Chapter 3

Fields

In Chapter 2, we explored problems about finding and expressing roots of polynomials, finally arriving at the goal of the course: proving that there are quintic polynomials that are *not* solvable by radicals. This chapter serves two main purposes. First, as we look at roots of polynomials and how they can be expressed, it will be convenient to have a common world (i.e. number system) in which they live. For us, this will be the complex numbers, denoted $\mathbb{C}$, which will be reviewed below. Our work with complex numbers will also supply the necessary language to properly talk about n^{th}-roots. Second, we are still in need of a proper definition of what it means for a polynomial to be "solvable by radicals"; this is where the chapter will finish. But the middle of the chapter is perhaps the most interesting. There, on the way to defining "solvable by radicals", we will be led to abstract the structure of $\mathbb{C}$ (and of $\mathbb{Q}$ and $\mathbb{R}$), arriving at the definition of a *field*.

3.1 Complex Numbers

As mentioned above, we want to work in a world that contains all of the roots of all of the polynomials that we will be studying. Considering the roots of polynomials such as x^2+1, x^2-2, x^2-3, etc., we see that we need to include numbers like $\sqrt{-1}$, $\sqrt{2}$, $\sqrt{3}$, etc., so although there are smaller worlds one could choose, we will opt for the world containing both $\sqrt{-1}$ and $\mathbb{R}$, namely $\mathbb{C}$.

But before we proceed, note that $\sqrt{-1}$ is not really well defined. There are *two* solutions to x^2+1, so when we write $\sqrt{-1}$, we are all agreeing that we mean the same one.

Definition 3.1. Let i (or alternatively $\sqrt{-1}$) denote one particular solution to x^2+1.

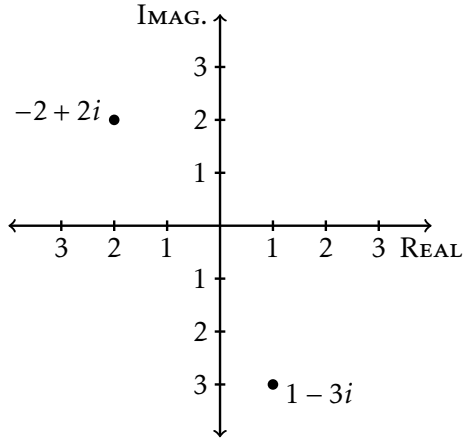
Of course, the previous definition implies that $i^2 = -1$. Using i and $\mathbb{R}$, we now build the complex numbers.

3.1.1 Definition and first principles

Definition 3.2. The **complex numbers** is the set $\mathbb{C} := \{a+bi \mid a,b \in \mathbb{R}\}$. If $z = a+bi$, then a is called the **real part** of z and b is called the **imaginary part** of z.

Note that every complex number $z = a + bi$ is uniquely determined by two numbers: the real and imaginary parts a and b. As such, we often graph complex numbers in the coordinate plane with the x-axis denoting the real part and the y-axis denoting the imaginary part. This will be called the **complex plane**.

Example 3.3. We graph $-2 + 2i$ and $1 - 3i$ below.



We also define some operations on complex numbers.

Definition 3.4. We define the following operations on elements of $\mathbb{C}$.

- **Addition:** $(a + bi) + (c + di) := (a + b) + (c + d)i$
- **Multiplication:** $(a + bi) \cdot (c + di) := (ac - bd) + (ad + bc)i$
- **Complex Conjugation:** $\overline{a + bi} := a - bi$

Notice that in the definition of complex multiplication we are just using the normal distributive law (or FOIL if you like) together with the fact that $i^2 = -1$. Many of the familiar algebraic properties of $\mathbb{R}$ also hold for $\mathbb{C}$, which we will take as a fact.

Fact 3.5. The following are true for $\mathbb{C}$.

- **Addition Laws:** Addition is associative and commutative. There is a unique additive identity, namely $0 = 0 + 0i$, and every number has a unique additive inverse, denoted $-(a + bi)$.
- **Multiplication Laws:** Multiplication is associative and commutative. There is a unique multiplicative identity, namely $1 = 1 + 0i$, and every nonzero number has a unique multiplicative inverse, denote $(a + bi)^{-1}$ or $\frac{1}{a+bi}$.
- **Distributivity Laws:** For all $x, y, z \in \mathbb{C}$, $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$.
- **Conjugation Laws:** For all $x, y \in \mathbb{C}$, $\overline{x + y} = \overline{x} + \overline{y}$ and $\overline{xy} = \overline{xy}$.

