Math 81: Abstract Algebra

Prishita Dharampal

Credit Statement: Talked to Sair Shaikh'26, and Math Stack Exchange.

Problem 1. **Subgroups of fields.**
Let F be a field.

1. Let G be a finite abelian group. Prove that G is cyclic if and only if G has at most m elements of order dividing m for each $m \mid \#G$. *Hint.* One possible proof uses the structure theorem of finite abelian groups, but you can get away with slightly less.

2. Prove that every finite subgroup G of the multiplicative group $F^\times = F \setminus \{0\}$ is cyclic. *Hint.* Use the fact that a polynomial of degree m has at most m roots in F.

3. Deduce that if F is a finite field then $F^\times$ is cyclic. For each field F having at most 7 elements, find an explicit generator of $F^\times$.

4. Let p be an odd prime. Prove that $-1 \in \mathbb{F}_p^\times$ is a square if and only if $p \equiv 1 \pmod 4$.

5. Prove that for any odd prime p, the set of nonzero squares is an index 2 subgroup of $\mathbb{F}_p^\times$. *Hint.* You can use the above results, but there's also a purely combinatorial proof.

Solution.

1. $(\implies)$

   Assume G is cyclic. Then we know that for every positive integer m, $m \Big| |G|$ there exists a unique cyclic subgroup H of G with order m. Since H has m elements and $\forall h \in H, |h| \Big| m$, H would have at most m elements of order dividing m. Thus, there are at most m elements in G with order dividing m.

   $(\impliedby)$

To show that if group G has at most m elements of order dividing m for each $m \mid |G|$, then it must be cyclic, we prove the contrapositive.

To Show: If a abelian group G is not cyclic, then it has more than m elements of order dividing m for at least one $m \mid |G|$.

Then G cannot have a unique subgroup of order p for every prime $p \mid |G|$, since otherwise the product of generators of these cyclic subgroups would generate G, making it cyclic. Thus, there exists a prime $p \mid |G|$ such that G has at least two distinct subgroups of order p. Each subgroup of order p has exactly $p-1$ non-identity elements of order p, and different subgroups of order p intersect trivially. Hence G has at least $(2p-1)$ elements whose order divides p. Hence, there exists at least a p such that G has more than p elements of order diving p. Hence, proving the contrapositive, and the original proposition.

A finite, abelian group G is cyclic if and only if G has at most m elements of order dividing m for each $m \mid |G|$.

2. Let G be an arbitrary finite subgroup of the multiplicative group $F^{\times}$. G is abelian because F is a field. Then every element of order diving m for all $m \mid |G|$, would be a root to the equation

$$f(x) = x^m - 1 = 0$$

Since, $f(x)$ has at most m roots in F, there are at most m elements of order dividing m for every $m \mid |G|$. Hence, by subpart (1), G is cyclic. Since G was an arbitrary subgroup, every finite subgroup of the multiplicative group $F^{\times}$ is also cyclic.

3. Assume F is a finite field. $F^{\times}$ is a finite subgroup of $F^{\times}$, and hence is cyclic (subpart (2)).

   (a) Field of order $2 = \{0, 1\}$: $\mathbb{F}_2^{\times}$ is generated by 1.
   (b) Field of order $3 = \{0, 1, 2, 3\}$: $\mathbb{F}_3^{\times}$ is generated by 2.
   (c) Field of order $4 = \{0, 1, x, y\}$: $\mathbb{F}_4^{\times}$ is generated by x.
   (d) Field of order $5 = \{0, 1, 2, 3, 4\}$: $\mathbb{F}_5^{\times}$ is generated by 3.
   (e) Field of order $7 = \{0, 1, 2, 3, 5, 6\}$: $\mathbb{F}_7^{\times}$ is generated by 3.

   Note: Since $\mathbb{F}^{\times}$ is cyclic, any non identity element would generate it.

4. ($\implies$)
   If -1 is a square in $\mathbb{F}_p^{\times}$, $p \neq 2$ then there exists an element $n \in \mathbb{F}_p$ with order 4 ($|-1| = 2$). That means if there exists square root of -1 in $\mathbb{F}_p^{\times}$ then $4 \mid |\mathbb{F}_p^{\times}| \implies 4 \mid p-1 \implies p \equiv 1 \pmod 4$.

