1 Constructing the rational numbers

i) The equivalence relation captures the less rigorous definition of $\mathbb{Q}$ that we’re all familiar with, namely that two fractions $a/b$ and $c/d$ are equal iff we can multiply through by the denominators and have $ad = cd$.

ii) We want the field operations to align with our usual intuition for addition and multiplication of rational numbers. Since $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ we should have $[(a, b)] \cdot [(c, d)] = [(ac, bd)]$ (where $[(a, b)]$ denotes the equivalence class for $(a, b)$ modulo $\sim$). Similarly, $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$, so we define $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$. The fact that $\mathbb{Q}$ is a field under these operations follows from a straightforward check of the field axioms. (The additive and multiplicative identities are $[(0, 1)]$ and $[(1, 1)]$, respectively; given any nonzero element $[(a, b)]$, its inverse is $[(b, a)]$.)

2 Finite fields

i) Let $m = |F|$. For a nonnegative integer $n$, denote by $\pi$ the element

$$\pi = 1 + 1 + \cdots + 1.$$ 

and consider the $m + 1$ elements $1, 2, \ldots, m + 1$ of $F$. Since $F$ only have $m$ distinct elements, by the pigeonhole principle at least two of these elements must be the same, i.e.

$$\pi = 1 + 1 + \cdots + 1 = \pi$$

for some $1 \leq a < b \leq m + 1$. By subtracting 1 from each side of this equation $a$ times, we observe that $\pi = 1 + 1 + \cdots + 1 = 0$, so we can take $n = b - a > 0$.

ii) Lagrange’s theorem states that if $G$ is a group and $H$ is a subgroup of $G$, then $|H|$ divides $|G|$. (See [https://en.wikipedia.org/wiki/Group_(mathematics)](https://en.wikipedia.org/wiki/Group_(mathematics)) for the definition of group and subgroup.) It follows directly from the field axioms that $F$ is a group under $\cdot$. If we let $H = \{\pi : n \in \mathbb{Z}, n \geq 0\}$, we observe that $H$ is a subgroup of $F$. We have $0 \in H$ by definition. Closure under $\cdot$ is clear. To find the inverse of $\pi$ in $H$, note that we can assume that $n < c_F$. If $n \geq c_F$, we can subtract $c_F$ 1’s from $\pi$.
(which is the same as subtracting 0, so this does not change the element) to represent the element as a smaller number of 1’s. We can repeat this process until $0 \leq n < c_p$. Then the element $c_p - n$ is the additive inverse of $n$, and this is an element of $H$. Thus $H$ is a subgroup of $F$ under $+$. Finally, observe that $|H| = c_p$, so applying Lagrange’s theorem immediately gives us that $c_p$ divides $|F|$.

iii) By part (ii), we know that $c_p|p$, so $c_p = 1$ or $p$ since $p$ is prime. But we know that $H$ contains at least two distinct elements, namely 0 and 1, so $c_p > 1$. Therefore $c_p = p$ as desired.

iv) We first establish the existence of a field with $p$ elements. Denote by $\mathbb{Z}/p\mathbb{Z}$ the integers mod $p$. All of the field conditions are clearly met except potentially for the existence of multiplicative inverses. Let $a \neq 0 \in \mathbb{Z}/p\mathbb{Z}$ and consider the set $S = \{ax : x \in \mathbb{Z}/p\mathbb{Z}\}$. We claim that $ax \neq ay$ when $x \neq y$ in $\mathbb{Z}/p\mathbb{Z}$. Indeed, if $ax = ay$ in $\mathbb{Z}/p\mathbb{Z}$ then $a(x - y) = 0$ in $\mathbb{Z}/p\mathbb{Z}$, i.e. $p|a(x - y)$. Since $p$ is prime, $p$ must divide either $a$ or $x - y$. Since $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, $p$ does not divide $a$, so $p|(x - y)$ which is equivalent to saying that $x = y$ in $\mathbb{Z}/p\mathbb{Z}$. Thus the elements $ax$ are distinct for distinct values of $x$, so the set $S$ has exactly $p - 1$ elements. Since the elements of $S$ are nonzero elements of $\mathbb{Z}/p\mathbb{Z}$, and $\mathbb{Z}/p\mathbb{Z}$ has exactly $p - 1$ nonzero elements, $S$ is precisely the set of nonzero elements of $\mathbb{Z}/p\mathbb{Z}$; in particular, 1 $\in S$. Thus there exists $x \in \mathbb{Z}/p\mathbb{Z}$ such that $ax = 1$, so each $a \neq 0$ has a multiplicative inverse and $\mathbb{Z}/p\mathbb{Z}$ is a field.