Problem 3.6. Thinking of a complex number $z = a+bi$ as a point in the complex plane, describe *geometrically* what happens when $(c + di)$ is added to z. Also, describe *geometrically* how to find $\overline{z}$ from z.

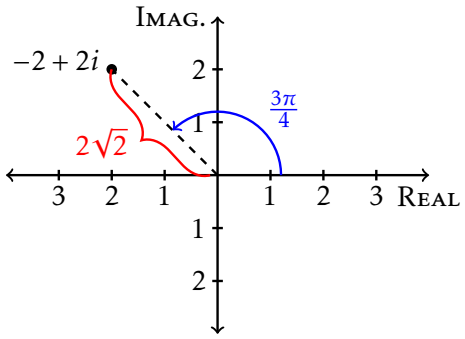
When we plot points, there are different coordinate systems we could use. It turns out that rectangular coordinates are good for adding complex numbers, but polar coordinates are better for multiplication. This lead to the following definition.

Definition 3.7. Let $z = a + bi$.

(1) The **modulus** of z, denoted $|z|$, is the radius of the point (a, b) when written in polar coordinates. Thus, $|z| = \sqrt{a^2 + b^2}$.

(2) The **argument** of z, denoted $\text{Arg}(z)$, is the angle of the point (a, b) when written in polar coordinates. Thus, $\text{Arg}(z)$ is the angle θ *in the appropriate quadrant* such that $0 \leq \theta < 2\pi$ and $\tan\theta = \frac{b}{a}$. The argument of 0 is undefined.

Example 3.8. We have that $|-2 + 2i| = \sqrt{(-2)^2 + 2^2} = 2\sqrt{2}$ and $\text{Arg}(-2 + 2i) = \frac{3\pi}{4}$. (But be careful, $\arctan\left(\frac{2}{-2}\right) = \frac{\pi}{4}$; you must pay attention to which quadrant the number is in.)



Problem 3.9. For each of the following complex numbers,

- write it in the form $a + bi$ (if it is not already),
- plot it in the complex plane,
- find the modulus and argument (if not exact, then a decimal approximation is okay).

(1) $u = -1 - i$

(2) $v = \frac{1}{1+i}$

(3) $w = \frac{(2-i)(1+2i)}{2+3i}$

(4) $z \in \mathbb{C}$ with $|z| = 3$ and $\text{Arg}(z) = \frac{4\pi}{3}$

Theorem 3.10. Let $z \in \mathbb{C}$. If $z \neq 0$, then $z^{-1} = \dfrac{\overline{z}}{|z|^2}$.

The next theorem shows how to find an expression for a complex number given its modulus and argument.

Theorem 3.11. Let $z \in \mathbb{C}$. Then $|z| = r$ and $\text{Arg}(z) = \theta$ if and only if $z = r\cos\theta + ir\sin\theta$ with $0 \leq \theta < 2\pi$.

We now derive some properties of multiplication. The first is quite useful and illustrates how multiplication is rather easy to deal with when numbers are in "polar form".

Theorem 3.12. If $z_1 = r_1\cos\theta_1 + ir_1\sin\theta_1$ and $z_2 = r_2\cos\theta_2 + ir_2\sin\theta_2$, then

$$z_1z_2 = r_1r_2\cos(\theta_1+\theta_2) + ir_1r_2\sin(\theta_1+\theta_2).$$

Corollary 3.13. If $z_1, z_2 \in \mathbb{C}$, then $|z_1z_2|$ is equal to $|z_1||z_2|$ and $\mathrm{Arg}(z_1z_2)$ is equivalent to $\mathrm{Arg}(z_1) + \mathrm{Arg}(z_2)$ modulo 2π.

Corollary 3.14 (De Moivre's formula)**.** For each positive $n \in \mathbb{Z}$,

$$(r\cos(\theta) + ir\sin(\theta))^n = r^n\cos(n\theta) + ir^n\sin(n\theta).$$

3.1.2 Roots of unity

We now arrive at an *extremely important* definition.

Definition 3.15. For each positive $n \in \mathbb{Z}$, define

$$\zeta_n := \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right).$$

Thus, ζ_n (read as "zeta n") is the unique number with magnitude 1 and argument $\frac{2\pi}{n}$.

Problem 3.16. Plot each of the following in the same complex plane: ζ_2, ζ_3, ζ_4, ζ_5.