   ($\impliedby$)
   If $p \equiv 1 \pmod 4 \implies p - 1 \equiv 0 \pmod 4 \implies 4 \mid p - 1 \implies 4 \mid |\mathbb{F}_p^{\times}| \implies \exists x \in \mathbb{F}_p^{\times}$,

such that $\mid x \mid = 4$ (converse of Lagrange's Theorem for Abelian Groups).

$x^4 = 1 \implies (x^2)^2 = 1 \implies x^2 = \pm 1$. But if $x^2 = 1$, the order of x would be 2, hence a contradiction. I.e. x^2 must be -1, and $x = \sqrt{-1}$.

Hence, $-1 \in \mathbb{F}_p^\times$ is a square if and only if $p \equiv 1 \pmod 4$.

5. Let S be the set of nonzero squares in $\mathbb{F}_p^\times$, and $g : \mathbb{F}_p^\times \to S$ such that $\forall a \in \mathbb{F}_p^\times,\ g(a) = a^2$. We can see that both $a \pmod p$ and $-a \pmod p \in \mathbb{F}_p^\times$ map to the same element $a^2 \in S$, because modulo p the following relations hold:

$$a * a = a^2, \qquad -a * -a = a^2$$

We prove that g is strictly a $2:1$ mapping by contradiction. Asssume there exist distinct elements $a, b, c \in \mathbb{F}_p^\times$ such that $a^2 = b^2 = c^2 = z$. Then, consider the polynomial $x^2 - z = 0 \in \mathbb{F}_p^\times[x]$. Since, a polynomial of degree 2 has at most 2 roots in $\mathbb{F}_p^\times$, a, b, c can't be distinct. Hence, a contradiction! And g is strictly a $2:1$ mapping.

To show that $S \leq \mathbb{F}_p^\times$ is a subgroup we show that the group axioms hold.

(a) Identity: $1^2 = 1$, hence $1 \in S$.

(b) Associativity: Inherited from $\mathbb{F}_p^\times$.

(c) Closure under multiplication and inverses:
We know that for any $a, b \in \mathbb{F}_p^\times$ there exist $y = a^2, z = b^2 \in S$. Then because $\mathbb{F}_p^\times$ is cyclic and hence abelian,

$$yz = a^2b^2 = (ab)^2 \in S$$

for some $ab \in \mathbb{F}_p^\times$.
Similarly, for any $a, \bar{a} \in \mathbb{F}_p^\times$, where $a \cdot \bar{a} = 1$, by definition there exist $y = a^2, z = \bar{a}^2 \in S$, such that,

$$yz = a^2\bar{a}^2 = (a\bar{a})^2 = 1$$

Hence, S is a subgroup. And since g is a $2:1$ mapping, $|\mathbb{F}_p^\times|/|S| = 2$, i.e. S is an index 2 subgroup of $\mathbb{F}_p^\times$.

Problem 2. Reducibility of $x^4 + 1$ modulo primes.
The goal is to prove that $f(x) = x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime number p. You already know (HW#1) that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

1. Factor $f(x)$ modulo 2.
2. Assume that $-1 = u^2$ is a square in $\mathbb{F}_p$. Then use the equality
$$x^4 + 1 = x^4 - u^2$$
to factor $f(x)$ modulo p.
3. Assume that p is odd and $2 = v^2$ is a square in $\mathbb{F}_p$. Then use the equality
$$x^4 + 1 = (x^2 + 1)^2 - (vx)^2$$
to factor $f(x)$ modulo p.
4. Prove that if p is odd and neither -1 nor 2 is a square in $\mathbb{F}_p$, then -2 is a square. In this case, factor $f(x)$ modulo any such p. *Hint.* For the first part, use the previous problem.
5. Conclude that $x^4 + 1$ is reducible modulo every prime p.

Solution.

