4 is the ring of integers in $\mathbb{Q}[\sqrt{d}]$ a unique factorization domain?*

*Solution.* Suppose $d \equiv 2 \bmod 4$. The integers $R$ in $\mathbb{Q}[\sqrt{d}]$ are of the form $a + b\sqrt{d}$ for $a, b \in \mathbb{Z}$ (Prop. 13.1.6). We claim $R$ is a UFD if and only if $d = -2$. $\Leftarrow$. $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain (Exercise 12.2.6), hence a UFD by Props. 12.2.7, 12.2.14($b$). $\Rightarrow$. Suppose $d \neq -2$. Consider $2(2 - d/2) = 4 - d = (2 - \sqrt{d})(2 + \sqrt{d})$. We claim 2 is irreducible in $R$; as on p. 386 it suffices to show there is no $a + b\sqrt{d}$ such that $N(a + b\sqrt{d}) = a^2 - b^2d = 2$. For, this would imply $2 \mid d$ hence $2 \mid a^2$, and so $2 \mid a$, which implies $a = 0, b = 1, d = -2$ is the only possibility, a contradiction. Thus, for $R$ to be a UFD we must have either $2 \mid 2 - \sqrt{d}$ or $2 + \sqrt{d}$, but $1 \pm \sqrt{d}/2 \notin R$ when $d \equiv 2 \bmod 4$ by Prop. 13.1.6. □

## 13.3 Ideals in $\mathbb{Z}[\sqrt{-5}]$

**Exercise 13.3.2.** *Let $\delta := \sqrt{-5}$. Decide whether or not the lattice of integer combinations of the given vectors is an ideal: ($a$) $(5, 1 + \delta)$, ($b$) $(7, 1 + \delta)$, ($c$) $(4 - 2\delta, 2 + 2\delta, 6 + 4\delta)$.*

*Remark.* We denote $A$ to be the lattice spanned by the given vectors.

*Solution for ($a$).* $A$ is not an ideal. For, suppose it were; then, $\delta(1+\delta) = -5+\delta \in A$, and so $-5 + \delta = 5a + (1 + \delta)b$ for some $a, b \in \mathbb{Z}$. Thus, $b = 1$, but $-5 = 5a + 1$ has no solution $a \in \mathbb{Z}$. □

*Solution for ($b$).* $A$ is not an ideal, for if it were, then as in ($a$), $\delta(1 + \delta) = -5 + \delta = 7a + (1 + \delta)b \in A$ implies $b = 1$, but $-5 = 7a + 1$ has no solution $a \in \mathbb{Z}$. □

*Solution for ($c$).* We claim $A$ is an ideal. $A$ is closed under addition since it is a lattice, and so it suffices to show $A$ is closed under external multiplication. By the distributive property, it is moreover sufficient to show $\delta$ times any of the generators is in $A$, for $A$ is closed under integer combinations. But this follows since

$$\begin{aligned}
\delta(4 - 2\delta) &= \quad 10 + 4\delta = \quad (4 - 2\delta) + 3(2 + 2\delta) \\
\delta(2 + 2\delta) &= -10 + 2\delta = -2(4 - 2\delta) \ - (2 + 2\delta) \\
\delta(6 + 4\delta) &= -20 + 6\delta = -4(4 - 2\delta) \ + (2 + 2\delta) - (6 + 4\delta)
\end{aligned}$$

□

**Exercise 13.3.3.** *Let $A$ be an ideal of the ring of integers $R$ in an imaginary quadratic field. Prove that there is a lattice basis for $A$, one of whose elements is an ordinary positive integer.*

*Proof.* Let $a' \in A$; then $\overline{a'}a' \in A$ is a positive integer hence $A \cap \mathbb{N}$ is nonempty. Choose $a \in A \cap \mathbb{N}$ that is minimal, and choose $b' \in A$ which is $\mathbb{Z}$-linearly independent from $a'$. Consider the parallelogram $\Pi(a, b') = \{ra + sb' \mid 0 \leq r, s \leq 1\}$. $A \cap \Pi(a, b')$ is finite, and so we can choose $b \in A \cap \Pi(a, b')$ with minimal positive imaginary part. We claim $a, b$ form a lattice basis for $A$. First, $A \cap \Pi(a, b) = \{0, a, b, a + b\}$, for if $c \in (A \cap \Pi(a, b)) \setminus \{0, a, b, a + b\}$, then either $c \in \mathbb{Z}$ but $c < a$, violating minimality of $a$, or $0 < \mathrm{Im}(c) < \mathrm{Im}(b)$, violating minimality of $b$. Finally, we can move $\Pi(a, b)$ by $\mathbb{Z}$-linear combinations of $a, b$, and none of these parallelograms contain anything in $A$ other than linear combinations of $a, b$ for otherwise we can move that point into the parallelogram $\Pi(a, b)$ with an appropriate $\mathbb{Z}$-linear combination of $a, b$. Thus, $a, b$ form a lattice basis for $A$. □

## 13.4 Ideal Multiplication

**Exercise 13.4.3.** *Let $R$ be the ring $\mathbb{Z}[\delta]$, where $\delta = \sqrt{-5}$, and let $A$ and $B$ be ideals of the form $A = (\alpha, \frac{1}{2}(\alpha + \alpha\delta))$, $B = (\beta, \frac{1}{2}(\beta + \beta\delta))$. Prove that $AB$ is a principal ideal by finding its generator.*

*Solution.* By Prop. 13.1.6, we know $2 \mid \alpha$ and $2 \mid \beta$. By Prop. 13.4.3($c$), we have $A = \frac{\alpha}{2}(2, 1 + \delta)$ and $B = \frac{\beta}{2}(2, 1 + \delta)$. Thus, by (13.4.2) and Prop. 13.4.3($a$), we get

$$AB = \frac{\alpha\beta}{4}(2, 1 + \delta)^2 = \frac{\alpha\beta}{4}(4, 2 + 2\delta, -4 + 2\delta) = \frac{\alpha\beta}{4}(2) = \left(\frac{\alpha\beta}{2}\right). \qquad \square$$

## 13.5 Factoring Ideals

**Exercise 13.5.2.** *Let $\delta = \sqrt{-3}$ and $R = \mathbb{Z}[\delta]$. This is not the ring of integers in the imaginary quadratic number field $\mathbb{Q}[\delta]$. Let $A$ be the ideal $(2, 1 + \delta)$.*

- ($a$) *Prove that $A$ is a maximal ideal, and identify the quotient ring $R/A$.*
- ($b$) *Prove that $\overline{A}A$ is not a principal ideal, and that the Main Lemma is not true for this ring.*
- ($c$) *Prove that $A$ contains the principal ideal $(2)$ but that $A$ does not divide $(2)$.*

*Proof of* ($a$). It suffices to show $R/A$ is a field by Prop. 11.8.2($b$). But $R/A = \mathbb{Z}[\delta]/(2, 1 + \delta) \approx \mathbb{Z}/(2) = \mathbb{F}_2$. □

*Proof of* $(b)$. First, we see

$$\overline{A}A = (2, 1-\delta)\cdot(2, 1+\delta) = (4, 2+2\delta, 2-2\delta, 4) = (4, 2+2\delta) = 2\overline{A}.$$

Now if the Main Lemma holds and $\overline{A}A$ is a principal ideal, then by the cancellation law (Cor. 13.4.9$(a)$) we have $A = (2)$, a contradiction since $1+\delta \in A \setminus (2)$. □

*Proof of* $(c)$. $(2) \subset A$ since 2 is a generator of $A$. Now suppose $AB = (2)$ for some ideal $B \subsetneq R$. $B \not\subset A$ for otherwise

$$(2) = AB \subset A^2 = (2, 1+\delta)^2 = (4, 2+2\delta, 2-2\delta) = 2A,$$

which implies $1 \in A$, contradicting that $A$ is maximal from $(a)$. Then, $2\overline{A} = \overline{A}AB = 2\overline{A}B$ by $(b)$, and so $\overline{A} = \overline{A}B$. Now let $C$ be a maximal ideal containing $B$ as exists by Thm. 11.9.2; note $C \neq A$ since $B \not\subset A$. Then, $\overline{A} = \overline{A}B \subset \overline{A}C \subset \overline{A}$, and so we have equalities throughout. But this contradicts Exercise 12.M.6, for $\overline{A}$ and $\overline{A}C$ are two distinct factorizations of $\overline{A}$ into a product of distinct maximal ideals. □

# 14 Linear Algebra in a Ring

## 14.1 Modules

**Exercise 14.1.3.** *Let $R = \mathbb{Z}[\alpha]$ be the ring generated over $\mathbb{Z}$ by an algebraic integer $\alpha$. Prove that for any integer $m$, $R/mR$ is finite.*

*Proof.* Let $f(x) \in \mathbb{Z}[x]$ be the (monic) irreducible polynomial for $\alpha$. Then, $I = (m, f)$ is an ideal in $\mathbb{Z}[x]$ generated by two polynomials that have no common factors, and so $R/mR \approx \mathbb{Z}[x]/(m, f)$ is finite by Exercise 12.M.7$(b)$. □

**Exercise 14.1.4.** *A module is called* simple *if it is not the zero module and if it has no proper submodule.*

- $(a)$ *Prove that any simple $R$ module is isomorphic to an $R$ module of the form $R/M$ where $M$ is a maximal ideal.*
- $(b)$ *Prove* Schur's Lemma: *Let $\varphi\colon S \to S'$ be a homomorphism of simple modules. Prove that $\varphi$ is either zero, or an isomorphism.*

*Proof of* $(a)$. Let $S$ be simple and let $s \in S$ be nonzero. Define $\psi\colon R \to S$ by $r \mapsto rs$; this is a homomorphism since $S$ is a module. Then, $\operatorname{im}\varphi$ is a submodule of $S$, hence equal to $S$ since $S$ is simple, and so $\psi$ is surjective. By the first isomorphism theorem (Thm. 14.1.6$(c)$), $R/\ker\varphi \approx S$. Now $M \coloneqq \ker\varphi$ is a submodule of $R$, then by the correspondence theorem (Thm. 14.1.6$(d)$) $M$ is a maximal submodule of $R$, hence a maximal ideal of $R$ by Prop. 14.1.3. □

*Proof of* $(b)$. $\ker\varphi$ is a submodule of $S$, and $\operatorname{im}\varphi$ is a submodule of $S'$. Since $S'$ is simple, $\operatorname{im}\varphi$ is 0 or $S'$. If $\operatorname{im}\varphi = 0$, then $\varphi = 0$. If $\operatorname{im}\varphi = S'$, then $\ker\varphi \subsetneq S'$, hence equals 0, and so $S \approx S'$ by the first isomorphism theorem (Thm. 14.1.6$(c)$). □

## 14.2 Free Modules

**Exercise 14.2.3.** *Let $A$ be the matrix of a homomorphism $\varphi\colon \mathbb{Z}^n \to \mathbb{Z}^m$ of free $\mathbb{Z}$-modules.*

- $(a)$ *Prove that $\varphi$ is injective if and only if the rank of $A$, as a real matrix, is $n$.*
- $(b)$ *Prove that $\varphi$ is surjective if and only if the greatest common divisor of the determinants of the $m \times m$ minors of $A$ is 1.*

*Remark.* By Thm. 14.4.6, there exist matrices $P \in GL_n(\mathbb{Z})$, $Q \in GL_m(\mathbb{Z})$ such that $A' = Q^{-1}AP$ is diagonal of the form

$$\left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & \\ & & d_k & \\ \hline & & & 0 \end{array}\right) \tag{4}$$

with $d_i \in \mathbb{Z}_{>0}$ and $d_1 \mid d_2 \mid \cdots \mid d_k$. Note $A$ defines an injective (resp. surjective) map $\varphi\colon \mathbb{Z}^n \to \mathbb{Z}^m$ if and only if $A'$ defines an injective (resp. surjective) map $\varphi'\colon \mathbb{Z}^n \to \mathbb{Z}^m$ since $P, Q$ are invertible as integer matrices.

*Proof of* $(a)$. $\varphi$ is injective if and only if $A'$ above has $k = n \leq m$, and this is equivalent to $A$ having rank $n$ as a real matrix since rank is preserved by column and row operations $P, Q$. □

*Proof of* $(b)$. $\varphi$ is surjective if and only if $A'$ above has $d_1 = \cdots = d_k = 1$ and $k = m \geq n$, i.e., the greatest commmon divisor of the determinants of the $m \times m$ minors of $A'$ is 1. It suffices to show that this property is preserved by column and row operations $P, Q$.

Recall (14.4.2): the operations are $(i)$ adding an integer multiple of a row (resp. column) to another, $(ii)$ interchanging two rows (resp. columns), and $(iii)$ multiplying a row (resp. column) by $-1$. But $(i)$ simply adds integer multiples of some determinants to others, $(ii)$ switches some pairs of determinants and multiplies some by $-1$, and $(iii)$ multiplies some determinants by $-1$. So we are done. □

## 14.4 Diagonalizing Integer Matrices

**Exercise 14.4.6.** *Let $\varphi\colon \mathbb{Z}^k \to \mathbb{Z}^k$ be a homomorphism given by multiplication by an integer matrix $A$. Show that the image of $\varphi$ is of finite index if and only if $A$ is non-singular that it if so, then the index is equal to $|\det A|$.*

*Proof.* Since $\mathbb{Z}^k$ is abelian, the index of $\operatorname{im}\varphi \leqslant \mathbb{Z}^k$ is given by $|\mathbb{Z}^k/\operatorname{im}\varphi|$. By Thm. 14.4.6, there exist $P, Q \in GL_k(\mathbb{Z})$ such that $A' = Q^{-1}AP$ is diagonal of the form (4), with diagonal entries $d_1 \mid d_2 \mid \cdots \mid d_r$ followed by $k-r$ zeros, and so

$$\mathbb{Z}^k/\operatorname{im}\varphi = \mathbb{Z}^k/A\mathbb{Z}^k \approx \mathbb{Z}^k/A'\mathbb{Z}^k \approx \prod_{i=1}^{r}(\mathbb{Z}/d_1\mathbb{Z}) \times \mathbb{Z}^{k-r}. \tag{5}$$

Thus, $|\mathbb{Z}^k/\operatorname{im}\varphi| < \infty$ if and only if $r = k$. But this is true if and only if

$$\det A = \det Q \det A' \det P = \det Q \det P \prod_{i=1}^{k} d_i \neq 0, \tag{6}$$

i.e., $\det A$ is nonsingular. If $|\mathbb{Z}^k/\operatorname{im}\varphi| < \infty$, then (5) gives $|\mathbb{Z}^k/\operatorname{im}\varphi| = \prod_{i=1}^{k} d_i$, which equals $|\det A|$ by (6). □

## 14.5 Generators and Relations

**Exercise 14.5.1.** *Let $R = \mathbb{Z}[\delta]$ where $\delta = \sqrt{-5}$. Determine a presentation matrix as an $R$-module for the ideal $(2, 1+\delta)$.*

*Proof.* Let $\varphi\colon R^2 \to I$ that sends $(x, y) \rightsquigarrow 2x + (1+\delta)y$. Now

$$\ker\varphi = \left\{(x,y) \in R^2 \;\middle|\; x = -\frac{1+\delta}{2}y\right\} \leftrightarrow \left\{y \in R^2 \;\middle|\; \frac{1+\delta}{2}y \in R\right\}$$

where $\leftrightarrow$ denotes bijection. But $y = 2, 1-\delta$ are the elements in $R$ with smallest norm satisfying this condition, and moreover the corresponding vectors $(-3, 1-\delta), (-1-\delta, 2) \in R$ are independent over $R$ since $2r \neq 1-\delta$ for any $r \in R$. Thus, $\ker\varphi$ is generated by these two vectors, and by pp. 424–425 we have a presentation matrix

$$A = \begin{pmatrix} -3 & -1-\delta \\ 1-\delta & 2 \end{pmatrix}. \qquad \square$$