Problem 3.17. Plot each of the following in the same complex plane: ζ_6, $(\zeta_6)^2$, $(\zeta_6)^3$, $(\zeta_6)^4$, $(\zeta_6)^5$, $(\zeta_6)^6$.

Problem 3.18. Write $\overline{\zeta_8}$ as a power of ζ_8. Conjecture and prove a formula that expresses $\overline{(\zeta_n)^k}$ as a power of ζ_n, but with no bar on top.

We now turn our attention back to solving polynomial equations, focusing on those of the form $x^n - a$.

Definition 3.19. Let $a \in \mathbb{C}$. A number $z \in \mathbb{C}$ is called an n^{th} **root of** a if $z^n = a$. In other words, the n^{th} roots of a are the roots of the polynomial $x^n - a$. The n^{th} roots of 1 are also called n^{th} **roots of unity**.

Problem 3.20. Find a 4^{th} root of each of the following: ζ_3 and $-1 + i\sqrt{3}$.

Theorem 3.21. For each non-negative $k \in \mathbb{Z}$, $(\zeta_n)^k$ is an n^{th} root of 1.

Lemma 3.22. If z is an n^{th} root of 1, then $z = (\zeta_n)^k$ for some non-negative $k \in \mathbb{Z}$.

Lemma 3.23. For each non-negative $k \in \mathbb{Z}$, $(\zeta_n)^k = (\zeta_n)^m$ for some $0 \le m \le n-1$.

Theorem 3.24. The set

$$\{1, \zeta_n, (\zeta_n)^2, \ldots, (\zeta_n)^{n-1}\}$$

is the set of *all* n^{th} roots of unity. Thus, there are n distinct n^{th} roots of unity.

Lemma 3.25. Let $a \in \mathbb{C}$ be nonzero, and let b be any one particular n^{th} root of a. Then z is an n^{th} root of a if and only if $\frac{z}{b}$ is an n^{th} root of 1.

Theorem 3.26. Let $a \in \mathbb{C}$ be nonzero, and let b be any one particular n^{th} root of a. The set

$$\{b, b\zeta_n, b(\zeta_n)^2, \ldots, b(\zeta_n)^{n-1}\}$$

is the set of *all* n^{th} roots of a. Thus, there are n distinct n^{th} roots of a.

Problem 3.27. Find *all* 4^{th} roots of each of the following: ζ_3 and $-1 + i\sqrt{3}$.

3.1.3 Roots of polynomials over $\mathbb{R}$ and $\mathbb{C}$

We conclude this section with a couple of general results about roots of polynomials.

Theorem 3.28. Suppose that $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ with all $a_i \in \mathbb{R}$. If z is a root of $p(x)$, then $\overline{z}$ is also a root of $p(x)$.

In words, the previous theorem says that if a polynomial has coefficients in $\mathbb{R}$, then the set of roots is "closed under complex conjugation." We end with an extremely important theorem, which will be quite useful for us. However, since its proof is not our main goal (and since it requires sophisticated techniques), we will take it as fact.

Fact 3.29 (Fundamental Theorem of Algebra)**.** If $p(x)$ is a non-constant polynomial with all coefficients in $\mathbb{C}$, then $p(x)$ has a root in $\mathbb{C}$.

In fact, we will see that this implies that *all* roots of such a $p(x)$ lie in $\mathbb{C}$, so in our of study polynomials (often with all coefficients even in $\mathbb{Q}$), $\mathbb{C}$ serves as a uniform world in which we can study the roots.

3.2 An aside: the quaternions

Our construction of the complex numbers creates a structure that contains the real numbers and possesses some nice properties not enjoyed by the real numbers, e.g. every non-constant polynomial with complex coefficients has a complex root. This raises the question: could we further extend the complex numbers to an even larger structure?

Concisely, we built the complex numbers as the set $\mathbb{C} = \mathbb{R} + \mathbb{R}i$ together with the operations of addition and multiplication, which were defined in a natural way from the key identity that $i^2 = -1$. Here, we briefly explore what happens if we build a larger structure in a similar way: $\mathbb{H} = \mathbb{C} + \mathbb{C}j$ where, again, $j^2 = -1$.

Following this path, we formally arrive at $\mathbb{H} = \mathbb{C} + \mathbb{C}j = (\mathbb{R} + \mathbb{R}i) + (\mathbb{R} + \mathbb{R}i)j$, and any definition we give for multiplication of two elements of $\mathbb{H}$ must first define how to multiply i and j (or rather, what properties ij should have). If we set $k = ij$, it turns out that a good route to follow is to decide that k also has the property that it squares to 1, i.e. $k^2 = -1$. There is another important choice one is "forced" to make, namely that $ji = -k$.