For uniqueness, because of the previous parts of the problem the elements of the field have to be

$$1_F + 1_F + \cdots + 1_F$$

for $n \in \{0, \ldots, p - 1\}$. This determines the addition operation uniquely. Using the distributive property we can also determine the multiplication uniquely. This finishes the proof.

Here is a more precise version of the same idea using better mathematical language: we first make precise what it means for two fields to be “the same.” Let $F$ and $F'$ be any two fields. Roughly speaking, they are the same if the elements of $F$ and $F'$ are essentially just relabelings of each other, but the underlying field structure of addition and multiplication remains the same. More rigorously, we want to find a bijection $\phi : F \to F'$ which satisfies $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in F$. The fact that $\phi$ is a bijection ensures that there is a one-to-one correspondence between the elements of $F$ and $F'$ (so $\phi$ is our relabeling); the latter two properties ensure that the field structure is preserved.

Now let $F$ be any field of size $p$. Let $\pi = 1_F + 1_F + \cdots + 1_F$, where $1_F$ is the multiplicative identity for $F$. (If $n$ is negative, then we add $-1_F$ to itself $-n$ times.) Part (iii) of the problem tells us that the elements $0, 1, \ldots, p - 1$ are all distinct (make sure you see why). Since these are $p$ distinct elements of $F$ and $F$ has exactly $p$ elements, this list contains all of the elements of $F$. If we define the map $\phi : F \to \mathbb{Z}/p\mathbb{Z}$ by $\phi(\pi) = n$ for $n = 0, 1, \ldots, p - 1$, then this is indeed a well-defined bijection from $F$ to $\mathbb{Z}/p\mathbb{Z}$. To check that $\phi$ preserves field structure, we note that $\bar{m} + \bar{n} = \bar{m + n}$ and $\bar{m} \cdot \bar{n} = \bar{mn}$ for any two integers $m$ and $n$. The only thing left to check is that if $\bar{m} = \bar{n}$ (but $m \neq n$ as integers), then $m = n$ in $\mathbb{Z}/p\mathbb{Z}$. This will follow from the fact that $\bar{p} = 0$ in $F$.

This shows that any field with exactly $p$ elements is the same as $\mathbb{Z}/p\mathbb{Z}$ up to a relabeling, so there is only one field with $p$ elements, namely $\mathbb{Z}/p\mathbb{Z}$.

3 Subfields

i) The statement is tautologically true. We see that $F$ satisfies all of the field axioms by definition of $-a$ and $a^{-1}$ in $k$.

ii) The set of purely real numbers $A$ is a subfield of $\mathbb{C}$ essentially by the fact that the real numbers form a field. The set of purely imaginary numbers $B$ is not a subfield since $i \in B$ but $i \cdot i = -1 \notin B$, so $B$ is not closed under multiplication.


4 Solving an equation over different fields

Let \( f(x) = x^2 + 2x + 2 \). Using the quadratic formula, we see that the two solutions to \( f(x) = 0 \) over \( \mathbb{C} \) are \(-1 \pm i\). Note that neither of these roots are in \( \mathbb{R} \) or \( \mathbb{Q} \). If \( f \) had any roots over \( \mathbb{R} \) or \( \mathbb{Q} \), since \( \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \), this would mean that \( f \) has more than two distinct roots in \( \mathbb{C} \). However, a polynomial of degree \( d \) can have at most \( d \) distinct roots over \( \mathbb{C} \). Since the degree of \( f \) is 2, this cannot happen, so \( f \) has no roots over \( \mathbb{R} \) or \( \mathbb{Q} \). Another way to see that there are no solutions over \( \mathbb{R} \) or \( \mathbb{Q} \) would be to note that when \( x \) belongs to these fields \( x^2 + 2x + 2 = (x + 1)^2 + 1 > 0 \).

