

PS1

Sasha Redden

January 16, 2026

1. Let $p \in \mathbb{N}$ be a prime. Consider $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1 \in \mathbb{Q}[x]$. our goal is to prove that $\Phi_p(x)$ is irreducible.
 - (a) Show that $\Phi_p(x)$ is irreducible if and only if $\Phi_p(x+1)$ is irreducible.
 - (b) Prove that $\Phi_p(x+1)$ is irreducible using Eisenstien's criterion. Hint: use $\Phi_p(x)(x-1) = x^p - 1$.
 - (c) Let $\zeta_p = e^{2\pi i/p}$. Prove that $\mathbb{Q}(\zeta_p) \cong \mathbb{Q}[x]/\langle \Phi_p \rangle$.
 - (d) Prove that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a degree $p-1$ extension and that it contains all the p th roots of 1.

- (a) Consider the ring homomorphism $\varphi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[x+1]$ defined by $\varphi(f(x)) = f(x+1)$, this is a ring isomorphism because for any $f(x), g(x) \in \mathbb{Q}[x]$, $\varphi(f(x)g(x)) = f(x+1)g(x+1) = \varphi(f(x))\varphi(g(x))$, $\varphi(f(x)+g(x)) = f(x+1)+g(x+1) = \varphi(f(x))+\varphi(g(x))$, and for any $f(x+1) \in \mathbb{Q}[x+1]$, $\varphi^{-1}(f(x+1)) = f(x)$. Assume Φ_p is irreducible, then $\Phi_p(x) = F(x)G(x)$ for some $F(x), G(x) \in \mathbb{Q}[x]$ which have degree smaller than the degree of $f(x)$, then

$$\varphi(\Phi_p(x)) = \Phi_p(x+1) = F(x+1)G(x+1)$$

So $\Phi_p(x+1)$ is irreducible. Since φ is an isomorphism, by the same reasoning we have $\Phi_p(x)$ is irreducible if $\Phi_p(x+1)$ is irreducible.

- (b) $\varphi(\Phi_p(x)(x-1)) = \Phi_p(x+1)(x) = (x+1)^p - 1$. Using binomial theorem to expand the polynomial:

$$(x+1)^p - 1 = \sum_{k=0}^p \binom{p}{k} x^k - 1 = 1 + \frac{p!}{(p-1)!}x + \frac{p!}{2(p-2)!}x^2 + \cdots + x^p - 1$$

The 1's cancel and we obtain $px + \frac{p(p-1)}{2}x^2 + \cdots + x^p$, so dividing be zero we get that $\Phi_p(x+1) = p + \frac{p(p-1)}{2}x + \frac{p(p-1)(p-2)}{6}x^2 + \cdots + x^{p-1}$, so $n = p-1$, $p \nmid a_n = 1$, $p|a_i = \binom{p}{i}$, $i = 0, \dots, n-1$, $p^2 \nmid a_0 = p$ so Eisenstiens criterion is satisfied and thus $\Phi_p(x+1)$ is irreducible.

- (c) From b) and a) we can deduce that $\Phi_p(x) = \frac{x^p-1}{x-1}$ is irreducible and also that $\Phi_p(\zeta_p) = \frac{(e^{2\pi i/p})^p-1}{e^{2\pi i/p}-1} = 0$ so $\Phi_p(x)$ is the minimal polynomial for ζ_p and thus $\mathbb{Q}(\zeta_p) \cong \mathbb{Q}[x]/\langle \Phi_p(x) \rangle$.