## 14.7 Structure of Abelian Groups

**Exercise 14.7.7.** *Let $R = \mathbb{Z}[i]$ and let $V$ be the $R$-module given by the elements $v_1$ and $v_2$ with relations $(1+i)v_1 + (2-i)v_2 = 0$ and $3v_1 + 5iv_2 = 0$. Write this module as a direct sum of cyclic modules.*

*Proof.* We use the relations to find a presentation matrix $A$ and then diagonalize it following the proof of Thm. 14.4.6:

$$\begin{pmatrix} 1+i & 3 \\ 2-i & 5i \end{pmatrix} \xrightarrow{\left(\begin{smallmatrix} 1 & 0 \\ -1+i & 1 \end{smallmatrix}\right)\cdot} \begin{pmatrix} 1+i & 3 \\ -i & -3+8i \end{pmatrix} \xrightarrow{\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\cdot} \begin{pmatrix} -i & -3+8i \\ 1+i & 3 \end{pmatrix}$$

$$\xrightarrow{\left(\begin{smallmatrix} i & 0 \\ 1 & 0 \end{smallmatrix}\right)\cdot} \begin{pmatrix} 1 & -8-3i \\ 1+i & 3 \end{pmatrix} \xrightarrow{\left(\begin{smallmatrix} 1 & 0 \\ -1-i & 1 \end{smallmatrix}\right)\cdot} \begin{pmatrix} 1 & -8-3i \\ 0 & 8+11i \end{pmatrix}$$

This reduces to the $1\times 1$ matrix $(8+11i)$ by Prop. 14.5.7$(iv)$, and so $V \approx R/(8+11i)$. To decompose further, we need to factor $8+11i$. But

$$N(8+11i) = 64 + 121 = 185 = 5 \cdot 37 = (2+i)(2-i)(6+i)(6-i),$$

and $i(2-i)(6-i) = i(12-8i-1) = 8+11i$, hence $V \approx R/(8+11i) \approx R/(2-i) \oplus R/(6-i)$ by Exercise 11.6.8$(c)$, where we note the map $\varphi$ in Exercise 11.6.8 is also an $R$-module isomorphism. □

## 14.8 Applications to Linear Operators

**Exercise 14.8.2.** *Let $M$ be a $\mathbb{C}[t]$-module of the form $\mathbb{C}[t]/(t-\alpha)^n$. Show that there is a $\mathbb{C}$-basis for $M$, such that the matrix of the corresponding linear operator is a Jordan block.*

*Proof.* By Prop. 11.5.5, $1, t, \ldots, t^{n-1}$ is a basis for $M$ over $\mathbb{C}$, and following p. 435, we have the following matrix for multiplication by $t$ in this basis:

$$T = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix}, \quad a_{n-i} = (-\alpha)^i \binom{n}{i}$$

by using the binomial formula. This has characteristic polynomial $f(t) = (t-\alpha)^n$ as on p. 435, hence by the Jordan normal form it suffices to show $\dim \ker(\alpha I - T) = 1$. By rank-nullity it suffices to show $\mathrm{rk}(\alpha I - T) \geq n-1$, for an eigenvalue has geometric multiplicity at least one. For $\alpha = 0$, we are done, so suppose $\alpha \neq 0$. Then, the matrix

$$\alpha I - T = \begin{pmatrix} \alpha & & & & a_0 \\ -1 & \alpha & & & a_1 \\ & -1 & \ddots & & \vdots \\ & & \ddots & \alpha & a_{n-2} \\ & & & -1 & \alpha + a_{n-1} \end{pmatrix}$$

turns into the matrix

$$\begin{pmatrix} 1 & & & & a_0/\alpha \\ & 1 & & & a_1/\alpha + a_0/\alpha^2 \\ & & \ddots & & \vdots \\ & & & 1 & a_{n-2}/\alpha + \cdots + a_0/\alpha^{n-1} \\ & & & & 1 + a_{n-1}/\alpha + a_{n-2}/\alpha^2 + \cdots + a_0/\alpha^n \end{pmatrix}$$

by Gaussian elimination, and so $\mathrm{rk}(\alpha I - T) \geq n - 1$. □

**Exercise 14.8.4.** *Let $V$ be an $F[t]$-module, and let $\mathbf{B} = (v_1, \ldots, v_n)$ be a basis for $V$ as $F$-vector space. Let $B$ be the matrix of $T$ with respect to this basis. Prove that $A = tI - B$ is a presentation matrix for the module.*

*Proof.* We want to show that $\operatorname{im} A = \ker(p\colon F[t]^n \to V)$ where $p$ is given by $(f_i)_{i=1}^n \rightsquigarrow \sum_{i=1}^n f_i v_i$. The inclusion $\subset$ is clear, for $B$ is multiplication by $t$ on $V$.

For the other direction, suppose $(f_i)_{i=1}^n \in \ker p$, i.e., $\sum_{i=1}^n f_i v_i = 0$. If each $f_i = \sum a_{ij} t^j$, we then have

$$\begin{aligned} \sum_{i=1}^n f_i v_i &= \sum_{i=1}^n \sum_{j \geq 0} a_{ij} t^j v_i \\ &= \sum_{i=1}^n \left[ a_{i0} v_i + \sum_{j \geq 1} a_{ij} t^{j-1} ((t-B)v_i + Bv_i) \right] \\ &= (p \circ A) \left( \sum_{j \geq 0} a_{ij} t^{j-1} \right)_{i=1}^n + \sum_{i=1}^n \left[ a_{i0} v_i + \sum_{j \geq 1} a_{ij} t^{j-1} B v_i \right] \\ &= \sum_{i=1}^n \left[ a_{i0} v_i + \sum_{j \geq 1} a_{ij} t^{j-1} B v_i \right], \end{aligned}$$

since $p \circ A = 0$ by the above. Then, repeating this process, we get

$$\sum_{i=1}^{n} f_i v_i = \sum_{i=1}^{n} \sum_{j \geq 0} a_{ij} B^j v_i = \sum_{i=1}^{n} b_i v_i = 0$$

for some coefficients $b_i \in F$, i.e., each contribution from the $f_i$ above could be put in the form $(p \circ A)(w)$ for some $w \in F[t]^n$, and so $\operatorname{im} A \supset \ker p$. □

## 14.M Miscellaneous Problems

**Exercise 14.M.10.**

(*a*) *Prove that the multiplicative group $\mathbb{Q}^\times$ of rational numbers is isomorphic to the direct sum of a cyclic group of order 2 and a free abelian group with countably many generators.*

(*b*) *Prove that the additive group $\mathbb{Q}^+$ of rational numbers is not a direct sum of two proper subgroups.*

(*c*) *Prove that the quotient group $\mathbb{Q}^+/\mathbb{Z}^+$ is not a direct sum of cyclic groups.*

*Proof of* (*a*). Let $\langle -1 \rangle = \{-1, 1\}$ with the obvious group structure making it isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Let $\langle p \rangle = \{p^k \mid k \in \mathbb{Z}\}$ with the obvious group structure making it isomorphic to $\mathbb{Z}$. Then, define the map

$$\langle -1 \rangle \oplus \bigoplus_{p \text{ prime}} \langle p \rangle \to \mathbb{Q}^\times$$
$$\sigma \oplus \bigoplus_{p \text{ prime}} p^{k_p} \rightsquigarrow \sigma \prod_{p \text{ prime}} p^{k_p}$$

Note that $\bigoplus \langle p \rangle$ is a free abelian group. This map is a group homomorphism since $(\sigma, k_2, \ldots) \cdot (\tau, \ell_2, \ldots)$ gets mapped to $\sigma\tau \prod p^{k_p + \ell_p} = \sigma \prod p^{k_p} \cdot \tau \prod p^{\ell_p}$. This map is clearly surjective since any rational number $r/s$ has prime decompositions for $r$ and $s$, which we use to find a preimage on the left. Similarly, this is injective since something on the right is equal to 1 if and only if $\sigma = 1$ and $k_p = 0$ for all $p$. □

*Proof of* (*b*). Let $G, H$ be proper nontrivial subgroups of $\mathbb{Q}^+$; it suffices to show they have nontrivial intersection by Prop. 2.11.4(*d*). If $p/q \in G, s/t \in H$ for some $p, s \neq 0$, then $qs(p/q) = pt(s/t) = ps \in G \cap H$, while $ps \neq 0$ by assumption. □

*Proof of* (*c*). Suppose $\mathbb{Q}^+/\mathbb{Z}^+ \approx \bigoplus_k H_k$ for $H_k$ cyclic. Let (the image of) $p_k/q_k + \mathbb{Z}^+ \in H_k$ generate $H_k$ for $(p_k, q_k) = 1$. Let $sp_k + tq_k = 1$ for some integers $s, t$; then,

$$\frac{1}{q_k} + \mathbb{Z}^+ = \frac{sp_k}{q_k} + \frac{tq_k}{q_k} + \mathbb{Z}^+ = s\frac{p_k}{q_k} + \mathbb{Z}^+ \in H_k,$$

hence we can assume that (the image of) $1/q_k$ generates $H_k$. Now consider the element $1/q_1^2 + \mathbb{Z}^+ \in \mathbb{Q}^+/\mathbb{Z}^+$. $1/q_1^2 + \mathbb{Z}^+$ then has a decomposition

$$\frac{1}{q_1^2} + \mathbb{Z}^+ = \sum_k \frac{r_k}{q_k} + \mathbb{Z}^+,$$

where $q_k \mid r_k$ for all but finitely many values of $k$. Adding it to itself $q_1$ times gives

$$\frac{1}{q_1} + \mathbb{Z}^+ = \sum_k \frac{q_1 r_k}{q_k} + \mathbb{Z}^+$$

and since we had a direct sum decomposition, $q_k \mid q_1 r_k$ for all $k \neq 1$, and $q_1 \mid q_1 r_1 - 1$. But this last property implies $q_1 \mid 1$, a contradiction. □

# 15 Fields

## 15.2 Algebraic and Transcendental Elements

**Exercise 15.2.1.** *Let $\alpha$ be a complex root of the polynomial $x^3 - 3x + 4$. Find the inverse of $\alpha^2 + \alpha + 1$ in the form $a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbb{Q}$*

*Proof.* Suppose $1 = (a + b\alpha + c\alpha^2)(1 + \alpha + \alpha^2)$. We can rewrite this as

$$1 = a + (a + b)\alpha + (a + b + c)\alpha^2 + (b + c)\alpha^3 + c\alpha^4$$

We then note that $\alpha^3 = 3\alpha - 4$ and $\alpha^4 = 3\alpha^2 - 4\alpha$, and so we get the equation

$$\begin{aligned} 1 &= a + (a + b)\alpha + (a + b + c)\alpha^2 + (b + c)(3\alpha - 4) + c(3\alpha^2 - 4\alpha) \\ &= (a - 4b - 4c) + (a + 4b - c)\alpha + (a + b + 4c)\alpha^2 \end{aligned}$$

Since $1, \alpha$, and $\alpha^2$ are linearly independent over $\mathbb{Q}$, we get a system of linear equations, with solution

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 & -4 & -4 \\ 1 & 4 & -1 \\ 1 & 1 & 4 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{49} \begin{pmatrix} 17 & 12 & 20 \\ -5 & 8 & -3 \\ -3 & -5 & 8 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{49} \begin{pmatrix} 17 \\ -5 \\ -3 \end{pmatrix}$$

and so $(1 + \alpha + \alpha^2)^{-1} = \frac{1}{49}(17 - 5\alpha - 3\alpha^2)$. □

**Exercise 15.2.3.** *Let $\beta = \omega\sqrt[3]{2}$ where $\omega = e^{2\pi i/3}$, and let $K = \mathbb{Q}(\beta)$. Prove that the equation $x_1^2 + \cdots + x_k^2 = -1$ has no solution with $x_i$ in $K$.*

*Proof.* $\beta$ has minimal polynomial $x^3 - 2$, which has roots $\sqrt[3]{2} = \omega^2\beta$, $\beta$, and $\omega\beta$. Thus, by Prop. 15.2.8, there is an isomorphism $\mathbb{Q}(\beta) \approx \mathbb{Q}(\sqrt[3]{2})$. But then, if $x_1^2 + \cdots + x_k^2 = -1$ has a solution in $\mathbb{Q}(\beta)$, it has a solution $x_i = a_i + b_i\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ by Prop. 15.2.10, contradicting that this equation has no real solutions. □

## 15.3 The Degree of a Field Extension

**Exercise 15.3.2.** *Prove that the polynomial $x^4 + 3x + 3$ is irreducible over the field $\mathbb{Q}[\sqrt[3]{2}]$.*

*Proof.* Since $f \coloneqq x^4 + 3x + 3 \equiv x^4 + x + 1 \bmod 2$ is irreducible over $\mathbb{F}_2$ by Exercise 12.4.19, $f$ is irreducible over $\mathbb{Q}$ as well by Prop. 12.4.3.

Now let $\alpha$ be a root of $f$; then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ while $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, and so $[\mathbb{Q}(\alpha, \sqrt[3]{2})] = 12$ by Cor. 15.3.8. But $12 = [\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ implies $[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 4$ by the multiplicative property of the degree (Thm. 15.3.5). Thus, the minimal polynomial of $\alpha$ over $\mathbb{Q}(\sqrt[3]{2})$ has degree 4, and so $x^4 + 3x + 3$ has no factors in $\mathbb{Q}(\sqrt[3]{2})[x]$ by Lem. 15.3.2($b$). □

**Exercise 15.3.5.** *Determine the values of $n$ such that $\zeta_n$ has degree at most 3 over $\mathbb{Q}$.*

*Proof.* If $p$ is a prime dividing $n$, then $\zeta_p^n = 1$, hence $\mathbb{Q}(\zeta_n) \supset \mathbb{Q}(\zeta_p)$. Now $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ by Thm. 12.4.9, and so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq 3$ implies that if $p \mid n$, then $p \in \{2, 3\}$. Thus, $n = 2^i 3^j$.

We claim $i \leq 2, j \leq 1$. $[\mathbb{Q}(\zeta_2) : \mathbb{Q}] = 1$ and $[\mathbb{Q}(\zeta_4) : \mathbb{Q}] = 2$ because the minimal polynomial of $\zeta_4$ is $x^2 + 1$. Similarly, $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$. But any extension of $\mathbb{Q}(\zeta_4)$ or $\mathbb{Q}(\zeta_3)$ will have degree $\geq 4$ over $\mathbb{Q}$ by Thm. 15.3.5, hence $i \leq 2, j \leq 1$.