1. $x^4 + 1 \pmod 2 \equiv (x^2 + 1)^2 \pmod 2$
2. In $\mathbb{F}_p[x]$, $u^2 = -1$,
$$x^4 + 1 = x^4 = u^2 = (x^2 + u)(x^2 - u)$$
3. In $\mathbb{F}_p[x]$, $v^2 = 2$,
$$x^4 + 1 = (x^2 + 1)^2 - (vx)^2 = (x^2 + 1 + vx)(x^2 + 1 - vx)$$
4. From problem 1.3 we know that for finite fields F, $F^\times$ is cyclic. Let g be the generator for the field $\mathbb{F}_p^\times$, where p is some odd prime.

   Claim: For all even powers k, g^k must be a square.

   Proof: Let $k = 2i$ for some i. Consider $g^k \in \mathbb{F}_p^\times$,
$$g^k = g^{2i} = g^{i+i} = g^i \cdot g^i$$
   It follows that g^k is a square in $\mathbb{F}_p^\times$ with square root g^i.

Let $g^i = -1 \pmod p$, $g^j = 2 \pmod p$ is not a square for some powers i, j. We know that i, j are both odd from the claim above; then $i + j$ would be even, and $g^{i+j} = 2 \cdot (-1) = -2$ is a square in $F^\times$.

In $\mathbb{F}_p[x]$, $w^2 = -2$,

$$x^4 + 1 = (x^2 - 1)^2 - (wx)^2 = (x^2 - 1 + wx)(x^2 - 1 - wx)$$

5. To see if $f(x)$ is reducible modulo every prime p, we check the following 2 cases,

   (a) $p = 2$: from subpart (1) we know that $f(x)$ is reducible modulo 2.

   (b) $p \neq 2$: from subpart (4) we see that for all odd primes, one of -1, 2, or -2 must be a square in $\mathbb{F}_p^\times$. And we know $f(x)$ is factorable modulo p in all three cases (subparts (2),(3),(4)).

   Therefore, $f(x)$ is reducible modulo every prime p.

Problem 3. Field homomorphisms.
Let K and K' be field extensions of a field F.

1. Prove that any F-homomorphism $\varphi : K \to K'$ is injective.
2. Prove that if K'/F is finite and $\varphi : K \to K'$ is an F-homomorphism, then K/F is finite.
3. Assume that both K and K' are finite over F, and that $\varphi : K \to K'$ is an F-homomorphism. Prove that φ is an F-isomorphism if and only if $[K : F] = [K' : F]$.
4. Prove that $f(x) = x^2 - 4x + 2 \in \mathbb{Q}[x]$ is irreducible. Prove that the extensions

$$K = \mathbb{Q}[x]/(f(x)) \quad \text{and} \quad \mathbb{Q}(\sqrt{2})$$

of $\mathbb{Q}$ are $\mathbb{Q}$-isomorphic and exhibit an explicit $\mathbb{Q}$-isomorphism between them.

Solution.

1. An F-homomorphism $\varphi : K \to K'$ is a homomorphism such that $\varphi(x) = x, \forall x \in F$. Moreover, the kernel of the F-homomorphism $\varphi : K \to K'$ is an ideal of K. But since K is a field, it only has two ideals (0) and K, and because by definition elements in $F \in K$ are mapped to non-zero elements in K', the kernel must be the zero ideal.

   Since the kernel is zero, the F-homomorphism is injective.

2. Assume $[K' : F] < \infty$, and $\varphi : K \to K'$ is an F-homomorphism. From subpart (1) we know that φ must be injective. Then by rank-nulity, we know that

$$\dim(K) = \dim(\ker\varphi) + \dim(\mathrm{im}\varphi) \leq \dim(K')$$

   Since, the kernel is trivial, $\dim(K) = \dim(\mathrm{im}\varphi) \leq \dim(K')$. Hence, if K' is finite dimensional, K must be too, i.e. $[K : F] < \infty$.

3. Assume $[K : F]$, $[K' : F] < \infty$, and $\varphi : K \to K'$ is an F-homomorphism.

   $(\implies)$

   Assume φ is an F-isomorphism. An F-isomorphism is in particular is a bijective linear map. Which means that K and K' have the same dimension. That is, $[K : F] = [K' : F]$.