Definition 3.30. The **quaternions** are the elements of $\mathbb{H} := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$, where $i^2 = j^2 = k^2 = -1$. We also define the following operations on elements of $\mathbb{H}$.

- **Addition:** $(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) := (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$
- **Multiplication:** use the usual distributive laws together with the identities:

$$\begin{array}{lll} ij = k, & jk = i, & ki = j, \\ ji = -k, & kj = -i, & ik = -j. \end{array}$$

- **Conjugation:** $\overline{a + bi + cj + dk} := a - bi - cj - dk$

Indeed, $\mathbb{H}$ extends the complex numbers, and we have the following containments: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$. It turns out that $\mathbb{H}$ satisfies nearly all of the common algebraic properties of $\mathbb{R}$ and $\mathbb{C}$, with one notable exception, which is highlighted in bold below.

Fact 3.31. The following are true for $\mathbb{H}$.

- **Addition Laws:** Addition is associative and commutative. There is a unique additive identity, namely $0 = 0 + 0i + 0j + 0k$, and every number has a unique additive inverse.
- **Multiplication Laws:** Multiplication is associative but **noncommutative**. There is a unique multiplicative identity, namely $1 = 1+0i+0j+0k$, and every nonzero number has a unique multiplicative inverse.
- **Distributivity Laws:** For all $x, y, z \in \mathbb{H}$, $x(y+z) = xy + xz$ and $(y+z)x = yx + zx$.
- **Conjugation Laws:** For all $x, y \in \mathbb{H}$, $\overline{x+y} = \overline{x} + \overline{y}$ and $\overline{xy} = \overline{xy}$.

We can also define the modulus of a quaternion, analogous to how we defined it for a complex number.

Definition 3.32. The **modulus** of $h = a+bi+cj+dk$, denoted $|h|$, is $|h| = \sqrt{a^2+b^2+c^2+d^2}$.

Problem 3.33. Write each of the following quaternions in the form $a + bi + cj + dk$, and find its modulus.

(1) $h = (2i + 4k)(7 - 3j + k)$

(2) k^{-1}

(3) $w = (i + j)^{-1}$

Theorem 3.34. Let $h \in \mathbb{H}$. If $h \neq 0$, then $h^{-1} = \dfrac{\overline{h}}{|h|^2}$.

And as in the complex numbers, the modulus function is multiplicative—we will take this as fact.

Fact 3.35. If $h_1, h_2 \in \mathbb{H}$, then $|h_1 h_2| = |h_1||h_2|$.

We conclude this section by looking at multiplication of quaternions a little closer. As we do, we return to the mathematical notion of a *group*. Please feel free to look over old notes or other books to review the basics. As mentioned in the introduction, our main reference for groups will be An Inquiry-Based Approach to Abstract Algebra.

Problem 3.36. Let G be the subset of $\mathbb{H}$ defined as $G := \{\pm 1, \pm i, \pm j, \pm k\}$. Show that G, together with the operation of quaternion multiplication, is a nonabelian group. If you have encountered this group before, what name (or symbol) did you know it by?

Problem 3.37. Let S be the subset of $\mathbb{H}$ consisting of all quaternions with modulus equal to 1, i.e. $S := \{h \in \mathbb{H} \mid |h| = 1\}$. Show that S, together with the operation of quaternion multiplication, is an infinite, nonabelian group.

It turns out that the group S from the previous problem is isomorphic to the group SU(2) (one the the so-called special unitary groups), which is quite important in theoretical physics. If you want to learn more, you can start on Wikipedia.

3.3 Abstract fields

Notice that $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ satisfy many common algebraic properties with respect to addition and multiplication. Of course, $\mathbb{H}$ does too, though it lacks commutativity of multiplication. When objects have common properties, it can be extremely valuable to abstract those properties and study them once and for all (as opposed to trying to prove things about each individual structure). This is where we are headed, but first we highlight some related structures (again with algebraic properties similar to $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$) that help to connect this work to our main goal of expressing roots of polynomials.

Problem 3.38. Let $p(x) = x^2 + 3x + 1$. Find the roots of $p(x)$, and show that each root can be written in the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$.

Problem 3.39. Let $S = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$.

(1) Show that S is closed under addition; that is, show that for all $x, y \in S$, $x + y \in S$.