- (d) $\deg(\Phi_p(x)) = p-1$ so $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a degree $p-1$ extension and $\{(\zeta_p)^k : k = 0, \dots, p-1\} \subset \mathbb{Q}(\zeta_p)$, so it contains all the p th roots of 1.
2. Let $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$.
- (a) Prove that f is irreducible by showing that it has no roots.
 - (b) Let $F = \mathbb{F}_2[x]/\langle f \rangle$. Prove that F is a field with 4 elements.
 - (c) Consider F as an abelian group under addition. What is its structure?
 - (d) Prove that there exists a field with 8 elements.
- (a) $\mathbb{F}_2 = \{0, 1\}$. We have $f(0) = 1$ and $f(1) = 1 + 1 + 1 = 1$ so these are not roots and thus the polynomial f is irreducible in $\mathbb{F}_2$.
- (b) Since f is irreducible, $\langle f \rangle$ is a maximal ideal and thus F is a field. We know that $\bar{0} \in F$ and $\bar{1} \in F$ and since $\deg(f) = 2$ and from a theorem we saw in class, if we let $\theta = \bar{x}$ then $\{1, \theta, \theta^2\}$ is a basis for F (as a $\mathbb{F}_2$ vector space) so $F = \{\bar{0}, \bar{1}, \theta, \theta + 1\}$ because since $x^2 = x + 1$ we can always reduce polynomials with degree higher than 1 to one represented one of the 4 elements in F .
- (c) If we consider F as an abelian group under addition, it must have the same structure as $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$, but $1 + 1 = 0$ so it will not generate F . Construct a map from $\mathbb{Z}_2 \times \mathbb{Z}_2$ to F : $(0, 0) \rightarrow 0, (1, 1) \rightarrow 1, (1, 0) \rightarrow \theta, (0, 1) \rightarrow (\theta + 1)$ we can deduce that the structure of F as an abelian group under addition is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.
- (d) Let $\theta = \bar{x}$, then $F' = \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle = \{0, 1, \theta, \theta + 1, \theta^2, \theta^2 + 1, \theta^2 + \theta, \theta^2 + \theta + 1\}$
3. Let F be a field. The **characteristic** of F is the smallest p such that $1 + \dots + 1 = 0$ (where there are p ones). If there is no such n , then we say that F has characteristic 0. Last semester we showed that p is prime.
- (a) Suppose that F has characteristic 0. Prove that F contains a copy of $\mathbb{Q}$.
 - (b) Suppose that F has characteristic $p \neq 0$. Prove that F contains a copy of $\mathbb{F}_p$.
 - (c) Suppose that F has finitely many elements. Prove that $|F| = p^n$ for some prime p and some natural number n .
- (a) We can construct an injective homomorphism $\varphi : \mathbb{Z} \rightarrow F$ described by $\varphi(1) = 1$, similar to PS8 Q3 from last semester. Then we can extend this homomorphism to $\mathbb{Q}$, $\phi : \mathbb{Q} \rightarrow F$ described by $\phi(\frac{a}{b}) = \frac{\varphi(a)}{\varphi(b)} = \frac{a \cdot (1)}{b \cdot (1)} = a \cdot (1) \cdot \frac{1}{b \cdot (1)}$, where $a \cdot (1)$ is the element obtained from summing a ones in F , and since F is a field, $\frac{1}{b \cdot (1)}$ exists for any b and ϕ is an injective homomorphism, thus F contains a copy of $\mathbb{Q}$, namely $\phi(\mathbb{Q})$.
- (b) Consider homomorphism $\varphi : \mathbb{F}_2 \rightarrow F$ described by $\varphi(1) = 1$, then $\varphi(0) = \varphi(p) = p \cdot (1) = 0$ as desired and φ is a homomorphism between fields so it is injective and thus F contains a copy of $\mathbb{F}_2$.

- (c) F is finite so it must have characteristic $p \neq 0$, and we know that p is prime. We can construct a sub field of F , K , such that F is a K vector space. Let $[F : K] = n$ and any element $f \in F$ can be written as a linear combination of $k_1, \dots, k_n \in K$ and basis elements $f_1, \dots, f_k \in f$ s.t. $f = k_1 f_1 + \dots + k_n f_n$. Each k_i has p choices, so over the n basis elements there is exactly p^n choices for each unique $f \in F$, so thus $|F| = p^n$ for some p prime and some $n \in \mathbb{N}$.
4. Find the minimal polynomial over $\mathbb{Q}$ of $\sqrt{2} + \sqrt{3}$. (You should verify that the polynomial you obtain is irreducible.) Prove that $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
The inclusion $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is obvious. To show the other inclusion:

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

so $\sqrt{2} + \sqrt{3} + \sqrt{3} - \sqrt{2} = 2\sqrt{3}$ so $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and $\sqrt{2} + \sqrt{3} - \sqrt{3} + \sqrt{2} = 2\sqrt{2}$ so $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Tower theorem tells us that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. We know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $x^2 - 2$ and $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ because that is the dimension of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a $\mathbb{Q}(\sqrt{2})$ vector space. so $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$ and then 4 is the degree of the minimal polynomial. Consider $f(x) = x^4 - 10x^2 + 1$, $f(\sqrt{2} + \sqrt{3}) = (5 + 2\sqrt{6})^2 - 10(5 + 2\sqrt{6}) + 1 = 49 + 20\sqrt{6} - 50 - 20\sqrt{6} + 1 = 0$, so $f(x)$ is the minimal polynomial and thus irreducible.

5. Let K be a field and suppose that $[K(c) : K]$ is odd. Prove that $K(c^2) = K(c)$.
We already have the inclusion $K(c^2) \subset K(c)$ so now we must show that $K(c) \subset K(c^2)$. Lets suppose that $K(c^2) \neq K(c)$, then $[K(c) : K(c^2)] \neq 1$. Tower theorem tells us that $[K(c) : K] = [K(c) : K(c^2)][K(c^2) : K]$ is odd, and $c^2 - x^2 \in K(c)[x]$ so the minimal polynomial m_c has to have degree 2 because we assumed it was not 1. This implies that $2 \mid [K(c) : K]$ which is a contradiction, so we must have $K(c^2) = K(c)$.