   $(\impliedby)$

   Assume $[K : F] = [K' : F]$, that is $\dim(K) = \dim(K')$. We already know (from subpart (1)) that any F-homomorphism $\varphi : K \to K'$ is injective. Thus $\varphi(K)$ is an F-subspace of K' with

$$\dim(\varphi(K)) = \dim(K) = [K : F].$$

Since $[K:F] = [K':F] = \dim(K')$, it follows that $\varphi(K) = K'$. Therefore φ is surjective. Hence φ is both injective and surjective, and therefore an F-isomorphism.

4. Using the rational root test, we know that $f(x) = x^2 - 4x + 2$ has the folowing possible roots $\frac{p}{q} \in \mathbb{Q}$: $p = \{\pm 1, \pm 2\}$, $q = \{\pm 1\}$, that is $\frac{p}{q} = \{\pm 1, \pm 2\}$. Checking if any of these roots satisfy $f(x)$,

$$\begin{aligned} f(1) &= 1 - 4 + 2 = -1 \neq 0 \\ f(-1) &= 1 + 4 + 2 = 7 \neq 0 \\ f(2) &= 4 - 8 + 2 = -2 \neq 0 \\ f(-2) &= 4 + 8 + 2 = 14 \neq 0 \end{aligned}$$

None of them do. Since $f(x)$ is quadratic and has no rational roots it is irreducible in $\mathbb{Q}[x]$.

$K = \mathbb{Q}[x]/(f(x)) = \mathbb{Q}[x]/(x^2 - 4x + 2)$. The degree of the field extension K, is equal to the degree of the minimal polynomial.

$$[K : \mathbb{Q}[x]] = 2$$

That is, the dimension of K as a $\mathbb{Q}$ vector space is 2. The dimension of $\mathbb{Q}[\sqrt{2}]$ as a $\mathbb{Q}$ vector space is also 2. That is, $[Q[\sqrt{2}] : \mathbb{Q}] = [K : \mathbb{Q}] = 2$. Define an F-homomorphism $\varphi : K \to \mathbb{Q}[\sqrt{2}]$. From subpart (3), we know that any F-homomorphism between field extensions of the same degree is a F-isomorphism. Hence, the fields are $\mathbb{Q}$-isomorphic.

$$K \cong \mathbb{Q}[\sqrt{2}]$$

Let $\alpha \in K$ be a root to $f(x)$.

$$\alpha^2 - 4\alpha + 2 = 0 \implies (\alpha - 2)^2 = 2$$

Thus,

$$K = \mathbb{Q}(\alpha)$$

Define φ specifically to be, $\varphi(x) = 2 + \sqrt{2}$. Since

$$(2 + \sqrt{2})^2 - 4(2 + \sqrt{2}) + 2 = 0$$

we have $f(2 + \sqrt{2}) = 0$, so $(f(x)) \subset \ker \varphi$.

Problem 4. Inverses in a cubic extension.
Let $\alpha \approx -1.7693$ be the real root of $x^3 - 2x + 2$. In the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$, write the elements α^{-1} and $(\alpha+1)^{-1}$ explicitly as a polynomial in α with coefficients in $\mathbb{Q}$.
Hint. Remember the algorithm using the Bézout identity (e.g. FT pp. 16–17).

Solution.

1. α^{-1}

   We know that $\alpha^3 - 2\alpha + 2 = 0$. Upon rearranging we get,

$$\begin{aligned} \alpha^3 - 2\alpha &= -2 \\ \frac{-1}{2}(\alpha^3 - 2\alpha) &= 1 \\ \alpha\left(\frac{-1}{2}(\alpha^2 - 2)\right) &= 1 \end{aligned}$$

   $\implies \alpha^{-1} = \left(\frac{-1}{2}(\alpha^2 - 2)\right)$.