(2) Show that S is closed under multiplication; that is, show that for all $x, y \in S$, $xy \in S$.

(3) Use that $S \subset \mathbb{R}$ to explain why both addition and multiplication of elements of S are associative and commutative and why multiplication distributes over addition.

Problem 3.40. Let $S = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. Prove or disprove: if $x \in S$ and $x \neq 0$, then x has a multiplicative inverse *in* S (i.e. there is a $y \in S$ such that $xy = 1$).

3.3.1 Definition

We now abstract the common properties of $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ (and also S from Problem 3.39), arriving at the definition of a field.

Definition 3.41. A **field** is a structure $(F, +, \cdot)$ consisting of a set F, containing at least two elements, together with two binary operations $+$ and $\cdot$ (which we call *addition* and *multiplication*) such that for some elements $0, 1 \in F$ the following axioms hold.

- **Addition Axioms:** Addition is associative and commutative; the element 0 is an additive identity; every $x \in F$ has an additive inverse with respect to 0, denoted $-x$.
- **Multiplication Axioms:** Multiplication is associative and commutative; the element 1 is a multiplicative identity; every $x \in F \setminus \{0\}$ has a multiplicative inverse with respect to 1, denoted x^{-1}.
- **Distributivity Axioms:** For all $x, y, z \in \mathbb{F}$, $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$.

Recall that "0 is an additive identity" means that "for all $x \in F$, $0 + x = x + 0 = x$," and "$x \in F$ has an additive inverse with respect to 0" means that "there exists some $y \in F$ such that $x + y = y + x = 0$." The meanings of multiplicative identities and inverses are similar to those for addition. Also, recall that $F \setminus \{0\}$ denotes the set obtained by removing the element 0 from F. We introduce some notation for this.

Definition 3.42. If F is a field, then $F \setminus \{0\}$ is denoted by F^*, i.e. F^* is the set of nonzero elements of F.

Using the language of groups, fields can be concisely defined as structures of the form $(F, +, \cdot)$ such that $(F, +)$ is an abelian group with identity 0, $(F^*, \cdot)$ is an abelian group with identity 1, and multiplication distributes over addition.

Now, as with any new definition, we look for examples and basic properties.

3.3.2 Examples and non-examples

It is not hard to verify that $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and S from Problem 3.39 are all fields (with their usual definitions of addition and multiplication). Let's search for more examples and non-examples.

Problem 3.43. Explain why $\mathbb{Z}$ is not a field.

Problem 3.44. Determine if each of the following is a field. If it is a field, identify an additive and multiplicative identity; if it is not a field, explain why not.

(1) $(F, +, \cdot)$ where $F = \{a, b, c\}$ and $+$ and $\cdot$ are defined as follows:

$+$	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

$\cdot$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

(2) $(F, +, \cdot)$ where $F = \{0, 1, 2, 3\}$ and $+$ and $\cdot$ are defined as follows:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(3) $(F, +, \cdot)$ where $F = \{0, 1, 2, 3\}$ and $+$ and $\cdot$ are defined as follows:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Problem 3.45. Look back at Problem 3.44. For those that are fields, determine which familiar group each of $(F, +)$ and $(F^*, \cdot)$ is isomorphic to.

To find more examples of fields, Problem 3.44 hints at the fact we may want to look back to modular arithmetic. Following An Inquiry-Based Approach to Abstract Algebra, we define the structures $(\mathbb{Z}_n, +_n, \cdot_n)$ as follows.

Definition 3.46. Let n be a positive integer. The structure $(\mathbb{Z}_n, +_n, \cdot_n)$ consists of the set $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$ together with the operations $+_n$ and $\cdot_n$ defined as follows.

- **Addition:** $x +_n y$ is the least non-negative number congruent to $x + y$ modulo n.
- **Multiplication:** $x \cdot_n y$ is the least non-negative number congruent to $x \cdot y$ modulo n.

We often refer to the entire structure $(\mathbb{Z}_n, +_n, \cdot_n)$ as simply $\mathbb{Z}_n$. Also, when the context is clear, we may write $+$ and $\cdot$ in place of $+_n$ and $\cdot_n$.

So, in $\mathbb{Z}_5$, we write equations like $3+6=4$, since $3+6=9$ and 9 is congruent to 4 when working modulo 5. If needed, we can highlight that we are working modulo 5 by writing $3+6 \equiv_5 4$. And with respect to multiplication in $\mathbb{Z}_5$, we have equations like $2 \cdot 3 = 1$, which implies that 3 is a multiplicative inverse of 2 (and vice versa) in $\mathbb{Z}_5$.

