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, $m||G|$ there exists a subgroup H of G with order m. Since any H would have at most m elements of order dividing m, there are at most m elements in G with order dividing m.

   ($\impliedby$)

   Assume group G has at most m elements of order dividing m for each $m||G|$. **TODO:**

2. Let G be a finite subgroup of the multiplicative group $F^{\times}$. Then,

3.

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 $4 \bigm| |\mathbb{F}_p^{\times}| \implies 4 \mid p{-}1 \implies p \equiv 1 \pmod 4$.

($\impliedby$)
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.

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.

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

1. Prove that any F-homomorphism $\varphi : \mathsf{K} \to \mathsf{K}'$ is injective.

2. Prove that if K'/F is finite and $\varphi : \mathsf{K} \to \mathsf{K}'$ is an F-homomorphism, then K/F is finite.

3. Assume that both K and K' are finite over F, and that $\varphi : \mathsf{K} \to \mathsf{K}'$ is an F-homomorphism. Then φ is an F-isomorphism if and only if $[\mathsf{K} : \mathsf{F}] = [\mathsf{K}' : \mathsf{F}]$.

4. Prove that $f(x) = x^2 - 4x + 2 \in \mathbb{Q}[x]$ is irreducible. Prove that the extensions

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

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

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).

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

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

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

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

Problem 6. Minimal polynomials.
For each extension K/F and each element $\alpha \in \mathsf{K}$, 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 $\mathbb{R}/\mathbb{Q}$

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. $K/\mathbb{Q}(\pi+\alpha)$