2. $(\alpha+1)^{-1}$

   From the original equation we get that,

$$\alpha + 1 = x^3 - x + 3$$

   Let $f(x) = x^3 - 2x + 2$, $g(x) = x^3 - x + 3$. We can see that $f(x) \nmid g(x)$ and $g(x) \nmid f(x)$. We use Euclid's Extended Algorithm to obtain both the gcd and bezout's coefficients,

$$\begin{aligned} f(x) &= (1)g(x) - x - 1 \\ g(x) &= (-x^2 + x)(-x - 1) + 3 \\ (-x - 1) &= \left(\frac{-1}{3}(x+1)\right)3 \end{aligned}$$

   Working backwards,

$$\begin{aligned} 3 &= g(x) - (-x^2 + x)(-x - 1) \\ &= g(x) - (-x^2 + x)(f(x) - g(x)) \\ &= g(x) + x^2 f(x) - x f(x) - x^2 g(x) + x g(x) \\ &= f(x)(x^2 - x) + g(x)(1 - x^2 + x) \\ 1 &= \frac{1}{3}(x^2 - x)f(x) + \frac{1}{3}(-x^2 + x + 1)g(x) \\ 1 &= \frac{1}{3}(x^2 - x)(x^3 - 2x + 2) + \frac{1}{3}(-x^2 + x + 1)(x^3 - x + 3) \end{aligned}$$

Substituting α in we get,

$$1 = 0 + \frac{1}{3}(-\alpha^2 + \alpha + 1)(\alpha^3 - \alpha + 3)$$
$$1 = \frac{1}{3}(-\alpha^2 + \alpha + 1)(\alpha + 1)$$

The inverse of $(\alpha + 1)$ is $\frac{1}{3}(-\alpha^2 + \alpha + 1)$.

Problem 5. Quadratic extensions.
Let F be a field of characteristic $\neq 2$ and let K/F be a field extension of degree 2.

1. Prove that there exists $\alpha \in K$ with $\alpha^2 \in F$ such that $K = F(\alpha)$. We often write $\alpha = \sqrt{a}$ if $\alpha^2 = a \in F$. *Hint.* Get inspiration from the quadratic formula.

2. For $a, b \in F^\times$ prove that $F(\sqrt{a}) \cong F(\sqrt{b})$ if and only if $a = u^2 b$ for some $u \in F^\times$.

3. Deduce that there is a bijection between the set of F-isomorphism classes of field extensions K/F with $[K : F] \mid 2$ and the group $F^\times/F^{\times 2}$.

4. If F is a finite field of characteristic $\neq 2$, prove that F has a unique quadratic extension (up to F-isomorphism).

Solution.

1. Since K/F is a degree two field extension, the minimal polynomial for this extension is some monic quadratic, say $f(x) = x^2 + bx + c$. It suffices to adjoin the discriminant of the polynomial to get the field extension. $K = F(\sqrt{b^2 - 4c})$, where $b, c \in F$ that is, $b^2 - 4c \in F$.

2. $(\implies)$
If $F(\sqrt{a}) \cong F(\sqrt{b})$, then there exists a F-isomorphism $\varphi : F(\sqrt{a}) \to F(\sqrt{b})$. Since φ fixes F, and the following property holds:
$$\varphi(a) = \varphi(\sqrt{a}\sqrt{a}) = \varphi(\sqrt{a})\varphi(\sqrt{a}) = a$$
$\varphi(\sqrt{a})$ is a squareroot of $\varphi(a) \in F(\sqrt{b})$. Every element in $F(\sqrt{b})$ can be written as $x + y\sqrt{b}$ for some $x, y \in F$. Then,
$$\varphi(\sqrt{a}) = x + y\sqrt{b} \implies (\varphi(\sqrt{a}))^2 = x^2 + 2xy\sqrt{b} + y^2 b$$
Since, $(\varphi(\sqrt{a}))^2$ is a perfect square in $F(\sqrt{b})$, $\quad 2xy\sqrt{b}$ must be 0. Since, F is not characteristic 2, either $x = 0$ or $y = 0$. If $y = 0$, then
$$(\varphi(\sqrt{a}))^2 = x^2 \implies a = x^2$$
But $a, x \in F$, and φ fixes F. So this is not possible. x must be zero.
$$(\varphi(\sqrt{a}))^2 = \varphi(a) = y^2 b = a$$
Swapping y with u we get,
$$(\varphi(\sqrt{a}))^2 = \varphi(a) = u^2 b = a$$

Hence, if $F(\sqrt{a}) \cong F(\sqrt{b})$ then $a = u^2 b$, for some $u \in F^\times$.