Problem 3.47. Show that $\mathbb{Z}_5$ is a field but $\mathbb{Z}_6$ is not.

Problem 3.48. Make a conjecture as to when $\mathbb{Z}_n$ is a field and when it is not. That is, try to fill in the blank: "$\mathbb{Z}_n$ is a field provided ____(something about n)____." What evidence do you have to support this?

3.3.3 Basic properties

Let's now explore some basic properties of fields that follow from the definition. We list some of these as facts since they follow directly from basic group theory, remembering that, as observed above, $(F, +)$ and $(F^*, \cdot)$ are both groups.

From now on, when we write "let F be a field," we tacitly mean "let $(F, +, \cdot)$ be a field."

Fact 3.49. Let F be a field.

(1) The additive identity and the multiplicative identity are both unique.

(2) Additive inverses and multiplicative inverses are unique.

Theorem 3.50. Let F be a field.

(1) For all $x \in F$, $x \cdot 0 = 0$.

(2) For all $x, y \in F$, $(-x)y = -(xy)$ and $x(-y) = -(xy)$.

(3) For all $x \in F^*$, $-x \in F^*$ and $(-x)^{-1} = -(x^{-1})$.

(4) For all $x, y \in F$, if $xy = 0$, then $x = 0$ or $y = 0$.

(5) The additive and multiplicative identities are different, i.e. $0 \neq 1$.

3.3.4 Another example

We now return to the conjecture you made in Problem 3.48. Combining the next theorem with Theorem 3.50, we see that $\mathbb{Z}_n$ has no hope to be a field unless n is prime.

Theorem 3.51. Let n be a positive integer. If n is not prime, then there exist $a, b \in (\mathbb{Z}_n)^*$ such that $ab = 0$ in $\mathbb{Z}_n$.

And now we completely answer the question. As you explore the next theorem, you can use properties of modular arithmetic that you know from before. For example, you can take for granted that addition and multiplication are both associative and commutative. The crux is in showing that every nonzero element has a multiplicative inverse when n is prime. There are many ways to approach this; one way uses Bézout's lemma from basic number theory. Even if you don't use it now, it's a useful fact to remember.

Fact 3.52 (Bézout's lemma)**.** If $a, b \in \mathbb{Z}$, then there exist $k, l \in \mathbb{Z}$ such that $ka + lb = \gcd(a, b)$.

Theorem 3.53. Let n be a positive integer. Then $\mathbb{Z}_n$ is a field if and only if n is prime.

3.3.5 Subfields and extension fields

Just as with groups and subgroups, the notion of a subfield is extremely important. Analyzing the subfields of a field F can often yield a better understanding of the whole field F, and vice versa. Also, this will allow us to generate more examples of fields.

Definition 3.54. Let $(E, +, \cdot)$ be a field, and let F be a subset of E. Then F is a **subfield** of E if F is a field in its own right with respect to operations $+$ and $\cdot$ *inherited from* E. When F is a subfield of E, we call E an **extension field** of F.

When checking if a subset of a field is a subfield, it turns out that the subset will automatically satisfy many of the field axioms, leaving only a handful of things to verify.

Theorem 3.55. Let E be a field, and let $F \subseteq E$. Then F is a subfield of E if and only if

(1) F contains at least 2 elements;

(2) for all $x, y \in F$, $x + y \in F$ and $xy \in F$;

(3) for all $x \in F$, $-x \in F$; and

(4) for all $x \in F^*$, $x^{-1} \in F$.

The second item in the above theorem is stating that F is closed under the addition and multiplication inherited from E. The last two items could be read as F being closed under additive and multiplicative inverses.

Theorem 3.56. If F is a subfield of E, then F contains the additive and multiplicative identities of E (namely 0 and 1).

It is not difficult to check that $\mathbb{Q}$ and $\mathbb{R}$ are both subfields of $\mathbb{C}$; S from Problem 3.39 is also a subfield of $\mathbb{C}$ (and of $\mathbb{R}$). Let's look for more that are similar to S.

Problem 3.57. Determine which of the following are subfields of $\mathbb{C}$.