By the above, $n \in \{1, 2, 3, 4, 6, 12\}$, and also $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq 3$ for $n \in \{1, 2, 3, 4\}$, hence it suffices to check whether $n \in \{6, 12\}$ are also possible values of $n$. $\zeta_6 = -\zeta_3$ hence $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$. On the other hand, $\mathbb{Q}(\zeta_{12}) \supset \mathbb{Q}(\zeta_3, \zeta_4)$, which has degree $\geq 6$ over $\mathbb{Q}$ by Thm. 15.3.5, and so $n \neq 12$. Thus, $n \in \{1, 2, 3, 4, 5, \}$. □

**Exercise 15.3.7.** ($a$) *Is $i$ in the field $\mathbb{Q}(\sqrt[4]{-2})$?* ($b$) *Is $\sqrt[3]{5}$ in the field $\mathbb{Q}(\sqrt[3]{2})$?*

*Proof of* ($a$). Suppose $i \in \mathbb{Q}(\sqrt[4]{-2})$. Then, there exists $a, b \in \mathbb{Q}$ such that $(a + b\sqrt[4]{-2})^2 = -1$. But then,

$$(a + b\sqrt[4]{-2})^2 = a^2 + 2ab\sqrt[4]{-2} + b^2\sqrt[2]{-2} = -1,$$

and since $\{1, \sqrt[4]{-2}, \sqrt[2]{-2}\}$ are linearly independent over $\mathbb{Q}$ by Prop. 15.2.7, $a^2 = -1$, which is impossible since $a \in \mathbb{Q}$. □

*Proof of* ($b$). If $\sqrt[3]{5} \in \mathbb{Q}(\sqrt[3]{2})$, then $\alpha \coloneqq \sqrt[3]{2} + \sqrt[3]{5} \in \mathbb{Q}(\sqrt[3]{2})$ must have degree at most 3 over $\mathbb{Q}$. Let $f(x) = x^9 - 21x^6 - 123x^3 - 343$; then, $f(\alpha) = 0$. But $f(x)$ is irreducible by the Eisenstein criterion (Prop. 12.4.6) since $3 \mid 21, 123$ while $9 \nmid 343$, hence $f$ is irreducible and so $\alpha$ has degree 9 over $\mathbb{Q}$, a contradiction. □

**Exercise 15.3.9.** *Let $\alpha$ and $\beta$ be complex roots of irreducible polynomials $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$. Let $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$. Prove that $f(x)$ is irreducible in $L[x]$ iff $g(x)$ is irreducible in $K[x]$.*

*Proof.* Let $m = \deg f, n = \deg g$. By the multiplicative property of the degree (Thm. 15.3.5), we have $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [L(\alpha) : L][L : \mathbb{Q}] = [K(\beta) : K][K : \mathbb{Q}]$. Hence, $f(x)$ is irreducible in $L[x]$ if and only if $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = mn$ if and only if $g(x)$ is irreducible in $K[x]$. □

**Exercise 15.3.10.** *A field extension $K/F$ is an algebraic extension if every element of $K$ is algebraic over $F$. Let $K/F$ and $L/K$ be algebraic field extensions. Prove that $L/F$ is an algebraic extension.*

*Proof.* Let $\alpha \in L$; we want to show $\alpha$ is algebraic over $F$. Let $\alpha = \sum_{i=1}^{m} b_i \alpha_i$ for $b_i \in K$, $\alpha_i \in L$ linearly independent and algebraic over $K$. Write $\alpha_i = \sum_{j=1}^{n} c_j \beta_j$ for $c_j \in F$, $\beta_j \in K$ linearly independent and algebraic over $F$. Thus, we have $\alpha \in F(\beta_1, \ldots, \beta_n)(\alpha_1, \ldots, \alpha_m)$. Now if $\alpha$ is transcendental over $F$, then by Thm. 15.3.5,

$$[F(\beta_1, \ldots, \beta_n)(\alpha_1, \ldots, \alpha_m) : F(\beta_1, \ldots, \beta_n)][F(\beta_1, \ldots, \beta_n) : F] \geq [F(\alpha) : F] = \infty,$$

which contradicts Cor. 15.3.6($c$). □

## 15.4 Finding the Irreducible Polynomial

**Exercise 15.4.1.** *Let $K = \mathbb{Q}(\alpha)$, where $\alpha$ is a root of $x^3 - x - 1$. Determine the irreducible polynomial of $\gamma = 1 + \alpha^2$ over $\mathbb{Q}$.*

*Proof.* First, $\gamma$ satisfies $(x-1)(x-2)^2 - 1 = x^3 - 5x^2 + 8x - 5 = 0$ since

$$(\gamma - 1)(\gamma - 2)^2 - 1 = \alpha^2(\alpha^2 - 1)^2 - 1 = (\alpha^3 - \alpha)^2 - 1 = 1^2 - 1 = 0.$$

Now Thm. 15.3.5 implies $[K : \mathbb{Q}] = [K : \mathbb{Q}(\gamma)][\mathbb{Q}(\gamma) : \mathbb{Q}] = 3$ and so $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 3$ since $\gamma \notin \mathbb{Q}$. Thus, $x^3 - 5x^2 + 8x - 5$ is the irreducible polynomial of $\gamma$ over $\mathbb{Q}$. □

**Exercise 15.4.2.** *Determine the irreducible polynomial for $\alpha = \sqrt{3} + \sqrt{5}$ over the following fields. ($a$) $\mathbb{Q}$, ($b$) $\mathbb{Q}(\sqrt{5})$, ($c$) $\mathbb{Q}(\sqrt{10})$, ($d$) $\mathbb{Q}(\sqrt{15})$.*

*Solution for ($a$).* Let $f(x) = (x^2 - 8)^2 - 60 = x^4 - 16x^2 + 4$. Then, $f(\alpha) = 0$; we claim $f$ is irreducible. $f$ cannot have linear factors since a root must be an integer dividing 4 by the rational root test, and these are not roots. Now suppose $f$ had quadratic factors; then by Prop. 12.3.7($a$), for some $a, b, c, d \in \mathbb{Z}$ we have

$$f(x) = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd.$$

Now $a+c=0$ implies $ad+bc=a(d-b)=0$. $a\neq 0$ since otherwise $b+d=-16$ and $bd=4$, a contradiction. So, $d=b=2$, but then $2+ac+2=-16$ implies $ac=-20$, which contradicts $a+c=0$. Hence $f$ is the irreducible polynomial for $\alpha$ over $\mathbb{Q}$. $\square$

*Solution for* $(b)$. Let $f(x)=(x-\sqrt{5})^2-3=x^2-2\sqrt{5}+2$; then $f(\alpha)=0$. $f$ splits if and only if the two roots $\sqrt{5}\pm\sqrt{3}$ are in $\mathbb{Q}(\sqrt{5})$. But $\sqrt{3}\notin\mathbb{Q}(\sqrt{5})$, for otherwise $\sqrt{3}=a+b\sqrt{5}$ implies $3=a^2+2ab\sqrt{5}+5b^2$, and solving for $\sqrt{5}$ gives that $\sqrt{5}\in\mathbb{Q}$, a contradiction. Hence $f$ is the irreducible polynomial for $\alpha$ over $\mathbb{Q}(\sqrt{5})$. $\square$

*Solution for* $(c)$. Let $f(x)=x^4-16x^2+4$. By Cor. 15.3.8 and $(a)$, $\mathbb{Q}(\alpha,\sqrt{10})$ must have degree either 4 or 8 over $\mathbb{Q}$, hence by the multiplicative property of the degree (Thm. 15.3.5), $\sqrt{10}$ has degree 2 or 1 over $\mathbb{Q}(\alpha)$. To show $\sqrt{10}$ does not have degree 1 over $\mathbb{Q}(\alpha)$, it suffices to show it is not in $\mathbb{Q}(\alpha)$ by Lem. 15.3.2$(b)$. But this is clear since if $\sqrt{10}=a+b\alpha$ for $a,b\in\mathbb{Q}$, then

$$10=a^2+2ab\alpha+b^2\alpha^2=a^2+8b^2+2ab\sqrt{3}+2ab\sqrt{5}+2b^2\sqrt{15}$$

implies $b=0$, contradicting that $\sqrt{10}\notin\mathbb{Q}$. Now $\alpha$ has degree 4 over $\mathbb{Q}(\sqrt{10})$ since

$$[\mathbb{Q}(\alpha,\sqrt{10}):\mathbb{Q}(\sqrt{10})][\mathbb{Q}(\sqrt{10}):\mathbb{Q}]=[\mathbb{Q}(\alpha,\sqrt{10}):\mathbb{Q}(\sqrt{10})]\cdot 2=8$$

and so $f$ is the irreducible polynomial for $\alpha$ over $\mathbb{Q}(\sqrt{10})$. $\square$

*Solution for* $(d)$. Let $f(x)=x^2-8-2\sqrt{15}$; then $f(\alpha)=0$. Now

$$4=[\mathbb{Q}(\alpha,\sqrt{15}):\mathbb{Q}]=[\mathbb{Q}(\alpha,\sqrt{15}):\mathbb{Q}(\sqrt{15})][\mathbb{Q}(\sqrt{15}):\mathbb{Q}]$$

by $(a)$ since $\sqrt{15}=(\alpha^2-8)/2\in\mathbb{Q}(\alpha)$, hence $\alpha$ has degree 2 over $\mathbb{Q}(\sqrt{15})$, and so $f$ is the irreducible polynomial for $\alpha$ over $\mathbb{Q}(\sqrt{15})$. $\square$

## 15.6 Adjoining Roots

**Exercise 15.6.1.** *Let $F$ be a field of characteristic 0, let $f'$ be the derivative of $f\in F[x]$, and let $g$ be an irreducible polynomial that is a common divisor of $f$ and $f'$. Prove that $g^2$ divides $f$.*

*Proof.* $f=gh$ for some $h\in F[x]$, hence $f'=gh'+g'h$ by Exercise 11.3.5$(a)$. If $g\mid f'$, then $g\mid g'h$. $g$ is prime since it is irreducible, hence $g\mid g'$ or $g\mid h$. But $g\nmid g'$ since $\deg g'<\deg g$, hence $h=gr$ for some $r\in F[x]$. Thus, $f=g^2r$, i.e., $g^2\mid f$. $\square$

## 15.7 Finite Fields

**Exercise 15.7.4.** *Determine the number of irreducible polynomials of degree* 3 *over* $\mathbb{F}_3$ *and over* $\mathbb{F}_5$.

*Proof.* By Thm. 15.7.3($b$), for prime $p$ the irreducible factors of $x^{p^3}-x$ are the monic irreducible polynomials in $\mathbb{F}_p[x]$ with degree 1 or 3. $x, x-1, x-2, \ldots, x-(p-1)$ are the linear irreducible polynomials, hence there are $p(p-1)(p+1)/3$ monic irreducible polynomials of degree 3 in $\mathbb{F}_p[x]$. Since by Thm. 15.7.3($c$) there are $p-1$ units in $\mathbb{F}_p$, we have that there are $p(p-1)^2(p+1)/3$ irreducible polynomials of degree 3 over $\mathbb{F}_p$. Thus, for $\mathbb{F}_3$ we have 16, and for $\mathbb{F}_5$ we have 160 irreducible polynomials of degree 3. Note this matches our result from Exercise 12.4.12. □

**Exercise 15.7.6.** *Factor the polynomial* $x^{16}-x$ *over the fields* $\mathbb{F}_4$ *and* $\mathbb{F}_8$.

*Solution for* $\mathbb{F}_4$. We claim $x^{16}-x$ factors as the product of all monic irreducible polynomials over $\mathbb{F}_4$ of degree 1 and 2. First, $x^4-x \mid x^{16}-x$ by Thm. 15.7.3($a$), ($e$), hence every monic irreducible polynomial of degree 1, $x-a \mid x^{16}-x$ for $a \in \mathbb{F}_4$ divides $x^{16}-x$. Now let $g$ be a monic irreducible polynomial of degree 2 over $\mathbb{F}_4$. If $\beta$ is a root of $g$ in $\mathbb{F}_{16}$ then $[\mathbb{F}_4(\beta) : \mathbb{F}_4] = 2$, hence $\mathbb{F}_4(\beta) \approx \mathbb{F}_{16}$ by Thm. 15.7.3($d$). Thus, $x-\beta \mid x^{16}-x$, so $g \mid x^{16}-x$ by considering the other root of $g$ and proceeding in the same way. Thus, $x^{16}-x$ is divisible by every monic irreducible polynomial over $\mathbb{F}_4$ of degree 1 or 2. Now there are 4 irreducible monic polynomials of degree 1 and $4^2 - \binom{4}{2} - 4 = 6$ irreducible monic polynomials of degree 2 over $\mathbb{F}_4$, which means the total degree of their product is 16 as desired. Thus, we have that

$$\begin{aligned} x^{16}-x = x(x-1)(x-\alpha)(x-\alpha-1)(x^2+x+\alpha)(x^2+x+(\alpha+1)) \\ (x^2+\alpha x+1)(x^2+\alpha x+\alpha)(x^2+(\alpha+1)x+1)(x^2+(\alpha+1)x+(\alpha+1)). \end{aligned}$$ □

*Solution for* $\mathbb{F}_8$. We claim $x^{16}-x$ factors in the same way as over $\mathbb{F}_2$, i.e.,

$$x^{16}-x = x(x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

It suffices to show the degree 4 factors are irreducible over $\mathbb{F}_8$. Since there are no intermediate fields between $\mathbb{F}_2$ and $\mathbb{F}_8$ by Thm. 15.7.3($e$), we know there are no new linear factors of $x^{16}-x$, since its roots are the elements in $\mathbb{F}_{16}$. Let $\alpha \in \mathbb{F}_8$ such that $\mathbb{F}_8 \approx \mathbb{F}_2(\alpha)$. Suppose one of the degree 4 factors has a degree 2 factor. Let $\beta$ be one of its roots; by Thm. 15.7.3($a$) it is an element of $\mathbb{F}_{16}$, and $\mathbb{F}_{16} \approx \mathbb{F}_2(\beta)$ as in the solution for $\mathbb{F}_4$. Then, $[\mathbb{F}_8(\beta) : \mathbb{F}_8] = 2$, hence $\mathbb{F}_8(\beta) \approx \mathbb{F}_{64}$ by Thm. 15.7.3($d$). But $\mathbb{F}_{64} \approx \mathbb{F}_8(\beta) \approx \mathbb{F}_2(\alpha, \beta) \approx \mathbb{F}_{2^r}$ where $r = 12$ by Cor. 15.3.8, a contradiction. □

**Exercise 15.7.7.** *Let $K$ be a finite field. Prove that the product of the nonzero elements of $K$ is $-1$.*

*Proof.* For every nonzero $a \in K$ there is $a^{-1} \in K$ such that $aa^{-1} = 1$ since $K$ is a field. In the product $\Pi$ of nonzero elements of $K$, we can pair off each $a, a^{-1}$ such that $a \neq a^{-1}$ so that $\Pi$ is the product of all nonzero elements of $K$ such that $a^{-1} = a$. We claim this is true if and only if $a = \pm 1$. If $a = a^{-1}$, then $a^2 = 1$ and so $a$ is a root of $x^2 - 1 = (x+1)(x-1)$. Since $K[x]$ is a UFD (Prop. 12.2.14($c$)), this implies $a = \pm 1$. Thus, $\Pi = 1 \cdot (-1) = -1$. □

**Exercise 15.7.8.** *The polynomials $f(x) = x^3 + x + 1$ and $g(x) = x^3 + x^2 + 1$ are irreducible over $\mathbb{F}_2$. Let $K$ be the field extension obtained by adjoining a root of $f$, and let $L$ be the extension obtained by adjoining a root of $g$. Describe explicitly an isomorphism from $K$ to $L$, and determine the number of such isomorphisms.*

*Proof.* Let $\alpha$ be a root of $f$, and $\beta$ one of $g$. Then, $\alpha^3 = \alpha + 1$ and $\beta^3 = \beta^2 + 1$. Any field homomorphism $\varphi\colon K \to L$ is specified by $\varphi(\alpha)$, satisfying that $\varphi(\alpha^3) = \varphi(\alpha+1)$ by the mapping property of quotient rings (Thm. 11.4.2). So let $\varphi(\alpha) = a + b\beta + c\beta^2$.

$$\begin{aligned}\varphi(\alpha^3) &= (a^2 + b^2\beta^2 + c^2\beta^4)(a + b\beta + c\beta^2) \\ &= (a^3 + ac^2 + b^3 + b^2c + bc^2) + (a^2b + ac^2 + b^2c + bc^2 + c^3)\beta \\ &\quad + (a^2c + ab^2 + ac^2 + b^3 + b^2c + c^3)\beta^2\end{aligned}$$

must then be equal to $\varphi(\alpha + 1)$.