Determining whether or not the equation has roots in \( \mathbb{F}_p \) is more difficult. The answer is clearly “yes” when \( p = 2 \) (we can take \( x = 0 \)), so henceforth we assume that \( p > 2 \) is an odd prime. Observe that \( f(x) = (x + 1)^2 + 1 \), so if we take \( y = x + 1 \), we observe that \( f(x) = 0 \) has a solution in \( \mathbb{F}_p \) iff there is a solution to the equation \( y^2 + 1 = 0 \) in \( \mathbb{F}_p \). Alternatively, this is true iff there is some \( y \in \mathbb{F}_p \) such that \( y^2 = -1 \).

Let \( g \) be as in the hint. We claim that the set \( S = \{1 = g^0, g, g^2, \ldots, g^{p-2}\} \) contains each element of \( \mathbb{Z}/p\mathbb{Z} - \{0\} \) exactly once. First, observe that \( g^a \neq 0 \) for all \( a \), otherwise we could never have \( g^{p-1} = 1 \). Next, suppose \( g^a = g^b \) with \( 0 < a < b < p - 1 \). By multiplying by \( (g^a)^{-1} \) on both sides, we obtain \( g^{b-a} = 1 \). But note that \( 0 < b - a < p - 1 \), contradicting the fact that the smallest positive integer \( k \) for which \( g^k = 1 \) is \( k = p - 1 \). Thus \( g^a \) and \( g^b \) are distinct when \( 0 < a < b < p - 1 \), so the elements of \( S \) are distinct. Since \( S \) contains \( p - 1 \) distinct nonzero elements of \( \mathbb{Z}/p\mathbb{Z} \) and there are precisely \( p - 1 \) nonzero elements of \( \mathbb{Z}/p\mathbb{Z} \), \( S \) much contain each such element exactly once. Note also that this implies that for every element \( g^a \) (which is all the non-zero elements of our field) \( (g^a)^{p-1} = (g^{p-1})^a = 1 \).

We now return to the equation \( y^2 = -1 \) in \( \mathbb{Z}/p\mathbb{Z} \). Clearly \( y \neq 0 \), so by the above we have \( y = g^a \) for some nonnegative integer \( a \). Thus our equation becomes \( g^{2a} = -1 \). Squaring both sides, we see that \( g^{4a} = 1 \). Thus if \( \frac{p-1}{2} \) is an integer (i.e. \( p \equiv 1 \) (mod 4)), we can take \( a = \frac{p-1}{4} \) so that \( y = g^{(p-1)/4} \). Note that in this case, \( y^2 = g^{(p-1)/2} \). Since \( (p - 1)/2 < p - 1 \), \( y^2 \neq 1 \). However, we also know that \( (y^2)^2 = 1 \). We can factor this out (using distributive law) as \( (y^2 - 1)(y^2 + 1) = 0 \). Since \( y^2 \neq 1 \), we have to have \( y^2 + 1 = 0 \) as desired.

Finally, we claim that no solution exists when \( p \neq 1 \) (mod 4). Assume that there exists a solution \( y^2 = -1 \). We can take the \( \frac{p-1}{2} \)th power of both sides, obtaining \( y^{p-1} = (-1)^{\frac{p+1}{2}} \). We have proved two paragraphs ago that the LHS is equal to 1. Therefore, the RHS is equal to 1. Therefore \( \frac{p-1}{2} \) has to be an even number.

Thus the polynomial has no solutions when \( p \equiv 3 \) (mod 4), i.e. \( f(x) \) has a root in \( \mathbb{F}_p \) iff \( p = 2 \) or \( p \equiv 1 \) (mod 4).