(1) $T_1 = \{a + bi \mid a, b \in \mathbb{Q}\}$

(2) $T_2 = \{a + bi \mid a, b \in \mathbb{Z}\}$

(3) $T_3 = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$ where $\alpha = \sqrt{2} + i$

3.3.6 Generating fields

Paralleling the theory of groups, we now investigate how to generate subfields from subsets of elements. We first need a *definition* of "the subfield generated by a set of elements"; it is essentially the same as for all algebraic structures: take the intersection of all subfields containing the subset.

Theorem 3.58. Suppose S is a subset of a field E. Let K be the intersection of all subfields of E that contain S; that is

$$K := \bigcap \{F \mid F \text{ is a subfield of } E \text{ and } S \subseteq F\}.$$

Then

(1) K is a subfield of E that contains S, and

(2) if F is any subfield of E that contains S, then F also contains K.

In words, the previous theorem says that K is the "smallest" subfield of E containing S, so K is the correct candidate for the subfield generated by S.

Definition 3.59. Suppose S is a subset of a field E. The **subfield of E generated by S**, denoted $\langle S \rangle_{\text{FIELD}}$, is defined to be the intersection of all subfields of E that contain S.

In symbols, $S \subseteq \langle S \rangle_{\text{FIELD}} \subseteq E$, and if F is any subfield of E, then $S \subseteq F \implies \langle S \rangle_{\text{FIELD}} \subseteq F$.

Example 3.60. Let's explore $\langle 1 \rangle_{\text{FIELD}}$ in the field $\mathbb{C}$. By definition, $\langle 1 \rangle_{\text{FIELD}}$ is the intersection of all subfields of $\mathbb{C}$ that contain 1.

Let F be an arbitrary subfield of $\mathbb{C}$ containing 1. By Theorem 3.56, every subfield of $\mathbb{C}$ contains 0 and 1, so F must contain 0 (in addition to 1). Further, F must contain $1 + 1$, $1 + 1 + 1$, etc., because F is closed under addition. So, by induction, F contains the positive integers and 0. Then, since F is closed under additive inverses, F also contains the additive inverse of each positive integer, so in total, we now see that F contains $\mathbb{Z}$. Continuing on, F is closed under multiplicative inverses, so F also contains the multiplicative inverse of every nonzero integer. Thus, $\mathbb{Q} \subseteq F$.

Since F was an *arbitrary* subfield of $\mathbb{C}$ containing 1, everything we said above is true for *every* subfield of $\mathbb{C}$ containing 1; thus it is also true for the intersection of them. Hence $\mathbb{Q} \subseteq \langle 1 \rangle_{\text{FIELD}}$. Now we have $\{1\} \subset \mathbb{Q} \subseteq \langle 1 \rangle_{\text{FIELD}}$, so as $\mathbb{Q}$ is a subfield and $\langle 1 \rangle_{\text{FIELD}}$ is the *smallest* subfield containing 1, it must be that $\mathbb{Q} = \langle 1 \rangle_{\text{FIELD}}$.

Theorem 3.61. If $S \subseteq \mathbb{C}$, then $\mathbb{Q} \subseteq \langle S \rangle_{\text{FIELD}}$.

Problem 3.62. The field defined in Problem 3.44(3) is sometimes denoted $\mathbb{F}_4$. Determine $\langle 1 \rangle_{\text{FIELD}}$ in the field $\mathbb{F}_4$.

Most of the time, we will want to generate fields by adding some elements to an existing field, and we have special notation for this.

Notation 3.63. Let F be a subfield of E, and let $r_1, r_2, \ldots, r_n \in E$. The subfield of E generated by $F \cup \{r_1, r_2, \ldots, r_n\}$ is denoted $F(r_1, r_2, \ldots, r_n)$. In other words,

$$F(r_1, r_2, \ldots, r_n) := \langle F \cup \{r_1, r_2, \ldots, r_n\} \rangle_{\text{FIELD}}.$$

We read $F(r_1, r_2, \ldots, r_n)$ as "F adjoin $r_1, r_2, \ldots, r_n$"; it is the smallest field extension of F that contains $r_1, r_2, \ldots, r_n$.

In the following problems, we are working with subfields of $\mathbb{C}$, even if we don't say it explicitly. Thus, by Theorem 3.61, we are working with field extensions of $\mathbb{Q}$.

Problem 3.64. In Problem 3.57(1), we saw that $\{a + bi \mid a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$. Show that $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

Problem 3.65. Show that $\mathbb{R}(i) = \mathbb{C}$.

Problem 3.66. We saw previously that $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$. Find some $z \in \mathbb{C}$, such that $\mathbb{Q}(z) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$, and prove that your choice for z works. Do you think there is only one choice for z or might others work?