We claim $\varphi$ is an isomorphism if and only if $(a, b, c) \in \{(1,1,0), (1,0,1), (0,1,1)\}$. By Prop. 11.8.4($b$), it suffices to show $\varphi$ is surjective if and only if this is true. Suppose $\varphi$ is surjective; then not both $b, c$ are zero by the above. Matching $1, \beta, \beta^2$ terms, we have that if $b = 0$, then $a = c = 1$; if $c = 0$, then $a = b = 1$; and if $b = c = 1$, then $a = 0$. Conversely, since $\varphi(\alpha + 1) = \beta$ in the first case, $\varphi(\alpha^2 + \alpha + 1) = \beta$ in the second case, and $\varphi(\alpha^2 + 1) = \beta$ in the third case, we see in each case that $\varphi$ is surjective by using that $\varphi$ is an homomorphism. □

**Exercise 15.7.10.** *Let $F$ be a finite field, and let $f(x)$ be a nonconstant polynomial whose derivative is the zero polynomial. Prove that $f$ cannot be irreducible over $F$.*

**Lemma 15.7.10a.** *In a finite field of order $p^r$, every element is a $p$th power.*

*Proof of Lemma* 15.7.10$a$. Let $a \in F$; if $a = 0$ we are done so suppose not. $|F^\times| = p^r - 1$ by Thm. 15.7.3($c$), hence $a^{p^r - 1} = 1$ and $a^{p^r} = a$. Thus, $b \coloneqq a^{p^{r-1}}$ satisfies $b^p = a$. □

*Main Proof.* Let $f(x) = \sum_{i=0}^{n} a_i x^i$. Then, if $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1} = 0$, we have $ia_i = 0$ for all $i \geq 1$. Since $F$ is a domain, this implies either $a_i = 0$ or $i \equiv 0 \bmod p$. Thus, $f(x) = \sum_{j=0}^{m} a_j x^{pj}$ for some $a_j \in F$ where $p = \operatorname{char} F$. There exist $b_j$ such that $b_j^p = a_j$ by Lemma 15.7.10a. Thus, $f(x) = g(x)^p$ where $g(x) = \sum_{j=0}^{m} b_j x^j$ by Exercise 11.3.8, and so $f(x)$ is not irreducible. □

**Exercise 15.7.11.** *Let $f = ax^2 + bx + c$ with $a, b, c$ in a ring $R$. Show that the ideal of the polynomial ring $R[x]$ that is generated by $f$ and $f'$ contains the discriminant, the constant polynomial $b^2 - 4ac$.*

*Proof.* $f' = 2ax + b$. Proceeding as in the Euclidean algorithm (p. 45), we have

$$2ax^2 + 2bx + 2c = x(2ax + b) + (bx + 2c), \quad b(2ax + b) = 2a(bx + 2c) + (b^2 - 4ac),$$

hence $b^2 - 4ac = -4af + f'^2 \in (f, f') \subset R[x]$. □

**Exercise 15.7.13.** *Prove that a finite subgroup of the multiplicative group of any field $F$ is a cyclic group.*

*Proof.* A finite subgroup $H \leqslant F^\times$ is a finite abelian group. Thus, $H \approx C_1 \oplus \cdots \oplus C_n$ where the $C_i$ are cyclic groups, and $|C_i|$ divides $|C_{i+1}|$ by Thm. 14.7.3. Let $d \coloneqq |C_n|$. Then, $x^d = 1$ for every $x \in H$. This means that every $x \in H$ is a root of $x^d - 1$. Now, $x^d - 1$ has at most $d$ roots, so $d \geq |H|$. On the other hand, $d \leq |H|$ by the decomposition above, so $d = |H|$, and $n = 1$, i.e., $H$ is cyclic. □

## 15.8 Primitive Elements

**Exercise 15.8.2.** *Determine all primitive elements for the extension $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$ of $\mathbb{Q}$.*

*Proof.* We claim $\gamma = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ is a primitive element for the extension $K/\mathbb{Q}$ if and only if at least two of $b, c, d$ are nonzero. Recall that

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{3}, \sqrt{6}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.$$

We can assume without loss of generality that $a = 0$ since $\mathbb{Q}(\gamma) = \mathbb{Q}(\gamma - a)$. $\Rightarrow$ is clear since if only one of $b, c, d$ is nonzero, then $K = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, or $\mathbb{Q}(\sqrt{6})$.

Conversely, suppose at least two of $b, c, d$ are nonzero. If exactly two of $b, c, d$ are nonzero, then relabel $\gamma = k\alpha + j\beta$ for $\alpha, \beta \in \{\sqrt{2}, \sqrt{3}, \sqrt{6}\}$; we can moreover assume $k = 1$ by dividing by $k$. Note $K = \mathbb{Q}(\alpha, \beta)$ as above, and so by Lem. 15.8.2 $\gamma = \alpha + j\beta$ is a primitive element for $K/\mathbb{Q}$ for all but finitely many $j$. In particular,

as in the proof of Lem. 15.8.2, $\gamma$ fails to be primitive when at least two of $\pm\alpha \pm j\beta$ are equal, but this occurs if and only if $j = 0$, a contradiction.

Now suppose that all three of $b, c, d$ are nonzero. Letting

$$\gamma' = \gamma^2 - 2b^2 - 3c^2 - 6d^2 = 6cd\sqrt{2} + 4bd\sqrt{3} + 2bc\sqrt{6},$$

we have that

$$\begin{aligned} b\gamma' - 6cd\gamma &= 2d(2b^2 - 3c^2)\sqrt{3} + 2c(b^2 - 3d^2)\sqrt{6} \\ c\gamma' - 4bd\gamma &= 2d(3c^2 - 2b^2)\sqrt{2} + 2b(c^2 - 2d^2)\sqrt{6} \\ d\gamma' - 2bc\gamma &= \ \ 2c(3d^2 - b^2)\sqrt{2} + 2b(2d^2 - c^2)\sqrt{3} \end{aligned}$$

are all in $\mathbb{Q}(\gamma)$. But each of their coefficients have no nonzero solutions over $\mathbb{Q}$ by clearing denominators and checking for integer solutions, hence any three of these produces a primitive element for $K/\mathbb{Q}$ by the paragraph above, and so $\gamma$ is a primitive element for $K/\mathbb{Q}$ as well. □

## 15.9 Function Fields

**Exercise 15.9.1.** *Let $f(x)$ be a polynomial with coefficients in a field $F$. Prove that if there is a rational function $r(x)$ such that $r^2 = f$, then $r$ is a polynomial.*

*Proof.* Suppose $f \neq 0$ for otherwise $r$ is necessarily 0. Let $r = p(x)/q(x)$ for $p, q$ coprime; then $p^2 = fq^2$. Now using that $F[x]$ is a UFD (Prop. 12.2.14($c$)), since $p \nmid q$ we have $p^2 \mid f$, and so $f = p^2 s$ for some $s \in F[x]$. But then, $fq^2 = p^2 sq^2 = p^2$, and so $sq^2 = 1$ and $s, q \in F[x]$; since the units in $F[x]$ are the constant polynomials, we have $s, q \in F$ and so $r \in F[x]$. □

## 15.10 The Fundamental Theorem of Algebra

**Exercise 15.10.1.** *Prove that $A \subset \mathbb{C}$ is algebraically closed, where $A$ is the subset of $\mathbb{C}$ consisting of the algebraic numbers.*

*Remark.* We prove that a root of a polynomial with coefficients that are algebraic over a field $F$ is also algebraic.

*Proof.* Let $f \in A[x]$ be non-constant, and let $\alpha$ be a root of $f$. It suffices to show $\alpha$ is algebraic over $F$. Suppose not, and let $a_0, \ldots, a_n$ be the coefficients of $f$. Then,

$$[F(\alpha) : F] \leq [F(\alpha, a_0, \ldots, a_n) : F] \leq n \cdot \prod_{i=0}^{n} m_i < \infty$$

by Cor. 15.3.8, where $m_i$ is the degree of $a_i$ over $F$. Thus, there exists a polynomial in $F[x]$ of degree $\leq n \cdot \prod_{i=0}^{n} m_i$ with $\alpha$ as a root. □

**Exercise 15.10.2.** *Construct an algebraically closed field that contains the prime field $\mathbb{F}_p$.*

*Remark.* We prove that *any* field $K$ is contained in an algebraically closed field $L$.

*Proof.* We first claim the monic irreducible polynomials of degree $\geq 1$ in $K[x]$ can be well-ordered. This is a consequence of the well-ordering theorem, but in the case of $\mathbb{F}_p$ (or any countable field) it is possible to well-order these polynomials without the axiom of choice since there are only countably many of them. Then, letting $(f_i)$ be a well-ordering of these polynomials, and letting $L_0 = K$ and $L_i$ be the extension of $L_{i-1}$ such that $f_i$ splits completely which exists by Prop. 15.6.3, we claim $L \coloneqq \bigcup_i L_i$ is an algebraically closed field containing $K$. It suffices to show it is algebraically closed, but this is true since if $f(x) \in L[x]$ has a root $\alpha$, then the proof of Exercise 15.10.1 shows $\alpha$ is algebraic over $K$, hence in $L$ by construction. □

## 15.M Miscellaneous Problems

**Exercise 15.M.1.** *Let $K = F(\alpha)$ be a field extension generated by a transcendental element $\alpha$, and let $\beta$ be an element of $K$ that is not in $F$. Prove that $\alpha$ is algebraic over $F(\beta)$.*

*Proof.* Suppose $\beta \in K \setminus F$; then $\beta = p(\alpha)/q(\alpha)$ for $p(x), q(x) \in F[x]$, and so $\beta q(\alpha) - p(\alpha) = 0$. Thus, $\alpha$ is a root of the polynomial $\beta q(x) - p(x) \in F(\beta)[x]$, i.e., $\alpha$ is algebraic over $F(\beta)$. □

**Exercise 15.M.2.** *Factor $x^7 + x + 1$ in $\mathbb{F}_7[x]$.*

*Proof.* First substitute $x \rightsquigarrow x + 3$, giving $x^7 + x$. Then, $x^7 + x = x(x^6 + 1)$. Now $x^6 + 1$ has solutions $x^2 = 3, 5, 6 \in \mathbb{F}_7$, hence $x^7 + x = x(x^2 + 1)(x^2 + 2)(x^2 + 4)$. Now $1, 2, 4$ are the squares in $\mathbb{F}_7$, none of which are $3, 5, 6$, hence we cannot factor further. Substituting back $x \rightsquigarrow x - 3$, since $(x - 3)^2 = x^2 + x + 2$,

$$x^7 + x + 1 = (x - 3)(x^2 + x + 3)(x^2 + x + 4)(x^2 + x + 6).$$ □

**Exercise 15.M.3.** *Let $f(x)$ be an irreducible polynomial of degree 6 over a field $F$, and let $K$ be a quadratic extension of $F$. What can be said about the degrees of the irreducible factors of $f$ in $K[x]$?*

*Proof.* $K = F(\alpha)$, where $\alpha$ is the root of some irreducible quadratic polynomial $g \in F[x]$. Let $\beta$ be a root of $f$; then, $2 = [K : F]$ and $6 = [F(\beta) : F]$ divide $[K(\beta) : F] \leq 12$ by Cor. 15.3.8, and so $[K(\beta) : F] \in \{6, 12\}$. In either case, 3 divides $[K(\beta) : K]$, and so the minimal polynomial for $\beta$ over $K$ is of degree 3 or 6. In the former case, $f$ splits into a product of polynomials of degree 3 over $K$. In the latter, $f$ remains irreducible over $K$. These are the only possibilities for the irreducible factors of $f$ in $K$, for the only possibility is that the factors of degree 3 factor further to include linear factors, which is impossible since $\beta$ is of degree 6 over $F$. □

**Exercise 15.M.4.**

(*a*) *Let $p$ be an odd prime. Prove that exactly half of the elements of $\mathbb{F}_p^\times$ are squares and that if $\alpha$ and $\beta$ are nonsquares, then $\alpha\beta$ is a square.*
(*b*) *Prove the same assertion for any finite field of odd order.*
(*c*) *Prove that in a finite field of even order, every element is a square.*
(*d*) *Prove that the irreducible polynomial for $\gamma = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is reducible modulo $p$ for every prime $p$.*

*Remark.* (*b*) implies (*a*) and Lemma 15.7.10a implies (*c*), so it suffices to show (*b*) and (*d*).

*Proof of (b).* Let $F$ be our finite field of odd order, and consider the group homomorphism $\varphi\colon F^\times \to F^\times$ defined by $\alpha \rightsquigarrow \alpha^2$. If $\alpha \in \ker\varphi$ then $\alpha^2 = 1$, hence $(x-\alpha) \mid x^2-1$ in $F[x]$. Since $F[x]$ is a UFD (Prop. 12.2.14(*c*)), this implies $\alpha = \pm 1$. Thus $|\ker\varphi| = 2$ since $\operatorname{char} F \neq 2$ implies $1 \neq -1$, and so the set of squares $\operatorname{im}\varphi$ in $F^\times$ has order $\frac{1}{2}|F^\times|$ by the counting formula (Cor. 2.8.13).

Now let $\beta$ be a nonsquare. Consider the map $\mu\colon F^\times \to F^\times$ of sets defined by $\alpha \rightsquigarrow \alpha\beta$. This is a bijection, and so to show $\mu$ sends non-squares to squares, it suffices to show $\mu$ sends squares to non-squares. But this is true since if $\alpha$ is a square and $\alpha\beta$ is also a square, then $\alpha^{-1}$ is also a square, hence $\beta$ is also, a contradiction. □

*Proof of (d).* First, $f \coloneqq x^4 - 10x^2 + 1$ is the irreducible polynomial for $\gamma$ since $f(\gamma) = 0$ and $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$ by Exercise 11.1.3, and so $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$. In this field, we have the factorization

$$f = (x - (\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))(x - (-\sqrt{2} + \sqrt{3}))(x - (-\sqrt{2} - \sqrt{3})).$$

If $f$ reduces over $\mathbb{F}_p$, then it must reduce to quadratic factors since $\gamma \notin \mathbb{F}_p$; thus, $f$ can factor in one of the three following ways by pairing up the factors above:

$$(x^2 - 1 - 2\sqrt{2})(x^2 - 1 + 2\sqrt{2}), \quad (x^2 + 1 - 2\sqrt{3})(x^2 + 1 + 2\sqrt{3}),$$
$$(x^2 - 5 - 2\sqrt{6})(x^2 - 5 + 2\sqrt{6}).$$

The first factorization can occur if 2 is a square mod $p$, the second can occur if 3 is a square mod $p$, and the last can occur if 6 is a square mod $p$. By $(a), (c)$, at least one of $2, 3, 6$ is a square in $\mathbb{F}_p$, so at least one of these factorizations is possible and $f$ is reducible mod $p$ for all $p$. □

**Exercise 15.M.6.**

(a) *Prove that a rational function $f(t)$ that generates the field $\mathbb{C}(t)$ of all rational functions defines a bijective map $T' \to T'$.*

(b) *Prove a rational function $f(x)$ generates the field of rational functions $\mathbb{C}(x)$ if and only if it is of the form $(ax+b)/(cx+d)$, with $ad - bc \neq 0$.*

(c) *Identify the group of automorphisms of $\mathbb{C}(x)$ that are the identity on $\mathbb{C}$.*

*Proof of* $(a)$. Let $f(t) \in F = \mathbb{C}(t)$, and $f = p/q$ for some coprime $p, q \in \mathbb{C}[t]$. $\mathbb{C}[t](f)$ is then isomorphic to $F$, which is isomorphic to $F[x]/(p - qx)$; note this is still isomorphic to $F$. Likewise, consider $F[y]/(y)$; this is also isomorphic to $F$. By Prop. 15.9.5, we have isomorphic field extensions, hence the Riemann surfaces $\{p - qx = 0\}$ and $\{y = 0\}$ are isomorphic branched coverings of $T'$. Since $\{y = 0\}$ is the complex $t$-plane $T'$, the isomorphism of coverings is an isomorphism $T' \to T'$. □