$(\Longleftarrow)$

Assume $a = u^2 b$, where $a, b, u \in F^\times$. Since, $F(\sqrt{a}), F(\sqrt{b})$ are degree two extensions, they are 2-dimensional F-vector spaces with bases

$$\{1, \sqrt{a}\} \quad \text{and} \quad \{1, u\sqrt{b}\},$$

respectively. We can define an F-linear map

$$\varphi : F(\sqrt{a}) \to F(\sqrt{b})$$

by sending bases to bases:

$$\varphi(1) = 1, \qquad \varphi(\sqrt{a}) = u\sqrt{b}$$

By linearity, for $x, y \in F$,

$$\varphi(x + y\sqrt{a}) = x + yu\sqrt{b}$$

Since φ sends basis to basis, the two extensions are isomorphic as F-vector spaces. It remains to check if φ preserves multiplication:

$$\varphi(a) = \varphi(\sqrt{a}\sqrt{a}) = \varphi(\sqrt{a})\varphi(\sqrt{a}) = (u\sqrt{b})^2 = u^2 b = a$$

And since φ fixes F, $\forall x, y \in F(\sqrt{a})$,

$$\varphi(xy) = \varphi(x)\varphi(y)$$

It holds! Hence, φ is an F-algebra isomorphism:

$$F(\sqrt{a}) \cong F(\sqrt{b})$$

3. For each $a \in F^\times$, let $K_a = F(\sqrt{a})$. Since we are adjoining a square root, the extension K_a/F has degree at most 2. Thus every field extension K/F with $[K : F] \mid 2$ is either equal to F or of the form $F(\sqrt{a})$ for some $a \in F^\times$. Thus every such extension is represented by some $a \in F^\times$.

   From subpart (2), we know that for any $a, b \in F^\times$,

   $$F(\sqrt{a}) \cong F(\sqrt{b}) \quad \Longleftrightarrow \quad a = u^2 b \text{ for some } u \in F^\times.$$

   That is, $F(\sqrt{a})$ and $F(\sqrt{b})$ are F-isomorphic if and only if a and b represent the same element of the quotient group $F^\times/F^{\times 2}$. Therefore assigning each such extension to it's represtative class in the quotinent group $F^\times/F^{\times 2}$, defines a bijection between the set of F-isomorphism classes of field extensions K/F with $[K : F] \mid 2$ and the group $F^\times/F^{\times 2}$

4. From Problem (1.5) we know that in finite fields, the set of non-zero squares forms an index 2 subgroup of $F^\times$. That is, $F^\times/F^{\times 2}$ has two cosets. Moreover from subpart (4) we know that there exists a bijection between the set of F-isomorphism classes of field extensions K/F with $[K : F] \mid 2$ and the group $F^\times/F^{\times 2}$. The coset corresponding to the squares maps to the trivial extension F/F, and the other one maps to K/F where $K = F(\sqrt{a})$ for some a in the coset. Hence, there exists a unique quadratic extension for F upto isomorphism.

Problem 6. Minimal polynomials.
For each extension K/F and each element $\alpha \in K$, find the minimal polynomial of α over F (and prove that it is the minimal polynomial).

1. i in $\mathbb{C}/\mathbb{R}$
2. i in $\mathbb{C}/\mathbb{Q}$
3. $\dfrac{1+\sqrt{5}}{2}$ in $\mathbb{R}/\mathbb{Q}$
4. $\sqrt{2}+\sqrt{2}$ in $\mathbb{R}/\mathbb{Q}$

Solution.

1. i in $\mathbb{C}/\mathbb{R}$

   Minimal Polynomial: $f(x) = x^2 + 1$.

   To prove that $f(x)$ is the minimal polynomial, we first check that i satisfies it, then check if the degree of the extension and the degree of the polynomial match, and then check that it is irreducible over $\mathbb{R}$.

   (a) $i^2 + 1 = (-1) + 1 = 0$. Hence, i satisfies $f(x)$.