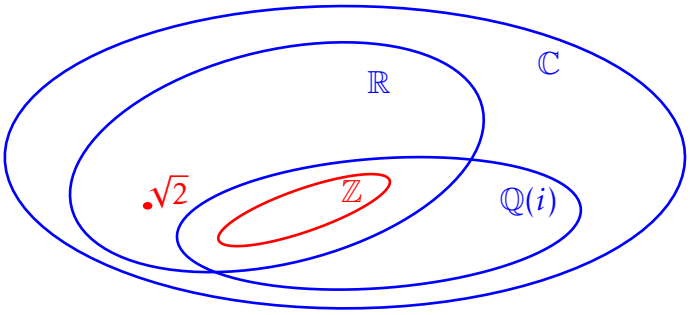
Problem 3.67. Let $\alpha = \sqrt{2} + i$. Show $\{a + b\alpha \mid a, b \in \mathbb{Q}\} \subset \mathbb{Q}(\alpha)$, but $\{a + b\alpha \mid a, b \in \mathbb{Q}\} \neq \mathbb{Q}(\alpha)$.

Theorem 3.68. Let F, L be subfields of E, and let $r_1, r_2, \ldots, r_n \in E$. Then $F(r_1, r_2, \ldots, r_n) \subseteq L$ if and only if $F \subseteq L$ and $r_1, r_2, \ldots, r_n \in L$.

Problem 3.69. Show that $\mathbb{Q}\left(3 - \sqrt{2}, 5 + i\right) = \mathbb{Q}\left(\sqrt{2}, i\right)$.

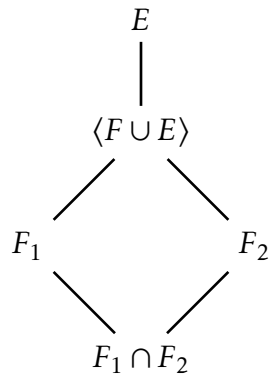
Problem 3.70. Complete the diagram below to illustrate how each of the following sets intersect and where each element is located. Each set that is a field should be drawn in blue; each set that is not a field should be drawn in red. Elements should be illustrated by a dot and then labeled by the name of the element. Some have already been done.

$$\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, 0, 1, \sqrt{2}, i, i\sqrt{2}, \sqrt{2} + i, \mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}(i), \mathbb{Q}\left(i\sqrt{2}\right) \mathbb{Q}\left(\sqrt{2}, i\right), \{a + bi \mid a, b \in \mathbb{Z}\}$$

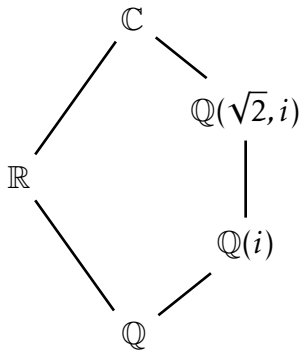


Problem 3.71. Conjecture where $\mathbb{Q}\left(\sqrt{2} + i\right)$ would be in the previous diagram.

Suppose that F_1 and F_2 are subfields of E. Theorem 3.58 tells us that $F_1 \cap F_2$ is again a subfield, and it is the largest subfield contained in both F_1 and F_2. The same theorem, together with Definition 3.59, also tells us that $\langle F_1 \cup F_2 \rangle_{\text{FIELD}}$ is a subfield, and it is the smallest subfield containing both $F_1$and F_2. This implies that the set of all subfields of E forms a lattice. Lattices will not be defined here, but feel free to look them up on your own. We will, however, be interested in illustrating these relationships with a diagram. The situation for F_1 and F_2 described above would be drawn as follows.



For a concrete example, let's draw the portion of the subfield lattice of $\mathbb{C}$ containing $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}(i)$, and $\mathbb{Q}\left(\sqrt{2}, i\right)$; this uses some of what you discovered in Problem 3.70.



Problem 3.72. Draw the portion of the subfield lattice of $\mathbb{C}$ that contains the following fields: $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathbb{Q}(i)$, $\mathbb{Q}\left(i\sqrt{2}\right)$, and $\mathbb{Q}\left(\sqrt{2}, i\right)$.

Problem 3.73. Draw the portion of the subfield lattice of $\mathbb{C}$ that contains the following fields: $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Q}(\zeta_4)$, $\mathbb{Q}(\zeta_8)$, and $\mathbb{Q}(\zeta_{16})$.