*Proof of* $(b)$. Any function $(ax + b)/(cx + d)$ with $ad - bc \neq 0$ generates $\mathbb{C}(x)$ by Exercise 12.2.5, since any element in $\mathbb{C}(x)$ can be expressed as a $\mathbb{C}$-linear combination of elements $1/(cx + d)^i$, and then by using the Euclidean algorithm (p. 45) to get

$$\frac{ax+b}{cx+d} = \frac{q(cx+d)+r}{cx+d} = q + \frac{r}{cx+d}, \quad q, r \in \mathbb{C}$$

which implies $1/(cx + d)^i$ for any $i$ can be expressed as a $\mathbb{C}$-linear combination of $(ax + b)^i/(cx + d)^i$. Conversely, suppose a rational function $f(x)$ generates $\mathbb{C}(x)$. By $(a)$, it induces an automorphism of the Riemann surface $T'$; it suffices to show that the automorphisms of $T'$ are of the stated form. Suppose $f = p/q$ defines an automorphism of $T'$; then, if either $p, q$ had degree larger than 1, the induced morphism would not be bijective since then $p$ has two zeros; likewise, if $q$ had degree larger than 1, considering $1/f$ gives us the same argument. Moreover, one of $p, q$ must be non-constant also to induce a bijection. $ad - bc \neq 0$ corresponds to having $p, q$ coprime, which was necessary in $(a)$. □

*Solution for* $(c)$. By $(a), (b)$, $\mathrm{Aut}(\mathbb{C}(x))$ consists of maps $x \rightsquigarrow (ax + b)/(cx + d)$ for $ad - bc \neq 0$, which is a group under composition. We claim there is a surjective homomorphism $\varphi\colon GL_2(\mathbb{C}) \to \mathrm{Aut}(\mathbb{C}(x))$ defined by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \rightsquigarrow (ax+b)/(cx+d)$. This map clearly maps $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \rightsquigarrow x$, is surjective, and is a homomorphism since

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} aa' + b'c & a'b + b'd \\ ac' + cd' & bc' + dd' \end{pmatrix},$$

and both sides get mapped to

$$\left(\frac{a'x+b'}{c'x+d'}\right)\circ\left(\frac{ax+b}{cx+d}\right)=\frac{a'(ax+b)+b'(cx+d)}{c'(ax+b)+d'(cx+d)}=\frac{(aa'+b'c)x+(a'b+b'd)}{(ac'+cd')x+(bc'+dd')}.$$

It remains to find the kernel of $\varphi$. $(ax+b)/(cx+d)=x\in\mathbb{C}(x)$ if and only if $ax+b=x(cx+d)$ if and only if $c=b=0$ and $a=d$. Hence $\ker\varphi=\mathbb{C}\cdot\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, and so by the first isomorphism theorem (Thm. 11.4.2(*b*)), $\mathrm{Aut}(\mathbb{C}(x))\approx GL_2(\mathbb{C})/\ker\varphi =: PGL_2(\mathbb{C})$, the projective general linear group of order 2. □

**Exercise 15.M.7.** *Prove that the homomorphism $SL_2(\mathbb{Z})\to SL_2(\mathbb{F}_p)$ obtained by reducing the matrix entries modulo $p$ is surjective.*

*Proof.* Let $\pi\colon\mathbb{Z}\to\mathbb{F}_p$ be the quotient map reducing mod $p$. We first show that if $u,v\in\mathbb{F}_p$ are not both zero, then there exist $c,d\in\mathbb{Z}$ such that $\pi(c)=u$, $\pi(d)=v$, and $\gcd(c,d)=1$. So suppose $v\neq 0$, and let $0\leq\tilde{u},\tilde{v}<p$ be lifts of $u,v$ in $\mathbb{Z}$. Now since $p\nmid\tilde{v}$, there exist $x,y\in\mathbb{Z}$ such that $x\tilde{v}+yp=1$ since $(p)$ is maximal in $\mathbb{Z}$, and so let $c=x\tilde{u}\tilde{v}+yp$ and $d=\tilde{v}$. Then, $\pi(d)=v$, $\pi(c)=u$ since $x\tilde{v}\equiv 1 \bmod p$, and $\gcd(c,d)=1$ since $1=c+xd(1-\tilde{u})$. If $v=0$, then necessarily $u\neq 0$, and switching the roles of $u,v$ gives the desired result.

Now suppose we have $\left(\begin{smallmatrix}s&t\\u&v\end{smallmatrix}\right)\in SL_2(\mathbb{F}_p)$; let $0\leq\tilde{s},\tilde{t}<p$ be lifts of $s,t$ in $\mathbb{Z}$. Then, letting $c,d$ as constructed above, we have $\tilde{s}d-\tilde{t}c=1+Np$ for some $N\in\mathbb{Z}$. So, letting $a=\tilde{s}+mp$ and $b=\tilde{t}+np$ where $m,n\in\mathbb{Z}$ such that $N=cn-dm$, which is possible since $\gcd(c,d)=1$,

$$\begin{aligned}ad-bc&=(\tilde{s}+mp)d-(\tilde{t}+np)c\\&=\tilde{s}d-\tilde{t}c+(dm-cn)p=1+(N+dm-cn)p=1,\end{aligned}$$

hence $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in SL_2(\mathbb{Z})$ maps to $\left(\begin{smallmatrix}s&t\\u&v\end{smallmatrix}\right)\in SL_2(\mathbb{F}_p)$. □

# 16 Galois Theory

## 16.1 Symmetric Functions

**Exercise 16.1.1.** *Determine the orbit of the polynomial below. If the polynomial is symmetric, write it in terms of the elementary symmetric functions.*

(*a*) $u_1^2u_2+u_2^2u_3+u_3^2u_1\quad(n=3)$,
(*b*) $(u_1+u_2)(u_2+u_3)(u_1+u_3)\quad(n=3)$,
(*c*) $(u_1-u_2)(u_2-u_3)(u_1-u_3)\quad(n=3)$,

(*d*) $u_1^3u_2 + u_2^3u_3 + u_3^3u_1 - u_1u_2^3 - u_2u_3^3 - u_3u_1^3 \quad (n = 3)$,
(*e*) $u_1^3 + u_2^3 + \cdots + u_n^3$.

*Solution for* (*a*). The orbit consists of $u_1^2u_2 + u_2^2u_3 + u_3^2u_1$ and $u_3^2u_2 + u_2^2u_1 + u_1^2u_3$, corresponding to odd and even permutations respectively in $S_3$. □

*Solution for* (*b*). The orbit consists of only $(u_1 + u_2)(u_2 + u_3)(u_1 + u_3)$, i.e., this polynomial is symmetric. Since this polynomial is homogeneous of degree 3, write

$$(u_1 + u_2)(u_2 + u_3)(u_1 + u_3) = c_1s_1^3 + c_2s_1s_2 + c_3s_3.$$

Substituting $(1, 0, 0)$, we have $c_1 = 0$. Substituting $(1, 1, 0)$, we have $2 = 2c_2$ hence $c_2 = 1$. Lastly, substituting $(1, 1, 1)$, we have $8 = 9 + c_3$ hence $c_3 = -1$. Thus,

$$(u_1 + u_2)(u_2 + u_3)(u_1 + u_3) = s_1s_2 - s_3.$$ □

*Solution for* (*c*). The orbit consists of $(u_1-u_2)(u_2-u_3)(u_1-u_3)$ and $-(u_1-u_2)(u_2-u_3)(u_1-u_3)$, corresponding to odd and even permutations respectively in $S_3$. □

*Solution for* (*d*). The orbit consists of $u_1^3u_2 + u_2^3u_3 + u_3^3u_1 - u_1u_2^3 - u_2u_3^3 - u_3u_1^3$ and $u_3^3u_2+u_2^3u_1+u_1^3u_3-u_3u_2^3-u_2u_1^3-u_1u_3^3$, corresponding to odd and even permutations respectively in $S_3$. □

*Solution for* (*e*). The orbit consists of only $u_1^3 + u_2^3 + \cdots + u_n^3$, i.e., this polynomial is symmetric. Since this polynomial is homogeneous of degree 3, write

$$u_1^3 + u_2^3 + \cdots + u_n^3 = c_1s_1^3 + c_2s_1s_2 + c_3s_3.$$

Substituting $(1, 0, \ldots, 0)$, we have $1 = c_1$. Substituting $(1, 1, 0, \ldots, 0)$, we have $2 = 8+2c_2$ hence $c_2 = -3$. Lastly, substituting $(1, 1, 1, 0 \ldots, 0)$, we have $3 = 27-27+c_3$, hence $c_3 = 3$. Thus,

$$u_1^3 + u_2^3 + \cdots + u_n^3 = s_1^3 - 3s_1s_2 + 3s_3.$$ □

**Exercise 16.1.3.** *Let* $w_k = u_1^k + \cdots + u_n^k$.
(*a*) *Prove* Newton's identities: $w_k - s_1w_{k-1} + \cdots \pm s_{k-1}w_1 \mp ks_k = 0$.
(*b*) *Do* $w_1, \ldots, w_n$ *generate the ring of symmetric functions?*

*Proof of* (*a*). For $1 < i \leq k$, let $r_i$ be the sum of all distinct monomials of degree $k$ where each monomial is the product of one variable raised to the power $i$ and $k - i$ distinct other variables; note $r_k = w_k$. We claim $s_{k-i}w_i = r_i + r_{i+1}$ for $1 < i < k$. This is true since each product of terms with distinct variables on the left contributes

to $r_i$, while each product which has the term from $w_i$ occurring in the term from $s_{k-i}$ contributes to $r_{i+1}$, and since all terms on the right are obtained exactly once in this way. For $i = k$ we recall $s_0 = 1$, hence $s_0 w_k = w_k = r_k$. Finally, for $i = 1$ we have $s_{k-1} w_1 = k s_k + r_2$, since the terms contributing to $r_2$ arise in the same way as before, while the remaining terms produce $k$ times each monomial in $s_k$. The desired identity is formed by taking the alternating sum of these equations. □

**Claim** $(b)$**.** *$w_1, \ldots, w_n$ generates the ring of symmetric functions if and only if $m \in R^\times$ for all $1 \leq m \leq n$.*

*Proof of Claim $(b)$.* $\Leftarrow$. By Thm. 16.1.6, it suffices to show $s_k \in R[w_1, \ldots, w_n]$ for all $k$; we proceed by induction. If $k = 1$ then we are done, for $s_1 = w_1$. Then, if $s_j \in R[w_1, \ldots, w_n]$ for all $j < k$, by $(a)$ we have

$$s_k = \frac{1}{\pm k}(w_k - s_1 w_{k-1} + \cdots \pm s_{k-1} w_1) \in R[w_1, \ldots, w_n].$$

$\Rightarrow$. We show the contrapositive. Suppose $m \notin R^\times$ for some $0 < m \leq n$; we claim $s_m \notin R[w_1, \ldots, w_n]$. Suppose not; then, since $s_m$ is homogeneous of degree $m$, write

$$s_m = \sum_{\substack{I \subset \{1,\ldots,n\} \\ \sum_{i \in I} i = m}} r_I \prod_{i \in I} w_i, \quad r_I \in R.$$

Then, substituting $u_1 = \cdots = u_m = 1$, $u_{m+1} = \cdots = u_n = 0$, we get $w_i = m$ for all $i$, while $s_m = 1$. But this is a contradiction, for the right side is in the ideal $mR$ while the left side $= 1 \notin mR$. □

## 16.2 The Discriminant

**Exercise 16.2.2.**

$(a)$ *Prove that the discriminant of a real cubic is non-negative if and only if the cubic has three real roots.*

$(b)$ *Suppose that a real quartic polynomial has positive discriminant. What can you say about the number of real roots?*

*Proof of $(a)$.* Recall that the discriminant $D$ is the product of squares of the differences of roots. So, if $f$ has 3 roots in $\mathbb{R}$, then the discriminant is trivially non-negative. Conversely, if $f$ does not have 3 roots in $\mathbb{R}$, we know it must have one root $a \in \mathbb{R}$, and the other two roots must be a conjugate pair $z, \overline{z}$ since otherwise the constant term in $f$ would not be real. Then, we have

$$D = (a - z)^2 (a - \overline{z})^2 (z - \overline{z})^2 = (a - z)^2 \overline{(a - z)}^2 (z - \overline{z})^2.$$

Now $(a-z)\overline{(a-z)} > 0$, and so it suffices to show $(z-\overline{z})^2 < 0$. But this is true since $z - \overline{z} = 2\operatorname{Im} z$. □

*Solution for* (*b*). We claim that a real quartic polynomial with positive discriminant can have 0 or 4 real roots; note in particular this implies all roots are distinct. The discriminant is given by

$$D = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_1-\alpha_4)^2(\alpha_2-\alpha_3)^2(\alpha_2-\alpha_4)^2(\alpha_3-\alpha_4)^2,$$

where $\alpha_i$ are our roots; recall that complex roots must come in conjugate pairs, and so we can have 0, 2, or 4 real roots in general. If all the roots are real $D$ is clearly non-negative. If none of the roots are real and $\alpha_2 = \overline{\alpha_1}$, $\alpha_4 = \overline{\alpha_3}$, we get

$$\begin{aligned} D &= (\alpha_1-\overline{\alpha_1})^2(\alpha_1-\alpha_3)^2(\alpha_1-\overline{\alpha_3})^2(\overline{\alpha_1}-\alpha_3)^2(\overline{\alpha_1}-\overline{\alpha_3})^2(\alpha_3-\overline{\alpha_3})^2 \\ &= (2\operatorname{Im}\alpha_1)^2(2\operatorname{Im}\alpha_3)^2(\alpha_1-\alpha_3)^2\overline{(\alpha_1-\alpha_3)}^2(\alpha_1-\overline{\alpha_3})^2\overline{(\alpha_1-\overline{\alpha_3})}^2, \end{aligned}$$

which is positive since each consecutive pair of factors multiply to be positive. However, 2 real roots is impossible since if $\alpha_2 = \overline{\alpha_1}$ and $\alpha_3, \alpha_4$ are real,

$$\begin{aligned} D &= (2\operatorname{Im}\alpha_1)^2(\alpha_1-\alpha_3)^2(\alpha_1-\alpha_4)^2(\overline{\alpha_1}-\alpha_3)^2(\overline{\alpha_1}-\alpha_4)^2(\alpha_3-\alpha_4)^2 \\ &= (2\operatorname{Im}\alpha_1)^2(\alpha_1-\alpha_3)^2\overline{(\alpha_1-\alpha_3)}^2(\alpha_1-\alpha_4)^2\overline{(\alpha_1-\alpha_4)}^2(\alpha_3-\alpha_4)^2, \end{aligned}$$

which is negative since the first factor is negative and the rest of the product is positive. □

**Exercise 16.2.4.** *Use undetermined coefficients to determine the discriminant of the polynomial*
(*a*) $x^3+px+q$, (*b*) $x^4+px+q$, (*c*) $x^5+px+q$.

**Lemma 16.2.4a.** *The discriminant $D_n$ of $x^n+px+q$ for $n \geq 2$ is given by*

$$(-1)^{\frac{(n-1)(n-2)}{2}}(n-1)^{n-1}p^n + (-1)^{\frac{n(n-1)}{2}}n^n q^{n-1}.$$

*Proof of Lemma* 16.2.4*a*. Let $D_n(p,q)$ be the determinant of $x^n+px+q$. If $u_1,\ldots,u_n$ are the roots of $x^n+px+q$, by the first equation in §16.2 we have $s_n(u_1,\ldots,u_n) = (-1)^n q$, $s_{n-1}(u_1,\ldots,u_n) = (-1)^{n-1}p$, and $s_k(u_1,\ldots,u_n) = 0$ for all $0 < k < n-1$. Note the discriminant is a homogeneous symmetric polynomial of degree $n(n-1)$; we claim the only monomials in the $s_i$ appearing in $D_n(p,q)$ are $p^n, q^{n-1}$. For, by the above $s_{n-1}, s_n$ are the only nonzero elementary symmetric polynomials that would appear in $D_n(p,q)$, and moreover if $p^k q^j$ had degree $n(n-1)$, then the equation

$k(n-1)+jn = n(n-1)$ must hold, for which $k=0, j=n-1$ and $k=n, j=0$ are the only non-negative solutions. Thus, we have $D_n(p,q) = r(n)p^n + s(n)q^{n-1}$.