   (b) The basis of $\mathbb{C}$ over $\mathbb{R}$ is $\{1, i\}$, so $[\mathbb{C} : \mathbb{R}] = 2$. And the degree of the polynomial is also 2. Hence, the degrees match.

   (c) Assume $f(x)$ is reducible over $\mathbb{R}$, then there exist $a, b \in \mathbb{R}$ such that $x^2 + 1 = (x-a)(x-b)$. This implies a, b are roots, and $a^2 = -1$. But since, no real numbers have negative squares, this is not possible. Hence, a contradiction! $f(x)$ is irreducible over $\mathbb{R}$.

   Thus, $f(x) = x^2 + 1$ is the minimal polynomial of i in $\mathbb{C}/\mathbb{R}$.

2. i in $\mathbb{C}/\mathbb{Q}$

   Minimal Polynomial: $f(x) = x^2 + 1$.

   Since $\sqrt{-1} \notin \mathbb{Q}$, there are no rational numbers $\frac{a}{b}$ that satisfy $i - \frac{a}{b} = 0$. Hence, the minimal polynomial cannot have degree 1. So, it must be of degree 2 or more. $f(x)$ is a degree two irreducible polynomial with no rational roots, and hence must be the minimal polynomial.

3. $\dfrac{1+\sqrt{5}}{2}$ in $\mathbb{R}/\mathbb{Q}$

   Minimal Polynomial: $f(x) = x^2 - x - 1$.

To prove that $f(x)$ is the minimal polynomial, we first check that $\left(\frac{1+\sqrt{5}}{2}\right)$ satisfies it, then check if the degree of the minimal extension of $\mathbb{Q}$ such that it contains $\left(\frac{1+\sqrt{5}}{2}\right)$ and the degree of the polynomial match, and then check that it is irreducible over $\mathbb{Q}$.

(a) $\left(\dfrac{1+\sqrt{5}}{2}\right)^2 - \dfrac{1+\sqrt{5}}{2} - 1 = 0$. Hence, $\left(\dfrac{1+\sqrt{5}}{2}\right)$ satisfies $f(x)$.

(b) The basis of $\mathbb{Q}[\sqrt{5}]$ over $\mathbb{Q}$ is $\{1, \sqrt{5}\}$, so $[\mathbb{Q}[\sqrt{5}] : \mathbb{Q}] = 2$. And the degree of the polynomial is also 2. Hence, the degrees match.

(c) By the rational root test, the only possible roots are ± 1. We check to see if either satisfy $f(x)$:

$$f(1) = 1 - 1 - 1 = -2, \qquad f(-1) = 1 - (-1) - 1 = -1$$

Neither do. So, $f(x)$ is irreducible over $\mathbb{Q}$.

Thus, $f(x) = x^2 - x - 1$ is the minimal polynomial of $\left(\dfrac{1+\sqrt{5}}{2}\right)$ in $\mathbb{R}/\mathbb{Q}$.

4. $\sqrt{2} + \sqrt{2}$ in $\mathbb{R}/\mathbb{Q}$

Minimal Polynomial: $f(x) = x^2 - 8$.

To prove that $f(x)$ is the minimal polynomial, we first check that $(\sqrt{2} + \sqrt{2})$ satisfies it, then check if the degree of the minimal extension of $\mathbb{Q}$ such that it contains $(\sqrt{2} + \sqrt{2})$ and the degree of the polynomial match, and then check that it is irreducible over $\mathbb{Q}$.

(a) $(\sqrt{2} + \sqrt{2})^2 - 8 = 2 + 2\sqrt{2}\sqrt{2} + 2 - 8 = 0$. Hence, $(\sqrt{2} + \sqrt{2})$ satisfies $f(x)$.

(b) The basis of $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$ is $\{1, \sqrt{2}\}$, so $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. And the degree of the polynomial is also 2. Hence, the degrees match.

(c) By the rational root test, the possible values for roots $\frac{p}{q} \in \mathbb{Q}$ are $p \in \{\pm 1, \pm 2, \pm 4, \pm 8\}$ and $q \in \{\pm 1\}$, i.e., $\frac{p}{q} \in \{\pm 1, \pm 2, \pm 4, \pm 8\}$. We check if any of these are roots to $f(x)$:

$$\begin{aligned}
f(1) &= 1^2 - 8 = -7 \neq 0 \\
f(-1) &= 1^2 - 8 = -7 \neq 0 \\
f(2) &= 2^2 - 8 = -4 \neq 0, \\
f(-2) &= (-2)^2 - 8 = -4 \neq 0, \\
f(4) &= 4^2 - 8 = 8 \neq 0, \\
f(-4) &= (-4)^2 - 8 = 8 \neq 0, \\
f(8) &= 8^2 - 8 = 56 \neq 0.
\end{aligned}$$

None of them do. So, $f(x)$ is irreducible over $\mathbb{Q}$.

Thus, $f(x) = x^2 - 8$ is the minimal polynomial of $(\sqrt{2} + \sqrt{2})$ in $\mathbb{R}/\mathbb{Q}$.

Problem 7. Transcendental and algebraic extensions.
Let $\pi \in \mathbb{R}$ be the area of a unit circle and let $\alpha = \sqrt{\pi^2 + 2}$. Consider the field $K = \mathbb{Q}(\pi, \alpha)$.
For the following field extensions, determine whether they are transcendental and/or algebraic and/or finite and/or simple, and if you determine the extension is simple and algebraic, find a simple generator and determine its minimal polynomial.

1. $K/\mathbb{Q}$
2. $K/\mathbb{Q}(\pi)$
3. $K/\mathbb{Q}(\alpha)$
4. $K/\mathbb{Q}(\pi + \alpha)$

Solution.

1. $K/\mathbb{Q}$ - Transcendental, Infinite, and Simple.

   Consider the element $\pi + \alpha \in K$. Trivially, $\mathbb{Q}[\pi + \alpha] \subset \mathbb{Q}[\pi, \alpha]$. To show the opposite containment we check,

$$\begin{aligned}(\pi + \alpha)^2 &= \pi^2 + \alpha^2 + 2\pi\alpha \\ &= \pi^2 + \pi^2 + 2 + 2\pi\left(\sqrt{\pi^2 + 2}\right) \\ &= 2\pi\left(\pi + \left(\sqrt{\pi^2 + 2}\right)\right) + 2 \\ &= 2\pi\,(\pi + \alpha) + 2\end{aligned}$$

$$\pi = ((\pi + \alpha)^2 - 2)/(2(\pi + \alpha)), \qquad \alpha = (\pi + \alpha) - \pi$$

$$\implies Q[\pi + \alpha] \supset \mathbb{Q}[\pi, \alpha] \implies K = \mathbb{Q}(\pi, \alpha) = \mathbb{Q}(\pi + \alpha)$$

   Hence, $\mathbb{Q}[\pi, \alpha]$ is a simple extension.

   The extension is transcendental over $\mathbb{Q}$ because π satisfies no polynomials in $\mathbb{Q}[x]$. And as all powers of π are linearly independent over $\mathbb{Q}$, the extension is infinite over $\mathbb{Q}$.

2. $K/\mathbb{Q}(\pi)$ - Algebraic, Finite, and Simple.

   (a) $K = (\mathbb{Q}(\pi))(\alpha)$ with generator α
   (b) Minimal polynomial: $f(x) = x^2 - \pi^2 - 2$

   Since, the degree of the minimal polynomial is 2, the extension also has degree 2 and hence is finite.

3. $\mathsf{K}/\mathbb{Q}(\alpha)$ - Algebraic, Finite, and Simple

   (a) $\mathsf{K} = (\mathbb{Q}(\alpha))(\pi)$ with generator π

   (b) Minimal polynomial: $f(x) = x^2 - \alpha + 2$

   Since, the degree of the minimal polynomial is 2, the extension also has degree 2 and hence is finite.

4. $\mathsf{K}/\mathbb{Q}(\pi + \alpha)$ - Algebraic, Finite, and Simple

   (a) $\mathsf{K} = (\mathbb{Q}(\pi + \alpha))(67)$ with generator 67

   (b) Minimal polynomial: $f(x) = x - 67$

   Since, the degree of the minimal polynomial is 1, the extension also has degree 1 and hence is finite.