Now consider the discriminant $D_n(p,0)$ for $x^n+px$; since this has the same roots as $x^{n-1}+p$ in addition to the root $u_n = 0$, we have

$$D_n(p,0) = D_{n-1}(0,p)\prod_{i=1}^{n-1} u_i^2 = D_{n-1}(0,p)p^2$$

and so $r(n)p^n = s(n-1)p^n$, i.e., $r(n) = s(n-1)$, and $D_n(p,q) = s(n-1)p^n + s(n)q^{n-1}$.

It remains to find $s(n)$. Calculating the discriminant $D_n(0,-1)$ for $f \coloneqq x^n - 1$,

$$D_n(0,-1) = (-1)^{n-1}g(n) = (-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}\prod_{i\neq j}(\xi_i - \xi_j)$$

where $\xi_i$ are the roots of $x^n-1$. Then, we have the equation $x^n - 1 = \prod_i (x-\xi_i)$, and so deriving both sides and substituting in $x = \xi_i$, we get $n\xi_i^{n-1} = \prod_{i\neq j}(\xi_i - \xi_j)$, and so $D_n(0,-1) = (-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^n n\xi_i^{n-1}$. Since $\xi_i$ satisfies $f$, $\xi_i^{n-1} = \xi_i^{-1}$, and so

$$D_n(0,-1) = (-1)^{\frac{n(n-1)}{2}} n^n \prod_{i=1}^{n}\xi_i^{-1} = (-1)^{\frac{n(n-1)}{2}}(-1)^{n-1}n^n,$$

hence $s(n) = (-1)^{\frac{n(n-1)}{2}}n^n$, and finally

$$(-1)^{\frac{(n-1)(n-2)}{2}}(n-1)^{n-1}p^n + (-1)^{\frac{n(n-1)}{2}}n^n q^{n-1}. \qquad \square$$

*Solution for (a).* $D_3 = -4p^3 - 27q^2$ by Lemma 16.2.4a. $\square$

*Solution for (b).* $D_4 = -27p^4 + 256q^3$ by Lemma 16.2.4a. $\square$

*Solution for (c).* $D_5 = 256p^5 + 3125q^4$ by Lemma 16.2.4a. $\square$

**Exercise 16.2.7.** *There are $n$ variables. Let $m = u_1u_2^2u_3^3\cdots u_{n-1}^{n-1}$ and let $p(u) = \sum_{\sigma\in A_n}\sigma(m)$. The $S_n$-orbit of $p(u)$ contains two elements, $p$ and another polynomial $q$. Prove that $(p-q)^2 = D(u)$.*

*Proof.* Let $R[u_1,\ldots,u_n]$ be our polynomial ring, and let $\delta(u) = \prod_{i<j}(u_i - u_j)$. We first claim $u_i - u_j \mid p-q$ for all $i<j$. This is equivalent to showing $p-q=0$ if $u_i - u_j = 0$.

So suppose $u_i = u_j$ for $i < j$, and let $\tau = (ij) \in S_n$. Then, $p(u) = p(\tau(u))$ and $q(u) = q(\tau(u))$, and we have

$$p(\tau(u)) = \sum_{\sigma \in A_n} \sigma(\tau(m)) = \sum_{\sigma' \in A_n \cdot \tau} \sigma'(m) = q(u).$$

Similarly, $q(\tau(u)) = p(u)$, since $A_n$ has exactly two cosets in $S_n$. Thus, $p(u) - q(u) = q(u) - p(u)$, and so $p(u) - q(u) = 0$.

Now since $\delta(u)$ is homogeneous of degree $n(n-1)/2$, as are $p, q$, $u_i - u_j \mid p - q$ for all $i < j$ implies $p - q = a \prod_{i<j}(u_i - u_j)$ for some $a \in R$. But $a = \pm 1$ since in the equation $p - q = \prod_{\sigma \in S_n} \operatorname{sgn}(\sigma)\sigma(m)$, the coefficient on $m$ is 1, while in the expression $\delta(u) = \prod_{i<j}(u_i - u_j)$, the coefficient on $m$ is $\pm 1$. Thus, $(p-q)^2 = \delta(u)^2 = D(u)$. □

## 16.3 Splitting Fields

**Exercise 16.3.1.** *Let $f$ be a polynomial of degree $n$ with coefficients in $F$ and let $K$ be a splitting field for $f$ over $F$. Prove that $[K : F]$ divides $n!$.*

*Proof.* We use induction on the degree of $f$. The claim is trivial if $n = 1$, so suppose $n > 1$. Suppose $f$ is reducible, and let $g$ be an irreducible factor of $f$ of degree $m$. Then, we can choose a subfield $F_1 \subset K$ such that $g$ splits completely, hence $[F_1 : F] \mid m!$ by inductive hypothesis. Similarly, $[K : F_1] \mid (n-m)!$ by inductive hypothesis since $K$ is a splitting field for $f/g$ over $F_1$. Hence by the multiplicative property of the degree (Thm. 15.3.5), $[K : F] \mid m!(n-m)! \mid n!$.

Now suppose $f$ is irreducible. Then, $F_1 \coloneqq F[x]/(f)$ is a field extension of degree $n$ such that $f$ has a root $\alpha$. Thus, $[K : F_1] \mid (n-1)!$ by inductive hypothesis since $K$ is a splitting field for $f/(x-\alpha)$ over $F_1$, and so $[K : F] \mid n(n-1)! = n!$ as above. □

## 16.4 Isomorphisms of Field Extensions

**Exercise 16.4.1.**

(a) *Determine all automorphisms of the field $\mathbb{Q}(\sqrt[3]{2})$, and of the field $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = e^{2\pi i/3}$.*

(b) *Let $K$ be the splitting field over $\mathbb{Q}$ of $f(x) = (x^2 - 2x - 1)(x^2 - 2x - 7)$. Determine all automorphisms of $K$.*

*Solution for (a).* We first claim that any automorphism $\varphi$ of either field must leave $\mathbb{Q}$ fixed. Any integer is held fixed by Exercise 2.6.2 and since $\varphi(1) = 1$. Any rational $p/q$ must then be fixed since multiplicative inverses are preserved through $\varphi$.

Now let $\varphi \in \operatorname{Aut}\mathbb{Q}(\sqrt[3]{2})$. $\varphi$ is then determined by $\varphi(\sqrt[3]{2})$, and it is necessary that $\varphi(\sqrt[3]{2})^3 = 2$. Thus, $\varphi(\sqrt[3]{2}) = \omega^j\sqrt[3]{2}$ for some $j \in \{0,1,2\}$; however, $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, and $\omega \in \mathbb{C} \setminus \mathbb{R}$, hence $j = 0$ and $\varphi = \mathrm{id}$.

Now let $\varphi \in \operatorname{Aut}\mathbb{Q}(\sqrt[3]{2}, \omega)$. $\varphi$ is then determined by $\varphi(\sqrt[3]{2})$ and $\varphi(\omega)$, and it is necessary that $\varphi(\sqrt[3]{2})^3 = 2$ and $\varphi(\omega)^3 = 1$. Thus, $\varphi(\sqrt[3]{2}) = \omega^j\sqrt[3]{2}$ and $\varphi(\omega) = \omega^k$ for some $j, k \in \{0,1,2\}$. $k \neq 0$ for otherwise $\varphi$ is not surjective. Any of the remaining choices gives an automorphism, hence $\mathbb{Q}(\sqrt[3]{2}, \omega)$ has six automorphisms. □

*Solution for (b).* The roots of $f$ are $1 \pm \sqrt{2}, 1 \pm 2\sqrt{2}$ by the quadratic formula, hence $K = \mathbb{Q}(\sqrt{2})$, which only has the trivial automorphism and the automorphism sending $\sqrt{2} \rightsquigarrow -\sqrt{2}$ as in Ex. 16.4.1. □

## 16.5 Fixed Fields

**Exercise 16.5.2.** *Show that the automorphisms* $\sigma(t) = \dfrac{t+i}{t-i}$ *and* $\tau(t) = \dfrac{it-i}{t+1}$ *of* $\mathbb{C}(t)$ *generate a group isomorphic to the alternating group* $A_4$*, and determine the fixed field of this group.*

*Solution.* We first calculate products of $\sigma, \tau$:

$$\begin{aligned}
&\mathrm{id} = t, && \sigma\tau = -t, && \sigma\tau^2\sigma = \frac{1}{t}, && \tau\sigma = -\frac{1}{t},\\
&\sigma = \frac{t+i}{t-i}, && \sigma^2\tau = \frac{t-i}{t+i}, && \tau\sigma^2 = \frac{it+1}{-it+1}, && \tau^2 = \frac{-it+1}{it+1},\\
&\sigma^2 = \frac{t+1}{-it+i}, && \tau = \frac{it-i}{t+1}, && \tau^2\sigma = \frac{t+1}{it-i}, && \sigma\tau^2 = \frac{-it+1}{t+1},
\end{aligned} \tag{7}$$

where we have used the relations $\sigma^3 = \tau^3 = \sigma\tau\sigma\tau = \mathrm{id}$, hence there are 12 elements in this group $G$. Now consider the four pairs of 3 points defining circles in $\mathbb{CP}^1$:

$$\begin{aligned}
&\{\{0,-i,1\},\{-1,i,\infty\}\}, \quad \{\{0,-1,i\},\{-i,1,\infty\}\},\\
&\{\{0,i,1\},\{-1,-i,\infty\}\}, \quad \{\{0,-1,-i\},\{1,i,\infty\}\}.
\end{aligned}$$

Labeling these $1,2,3,4$ respectively, we have that $\sigma$ permutes these pairs as (123) and $\tau$ does as (234), hence $G$ is isomorphic to a subgroup of $S_4$. By the above, this has order 12; by Exercise 6.7.11 we then know that $G \approx A_4$.

To find the fixed field, the first row in (7) gives a subgroup of $A_4$ isomorphic to the Klein 4-group $C_2 \times C_2$. We then note by Thm. 16.5.2(*a*) that the irreducible polynomial for $t$ over the fixed field is the polynomial whose roots form its orbit:

$$(x-t)(x+t)(x-1/t)(x+1/t) = (x^2-t^2)(x^2-1/t^2) = x^4 - (t^2+t^{-2})x^2 + 1.$$

Thus letting $u = t^2 + t^{-2}$, we have that $[\mathbb{C}(t) : \mathbb{C}(u)] \leq 4$. Note $u$ is fixed by $C_2 \times C_2$, hence $\mathbb{C}(u) \subset \mathbb{C}(t)^{C_2 \times C_2}$, and that since by the fixed field theorem (Thm. 16.5.4), $[\mathbb{C}(t) : \mathbb{C}(t)^{C_2 \times C_2}] = 4$, it follows that $\mathbb{C}(u) = \mathbb{C}(t)^{C_2 \times C_2}$.

We now want to find the subfield of $\mathbb{C}(u)$ that is fixed by all of $A_4$; by (7) since $\sigma$ and $C_2 \times C_2$ generate $A_4$, it suffices to find the subfield of $\mathbb{C}(u)$ fixed by $\sigma$. We have

$$\sigma(u) = \sigma(t)^2 + \frac{1}{\sigma(t)^2} = \left(\frac{t+i}{t-i}\right)^2 + \left(\frac{t-i}{t+i}\right)^2 = \frac{2(t^4 - 6t^2 + 1)}{(t^2+1)^2} = \frac{2(u-6)}{u+2}$$

$$\sigma^2(u) = \sigma^2(t)^2 + \frac{1}{\sigma^2(t)^2} = \left(i\frac{t+1}{t-1}\right)^2 + \left(i\frac{t-1}{t+1}\right)^2 = \frac{-2(t^4 + 6t^2 + 1)}{(t^2-1)^2} = \frac{-2(u+6)}{u-2}$$

hence

$$(x-u)(x-\sigma(u))(x-\sigma^2(u)) = x^3 - \frac{u(u^2-36)}{u^2-4}x^2 - 36x + \frac{4u(u^2-36)}{u^2-4}.$$

Now letting $v = \frac{u(u^2-36)}{u^2-4}$, $v$ is fixed by $\sigma$ and $[\mathbb{C}(u) : \mathbb{C}(v)] \leq 3$, hence by the fixed field theorem (Thm. 16.5.4) $\mathbb{C}(v) = \mathbb{C}(u)^{\langle\sigma\rangle} = \mathbb{C}(t)^{A_4}$. Explicitly,

$$v = \frac{(t^4+1)(t^8 - 34t^4 + 1)}{t^2(t^4-1)^2}.$$ □

## 16.6 Galois Extensions

**Exercise 16.6.1.** *Let $\alpha$ be a complex root of $x^3 + x + 1$ over $\mathbb{Q}$, and let $K$ be a splitting field of this polynomial over $\mathbb{Q}$. Is $\sqrt{-31}$ in the field $\mathbb{Q}(\alpha)$? Is it in $K$?*

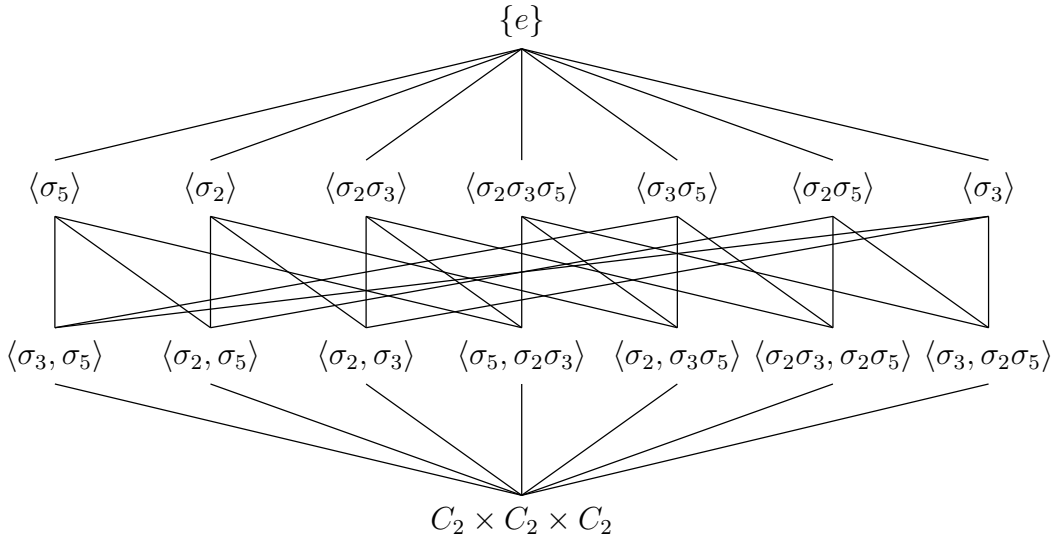
*Solution.* By the multiplicative property of degree (Thm. 15.3.5), $\sqrt{-31} \notin \mathbb{Q}(\alpha)$ since $\alpha$ has degree 3 while $\sqrt{-31}$ has degree 2 over $\mathbb{Q}$. However, $\sqrt{-31} \in K$ because the discriminant of $x^3 + x + 1$ is $-31$ by Exercise 16.2.4($a$), and the square root of the discriminant is a product of differences of elements in $K$. □

## 16.7 The Main Theorem

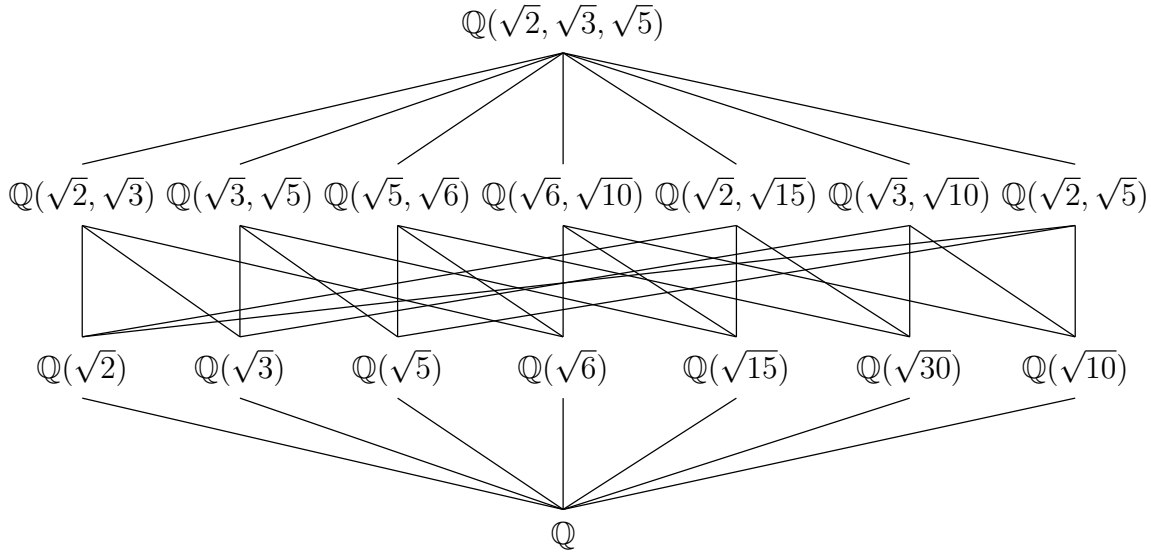
**Exercise 16.7.4.** *Let $F = \mathbb{Q}$, and let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine all intermediate fields.*

*Proof.* $K$ is the splitting field of the polynomial $(x^2-2)(x^2-3)(x^2-5)$, and so $F \subset K$ is a Galois extension of order 8 with Galois group $G = C_2 \times C_2 \times C_2 = \langle \sigma_2, \sigma_3, \sigma_5 \rangle$, where $\sigma_k$ is the field automorphism over $\mathbb{Q}$ such that $\sqrt{k} \rightsquigarrow -\sqrt{k}$.

The lattice diagram for subgroups of $C_2 \times C_2 \times C_2$ is given by




which corresponds to the lattice diagram of intermediate fields




by computing fixed fields according to Thm. 16.7.1. □

**Exercise 16.7.6.** *Let $K/F$ be a Galois extension whose Galois group is $S_3$. Is $K$ the splitting field of an irreducible cubic polynomial over $F$?*

*Solution.* We claim it is. Let $S_2 \leqslant S_3$ be the subgroup fixing 3, and consider the chain $F \subset K^{S_2} \subset K$. By Thm. 16.7.5, the first extension in this chain is not Galois since $S_2 \leqslant S_3$ is not normal, while the second extension is Galois with Galois group $S_2$. By Cor. 16.7.2($c$), $[K^{S_2} : F] = [S_3 : S_2] = 3$. Now if $\alpha \in K^{S_2} \setminus F$, let $f \in F[x]$ be its irreducible polynomial; note that $\deg f = 3$, and that $K^{S_2} = F(\alpha)$. Since $K^{S_2}/F$ is not Galois, $f$ does not split in $K^{S_2}$ by Thm. 16.6.4, but it does split in $K$ by the splitting theorem (Thm. 16.3.2). Since $[K : K^{S_2}] = 2$, there are no intermediate fields between $K^{S_2}, K$, and so $K/F$ must be the splitting field of $f$. □

**Exercise 16.7.10.** *Let $K/F$ be a Galois extension with Galois group $G$, and let $H$ be a subgroup of $G$. Prove that there exists an element $\beta \in K$ whose stabilizer is equal to $H$.*

*Proof.* Recall from p. 484 that we assume $K, F$ have characteristic zero, and that $K/F$ is a finite extension. So consider the chain of extensions $F \subset K^H \subset K$; by the primitive element theorem (Thm. 15.8.1) there exists $\beta \in K^H$ such that $K^H = F(\beta)$. We claim $G_\beta = H$. Clearly $H \subset G_\beta$, so suppose $\sigma \in G_\beta \setminus H$. Then, $H' \coloneqq \langle H, \sigma \rangle \supsetneq H$, and $K^{H'} \subset K^H$ by Cor. 16.7.2($a$). Every element in $K^H$ is fixed by $H'$, hence $K^{H'} = K^H$. But then $[K : K^H] = |H| = |H'|$ by Cor. 16.7.2($c$), contradicting that $H \subsetneq H'$. □

**Exercise 16.7.11.** *Let $\alpha = \sqrt[3]{2}$, $\beta = \sqrt{3}$, and $\gamma = \alpha + \beta$. Let $L$ be the field $\mathbb{Q}(\alpha, \beta)$, and let $K$ be the splitting field of the polynomial $(x^3 - 2)(x^2 - 3)$ over $\mathbb{Q}$.*

($a$) *Determine the irreducible polynomial $f$ for $\gamma$ over $\mathbb{Q}$, and its roots in $\mathbb{C}$.*

($b$) *Determine the Galois group of $K/\mathbb{Q}$.*

*Solution for ($a$).* First, $(\gamma - \beta)^3 = \gamma^3 - 3\beta\gamma^2 + 9\gamma - 3\beta = 2$, hence

$$\beta = \frac{\gamma^3 + 9\gamma - 2}{3\gamma^2 + 3},$$

and so $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$. Moreover, since $\alpha$ has degree 3 and $\beta$ has degree 2 over $\mathbb{Q}$, by Cor. 15.3.8 $[L : \mathbb{Q}] = 6$. Thus, the irreducible polynomial for $\gamma$ has degree 6. Now letting $f(x) = ((x - \beta)^3 - 2)((x + \beta)^3 - 2)$, $f(\gamma) = 0$ by construction, and

$$\begin{aligned} f(x) &= (x^3 + 9x - 2 - 3\beta(x^2 + 1))(x^3 + 9x - 2 + 3\beta(x^2 + 1)) \\ &= (x^3 + 9x - 2)^2 - 27(x^2 + 1)^2 = x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23. \end{aligned}$$

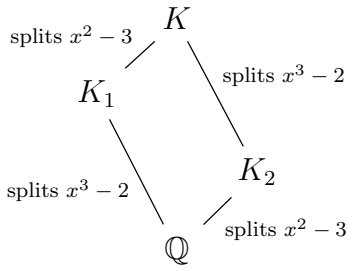
Since $\deg f(x) = 6$, it is then the irreducible polynomial for $\gamma$. Now $z \in \mathbb{C}$ is a root of $f(x)$ if and only if $z \pm \beta = \omega^j \alpha$ where $\omega = e^{2\pi i/3}$ and $j \in \{0, 1, 2\}$, hence the roots of $f(x)$ are $\pm\beta + \omega^j \alpha$. □

*Solution for* $(b)$. Denote $G = G(K/\mathbb{Q})$. $f(x)$ from $(a)$ splits completely in $K$ by the splitting theorem (Thm. 16.3.2); similarly, $(x^3-2)(x^2-3)$ splits completely in the splitting field for $f(x)$ since $\alpha, \beta$ can be obtained as linear combinations of the roots of $f(x)$. Thus, $K$ is the splitting field for $f(x)$. If $j \in \{1,2\}$,

$$\pm\beta + \omega^j\alpha = \pm\beta + \frac{-1-(-1)^j i\beta}{2}\alpha = \pm\beta - \frac{1}{2}\alpha - \frac{(-1)^j}{2}i\beta,$$

hence $K = \mathbb{Q}(\gamma, i) = \mathbb{Q}(\alpha, \beta, i)$, and so $[K:\mathbb{Q}] = [K:\mathbb{Q}(\gamma)][\mathbb{Q}(\gamma):\mathbb{Q}] = 12$ by the multiplicative property of the degree (Thm. 15.3.5).

Now let $K_1$ be the splitting field for $x^3-2$ and let $K_2$ be the splitting field for $x^2-3$. We have the lattice diagram of intermediate fields




Each field extension is Galois by Thm. 16.6.4$(c)$, and so in particular the subgroups $G_1 \coloneqq G(K/K_1)$ and $G_2 \coloneqq G(K/K_2)$ of $G$ fixing $K_1, K_2$ respectively are normal subgroups of $G$ by Thm. 16.7.5. The extension $K/K_1$ is quadratic, hence $G_1 \approx C_2$; the extension $K/K_2$ is cubic with $[K:K_2] = 6$, hence $G_2 \approx S_3$ as on p. 492.

We therefore claim $G \approx G_1 \times G_2 \approx C_2 \times S_3$. Consider the multiplication map $\mu\colon G_1 \times G_2 \to G$. We first claim $\mu$ is injective. By Thm. 16.6.6$(b)$, it suffices to show any $\sigma \in G_1 \cap G_2$ operates as the identity on $\pm\beta + \omega^j\alpha$. But $\omega^j\alpha \in K_1$ and $\pm\beta \in K_2$ by definition, hence $G_1 \cap G_2 = \{1\}$. Now since also $|G_1 \times G_2| = 12 = |G|$, $\mu$ is also surjective, and is therefore an isomorphism. $\square$

## 16.8 Cubic Equations

**Exercise 16.8.4.** *Let $K = \mathbb{Q}(\alpha)$, where $\alpha$ is a root of the polynomial $x^3 + 2x + 1$, and let $g(x) = x^3 + x + 1$. Does $g(x)$ have a root in $K$?*

*Solution.* Let $f(x) = x^3 + 2x + 1$. By the rational root test, $f(x), g(x)$ are both irreducible in $\mathbb{Q}[x]$. By (16.2.8), their discriminants are $-59, -31$ respectively, so since both are not squares, by Thm. 16.8.5 their splitting fields $L_f, L_g$ have degree 6 over $\mathbb{Q}$, with Galois group $S_3$. Now if $g(x)$ has a root in $K$, then it splits completely

in $K$ by the splitting theorem (Thm. 16.3.2), hence $L_f = L_g$ since both are of degree 6 over $\mathbb{Q}$. Since the Galois group is $S_3$, there should be one intermediate field of degree 2 over $\mathbb{Q}$, but we have two, $\mathbb{Q}(\sqrt{-59})$ and $\mathbb{Q}(\sqrt{-31})$, a contradiction. $\square$

## 16.9 Quartic Equations

**Exercise 16.9.6.** *Compute the discriminant of the quartic polynomial $x^4 + 1$, and determine its Galois group over $\mathbb{Q}$.*

*Solution.* By Exercise 16.2.4($c$), the discriminant is 256. By Prop. 16.9.5, this implies the Galois group $G$ is $A_4$ or $D_2$. Now the roots of $x^4 + 1$ are

$$\alpha_1 = \frac{1}{\sqrt{2}}(1+i),\ \alpha_2 = -\frac{1}{\sqrt{2}}(1+i), \quad \alpha_3 = \frac{1}{\sqrt{2}}(1-i), \quad \alpha_4 = -\frac{1}{\sqrt{2}}(1-i).$$

$\beta_1 = 0, \beta_2 = 2, \beta_3 = -2$ gives $g(x) = x(x-2)(x+2)$, so $G = D_2$ by Prop. 16.9.8. $\square$

**Exercise 16.9.13.** *Let $K$ be the splitting field over $\mathbb{Q}$ of the polynomial $x^4 - 2x^2 - 1$. Determine the Galois group $G$ of $K/\mathbb{Q}$, find all intermediate fields, and match them up with the subgroups of $G$.*

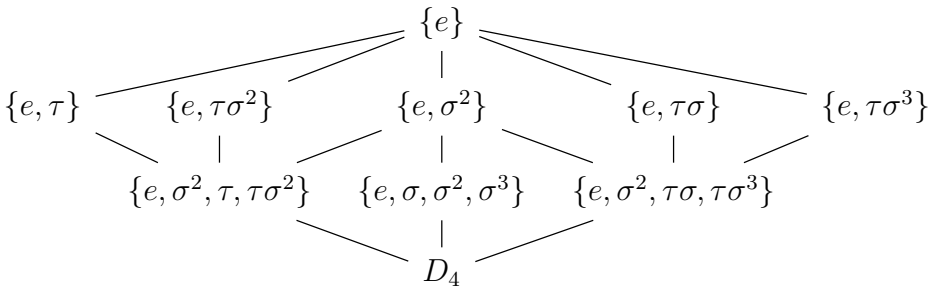
*Solution.* We find the roots of $x^4 - 2x^2 - 1$. We first apply the quadratic equation to get $x^2 = 1 \pm \sqrt{2}$; then,

$$\alpha_1 = \sqrt{1+\sqrt{2}},\ \alpha_2 = \sqrt{1-\sqrt{2}}, \quad \alpha_3 = -\alpha_1, \quad \alpha_4 = -\alpha_2.$$

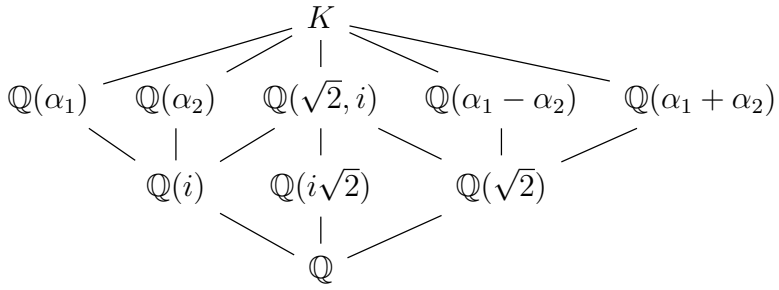
$\beta_1 = 2i, \beta_2 = -2, \beta_3 = -2i$, so $g(x) = (x+2)(x^2+4)$. As in Ex. 16.9.2(a), $G$ is a subgroup of $D_4 = \langle \sigma, \tau \rangle$ where $\sigma = (1234), \tau = (24)$. By Prop. 16.9.8, $G = D_4$ or $C_4$.

As in Ex. 16.9.2($a$), $\rho = \sigma^2 = (13)(24)$ corresponds to an automorphism $K/\mathbb{Q}$; call $N$ the normal subgroup of order 2 generated by $\rho$. Now $\alpha_1^2 = 1+\sqrt{2}$ and $\alpha_1\alpha_2 = i$ are both fixed by $\rho$, hence $\mathbb{Q}(\sqrt{2}, i) \subset K^N$. The chain of fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, i) \subset K^N \subset K$ has $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$, $[K : K^N] = 2$ by Thm. 16.5.4, and so $[K : \mathbb{Q}] = 8$, so $G = D_4$.

The lattice diagram for subgroups of $D_4$ is as given in Exercise 6.4.2:



which corresponds to the lattice diagram of intermediate fields




by computing fixed fields according to Thm. 16.7.1. □

**Exercise 16.9.14.** *Let $F = \mathbb{Q}(\omega)$, where $\omega = e^{2\pi i/3}$. Determine the Galois group over $F$ of the splitting field of (a) $\sqrt[3]{2+\sqrt{2}}$, (b) $\sqrt{2+\sqrt[3]{2}}$.*

*Remark.* We note there are analogues of results from §§12.3–12.4 for checking irreducibility of polynomials in $F[x]$: Gauss's lemma (Prop. 12.3.4($b$)) only needs $F$ to be the fraction field of a UFD, and $\mathbb{Z}[\omega]$ is a UFD by Exercise 12.2.6($a$) and Props. 12.2.7 and 12.2.14(b). Moreover, Eisensten's criterion generalizes to $\mathbb{Z}[\omega][x]$ by looking at prime elements $p \in \mathbb{Z}[\omega]$.

*Solution for ($a$).* Let $\alpha = \sqrt[3]{2+\sqrt{2}}$, with splitting field $K/F$. $\alpha$ satisfies the polynomial $f(x) = (x^3-2)^2 - 2 = x^6 - 4x^3 + 2$. The quadratic equation gives that $x^3 = 2 \pm \sqrt{2}$, hence writing $\alpha' = \sqrt[3]{2-\sqrt{2}}$, we can write the roots as

$$\alpha_1 = \alpha,\ \alpha_2 = \alpha', \quad \alpha_3 = \omega\alpha, \quad \alpha_4 = \omega\alpha', \quad \alpha_5 = \omega^2\alpha, \quad \alpha_6 = \omega^2\alpha'.$$

Thus if $\alpha_1 \rightsquigarrow \alpha_i$, then $\alpha_3 \rightsquigarrow \omega\alpha_i$, $\alpha_5 \rightsquigarrow \omega^2\alpha_i$. The permutations with this property are generated by $\sigma = (123456), \tau = (246)$ in $S_6$; these form what is called the *semidirect product* $C_6 \rtimes C_3$, and so $G(K/F) \leqslant C_6 \rtimes C_3$.

Now $f$ is irreducible over $F$ by Eisenstein's criterion using $p = 2$ which is prime by Exercise 12.5.9($b$), hence $[F(\alpha) : F] = 6$. Also, $\sqrt{2} \in F(\alpha)$, hence $\alpha'$ has degree 3 or 1 over $F(\alpha)$. Thus, $[K : F] = 6$ or 18.

We claim $[K : F] = 18$. Consider $\sigma^2 = (135)(246)$; it is in all subgroups of $C_6 \rtimes C_3$ of order 6, hence extends to an $F$-automorphism of $K$. Let $N$ be the subgroup of order 3 generated by $\sigma^2$. The fixed field $K^N$ contains $\alpha^2\alpha' = \sqrt[3]{2(2+\sqrt{2})}$; let $L$ be the field generated by this element over $F$. The chain $F \subset L \subset K^N \subset K$ has $[K : K^N] = 3$ by the fixed field theorem (Thm. 16.5.4), and $[L : F] \geq 3$, hence $[K : F] = 18$, and so $G(K/F) = C_6 \rtimes C_3$. □

*Solution for (b).* Let $\alpha = \sqrt{2+\sqrt[3]{2}}$, with splitting field $K/F$. $\alpha$ satisfies the polynomial $f(x) = (x^2-2)^3 - 2 = x^6 - 6x^4 + 12x^2 - 10$. The roots of $f(x)$ are

$$\alpha_1 = \alpha,\ \alpha_2 = \sqrt{2+\omega\sqrt[3]{2}},\ \alpha_2 = \sqrt{2+\omega^2\sqrt[3]{2}},\ \alpha_4 = -\alpha_1,\ \alpha_5 = -\alpha_2,\ \alpha_6 = -\alpha_3.$$

Thus if $\alpha_i \rightsquigarrow \alpha_j$, then $\alpha_{i+3} \rightsquigarrow \alpha_{j+3}$, where we treat subscripts mod 6. The group $G$ of permutations satisfying these is generated by the subgroup of $S_6$ isomorphic to $S_3$ permuting $\{\{1,4\},\{2,5\},\{3,6\}\}$ isomorphic to $S_3$ and $C_2 \approx \langle(14)(25)(36)\rangle \leqslant S_6$. Now $S_3 \cap C_2 = \{1\}$, and if $\sigma \in S_3, \tau \in C_2$, $\sigma\tau = \tau\sigma$, hence $S_3, C_2$ are normal in $G$, $G \approx S_3 \times C_2$ by Prop. 2.11.4($d$), and $G(K/F) \leqslant G$.

Now $f$ is irreducible over $F$ by Eisenstein's criterion, again using that 2 is prime, hence $[F(\alpha):F] = 6$. Also, $\omega^j\sqrt[3]{2} \in F(\alpha)$ for $j \in \{0,1,2\}$, hence $\alpha_2, \alpha_3$ have degree 2 or 1 over $F(\alpha)$. Thus, $[K:F] \in \{6,12,24\}$. But $|G| = 12$, hence $[K:F] = 24$ is impossible.

We claim $[K:F] = 12$. Consider $\rho = (\{1,4\}\{2,5\}\{3,6\}) \in G$; it is contained in every subgroup of $G$ of order 6, hence extends to an $F$-automorphism of $K$. Let $N$ be the subgroup of order 3 generated by $\rho$. The fixed field $K^N$ contains $\alpha_1\alpha_2\alpha_3 = \sqrt{10}$; let $L$ be the field generated by this element over $F$. The chain $F \subset L \subset K^N \subset K$ has $[K:K^N] = 3$ by the fixed field theorem (Thm. 16.5.4), and $[L:F] = 2$. But $[K^N:L] > 1$ since $\alpha_1+\alpha_2+\alpha_3 \in K^N \setminus L$, hence $[K:F] = 12$, and so $G(K/F) = S_3 \times C_2$. □

## 16.10 Roots of Unity

**Exercise 16.10.3.** *Let $\zeta = \zeta_7$. Determine the degree of the following elements over $\mathbb{Q}$.*
*(a) $\zeta + \zeta^5$, (b) $\zeta^3 + \zeta^4$, (c) $\zeta^3 + \zeta^5 + \zeta^6$.*

*Remark.* Suppose we want to find the degree of $\alpha \in \mathbb{Q}(\zeta)$. By Prop. 16.10.2, $G(\mathbb{Q}(\zeta)/\mathbb{Q}) = C_6$ consisting of $\sigma_i$ given by $\sigma_i(\zeta) = \zeta^i$ for $1 \leq i \leq 6$. If $H \leqslant C_6$ is the subgroup fixing $\alpha$, then by the main theorem (Thm. 16.7.1) $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)^H$. Thus, the multiplicative property of degree (Thm. 15.3.5) gives us $[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\zeta):\mathbb{Q}]/[\mathbb{Q}(\zeta):\mathbb{Q}(\zeta)^H] = 6/|H|$ by the fixed field theorem (Thm. 16.5.4).

*Solution for (a).* $\{\sigma_1\}$ fixes $\zeta + \zeta^5$, hence $\zeta + \zeta^5$ has degree 6. □

*Solution for (b).* $\{\sigma_1, \sigma_6\}$ fixes $\zeta^3 + \zeta^4$, hence $\zeta^3 + \zeta^4$ has degree 3. □

*Solution for (c).* $\{\sigma_1, \sigma_2, \sigma_4\}$ fixes $\zeta^3 + \zeta^5 + \zeta^6$, hence $\zeta^3 + \zeta^5 + \zeta^6$ has degree 2. □

## 16.11 Kummer Extensions

**Exercise 16.11.5.**

(*a*) *How does Cardano's formula* (16.11.5) *express the roots of the polynomials* $x^3+3x, x^3+2$ *and* $x^3-3x+2$*?*

(*b*) *What are the correct choices of roots in Cardano's formula?*

*Solution for* (*a*). For $x^3+3x$, we get $\sqrt[3]{0+\sqrt{1}}+\sqrt[3]{0-\sqrt{1}}$.

For $x^3+2$ we get $\sqrt[3]{-1+\sqrt{1}}+\sqrt[3]{-1-\sqrt{1}}$.

For $x^3-3x+2$ we get $\sqrt[3]{-1+\sqrt{0}}+\sqrt[3]{-1-\sqrt{0}}=\sqrt[3]{-1}+\sqrt[3]{-1}$. □

*Solution for* (*b*). For $x^3+3x$, the solutions are $0, \pm i\sqrt{3}$. To get 0, we choose $\sqrt{1}$ to have the same sign to be $\pm 1$ in both terms, and then choose $\sqrt[3]{\pm 1}=\pm e^{2\pi ik/3}$ and $\sqrt[3]{\mp 1}=\mp e^{2\pi ik/3}$ for $k\in\{1,2\}$. For $i\sqrt{3}$, we choose $\sqrt{1}$ to have different signs $\pm 1, \mp 1$ so that $\sqrt[3]{0+\sqrt{1}}+\sqrt[3]{0-\sqrt{1}}=2\sqrt[3]{\pm 1}=\pm 2\sqrt[3]{1}$, and then choose $\sqrt[3]{1}=e^{2\pi ik/3}$ for $k=1$ if we chose $\pm$ to be $+$, and $k=2$ if we chose $\pm$ to be $-$. For $-i\sqrt{3}$ we would switch our choice for $k$.

For $x^3+2$, we choose the same square roots, giving $\sqrt[3]{-1+\sqrt{1}}+\sqrt[3]{-1-\sqrt{1}}=\sqrt[3]{-2}$, and each choice of cube root gives us a solution.

For $x^3-3x+2$, $x^3-3x+2=(x-1)^2(x+2)$, so $1,-2$ are the solutions. $-2$ is obtained by choosing $-1$ for both. $-1$ is obtained by choosing a primitive cube root of unity $\alpha$ for one root, and $\overline{\alpha}$ for the other. □

## 16.12 Quintic Equations

**Exercise 16.12.7.** *Find a polynomial of degree* 7 *over* $\mathbb{Q}$ *whose Galois group is* $S_7$*.*

*Solution.* We first claim $S_p$ is generated by a $p$-cycle and a transposition for $p$ prime. Let $(ab\cdots cd),(ef)$ be our $p$-cycle and transposition. By renaming $e=1$, we can assume they are $(ab\cdots 1\cdots cd)=(1\cdots cdab\cdots),(1f)$. Now $(1\cdots cdab\cdots)^k=(1f\cdots)$ for some $1\le k\le p-1$ since $p$ is prime, hence we can assume our generators are $(1f\cdots),(1f)$; by renaming $f=2$ and the rest of the elements in $(1f\cdots)$ accordingly, we can assume our generators are $\alpha=(12\cdots p),\beta=(12)$. Now

$$\alpha^{-1}\beta\alpha=(1p),\ \alpha^{-1}(1p)\alpha=((p-1)p),\quad \alpha^{-1}((p-1)p)\alpha=((p-2)(p-1)),\quad \cdots$$

so we can generate all permutations of the form $((k-1)k)$. These generate $S_p$.

Now let $f(x)=(x^3-2)(x^2-4)(x^2-32)+2=x^7-36x^5-2x^4+128x^3+72x^2-254$. This is irreducible by the Eisenstein criterion; also it has 5 real roots and 2 complex roots by looking at its graph. The only permutations of its roots that fix the real

roots is conjugation, which corresponds to a transposition in $G$; moreover, $G$ operates transitively on the roots, hence contains a 7-cycle, and the Galois group is therefore $S_7$ by the above. □

## 16.M Miscellaneous Problems

**Exercise 16.M.4.**

(*a*) *The non-negative real numbers are those having a real square root. Use this fact to prove that the field* $\mathbb{R}$ *has no automorphism except the identity.*

(*b*) *Prove that* $\mathbb{C}$ *has no* continuous *automorphisms other than complex conjugation and the identity.*

*Proof of* (*a*). Any automorphism $\varphi$ is clearly the identity on the integers and rationals, since $\varphi(n) = \varphi(1+\cdots+1) = \varphi(1)+\cdots+\varphi(1) = n$, and then $q\varphi(p/q) = \varphi(p) = p$.

Let $a$ be such that $\varphi(a) = b \neq 0$. Then $b < a$ after possibly multiplying by $-1$. Subtracting a suitable rational from each, we get $b < 0 < a$. But then $a = \alpha^2$, so $\varphi(\alpha)^2 = \varphi(\alpha^2) = \varphi(a) = b$, contradicting $b < 0$. □

*Proof of* (*b*). By (*a*), any automorphism $\varphi$ is the identity on $\mathbb{Q}$. Now letting $i$ be such that $i^2 = -1$, we see $\varphi(i)^2 = -1$, but since only $\pm i$ square to get $-1$ in $\mathbb{C}$, on $\mathbb{Q}[i]$ we have that $\varphi$ is either the identity or complex conjugation.

Finally, $\mathbb{Q}[i]$ is dense in $\mathbb{C}$, hence any automorphism of $\mathbb{C}$ must also be either the identity or complex conjugation by continuity. □

**Exercise 16.M.7.** *A polynomial* $f$ *in* $F[u_1, \ldots, u_n]$ *is* $\frac{1}{2}$*-symmetric if* $f(u_{\sigma 1}, \ldots, u_{\sigma n}) = f(u_1, \ldots, u_n)$ *for every even permutation* $\sigma$*, and skew-symmetric if* $f(u_{\sigma 1}, \ldots, u_{\sigma n}) = (\operatorname{sign}\sigma) f(u_1, \ldots, u_n)$ *for every permutation* $\sigma$*.*

(*a*) *Prove that the square root of the discriminant* $\delta := \prod_{i<j}(x_i - x_j)$ *is skew-symmetric.*

(*b*) *Prove that every* $\frac{1}{2}$*-symmetric polynomial has the form* $f + g\delta$*, where* $f$*,* $g$ *are symmetric polynomials.*

*Proof of* (*a*). It suffices to show that for any permutation of two elements contributes a negative sign, for any permutation is generated by permutations of two elements, and the number of permutation of two elements needed to generate a given permutation is equal to its sign.

So suppose we are interchanging $u_i$, $u_j$; assume without loss of generality that $i < j$. Then the terms in $\delta$ involving $u_i, u_j$ have the product

$$(u_i - u_j)\prod_{k=1}^{i-1}(u_k - u_i)\prod_{k=1}^{j-1}(u_k - u_j)\prod_{k=i+1}^{j-1}(u_k - u_j)\prod_{k=i+1}^{j-1}(u_i - u_k)\prod_{k=j+1}^{n}(u_i - u_k)\prod_{k=j+1}^{n}(u_j - u_k)$$

Now interchanging $u_i$, $u_j$ causes a sign change in each factor; the sign change in $u_i - u_j$ is the only one that remains since each two adjacent factors in the rest of the product have canceling sign changes. Hence $\delta$ also changes sign when interchanging $u_i$ and $u_j$, i.e., $\delta$ is skew-symmetric. □

*Proof of* $(b)$. Let $h$ be our $\frac{1}{2}$-symmetric polynomial. Assume that $\operatorname{char} F \neq 2$. If $h$ is symmetric, we are done by letting $f = h$, $g = 0$ so suppose not. The action of $S = S_n$ on $h$ has orbit $\{h, h'\}$ for some other polynomial $h'$, since by the orbit-stabilizer theorem $|S_h||Sh| = |S|$, but $S_h = A_n$ so $|Sh| = 2$. This implies $f = \frac{1}{2}(h + h')$ is symmetric, for $h, h'$ will just be interchanged. $\tilde{g} = h - f = \frac{1}{2}(h - h')$ is antisymmetric for the same reason.

It now suffices to show that any antisymmetric polynomial $\tilde{g}$ is divisible by $\delta$, i.e., any binomial $u_i - u_j$ divides it. For, if $\varphi$ is the substitution map letting $u_j = u_i$, then $\varphi(\tilde{g}) = -\varphi(\tilde{g})$ implies $\varphi(\tilde{g}) = 0$. So letting $g = \tilde{g}/\delta$ suffices, since $g$ cannot be anti-symmetric otherwise $\tilde{g}$ would be symmetric by $(a)$. □

**Exercise 16.M.10.** *Let $K$ be a finite extension of a field $F$, and let $f(x)$ be in $K[x]$. Prove that there is a nonzero $g(x)$ in $K[x]$ such that the product $f(x)g(x)$ is in $F[x]$.*

*Proof.* We can assume $f(x)$ is irreducible by working with irreducible factors individually; suppose moreover that it is monic. Any root $\alpha$ of $f(x)$ is algebraic over $K$ hence algebraic over $F$ by Exercise 15.10.1. Thus we have $h(x) \in F[x]$ the minimal polynomial for $\alpha$ over $F$. Then $f \mid h$ since $f$ is defined over $K$; thus $h = fg$ for some $g \in K[x]$. □

# List of Solved Exercises