

1. The polynomial $x^2 + 1$ is irreducible over \mathbb{F}_3 . Thus $\mathbb{F}_9 \cong \mathbb{F}_3[x] / (x^2 + 1)$.
 Let θ be a root of $x^2 + 1$, for example $\theta := x + (x^2 + 1)$.

\mathbb{F}_9^* is cyclic of order 8, $\phi(8) = 4$ elements are generators, i.e. primitive roots.

We have $\theta^2 = -1$, $\theta^3 = -\theta$ and $\theta^4 = 1$ thus θ has order 4.

That is, all other elements of \mathbb{F}_9^* are primitive roots: $\{\theta + 1, \theta + 2, 2\theta + 1, 2\theta + 2\}$

Take $\theta + 1$, we get its conjugates by repeatedly powering up to exponent 3:

$$(\theta + 1)^3 = \theta^3 + 1 = \theta(\theta^2) + 1 = \theta(-1) + 1 = 2\theta + 1$$

Thus, the conjugates of $\theta + 1$ are $\{\theta + 1, 2\theta + 1\}$, all are primitive roots.

2. Let $\varphi: \mathbb{C} \rightarrow \mathbb{C}$ be an automorphism of \mathbb{C} which fixes \mathbb{R} elementwise.

Then since $x^2 + 1 = (x + i)(x - i) = x^2 + (i + (-i))x + (i) \cdot (-i)$ we see that φ permutes the set $\{i, -i\}$, here we have extended φ to a ring automorphism of $\mathbb{C}[x]$ by applying it to all coefficients of a polynomial.

Another proof: Let $\alpha \in \mathbb{C}$ be $\varphi(i)$. Since $-i = (-1) \cdot i$ we have

$$\varphi(-i) = \varphi(-1) \cdot \varphi(i) = -1 \cdot \alpha = -\alpha. \quad \text{Since } \varphi(i \cdot (-i)) = \alpha \cdot (-\alpha) = -\alpha^2$$

we have $\alpha \in \{i, -i\}$. Because $\{1, i\}$ is a basis of \mathbb{C} as \mathbb{R} -vector space, both proofs show that there is exactly two such automorphisms:

- ① the identity
- ② complex conjugation $i \mapsto -i$

3. Assume $\alpha = \gamma^q - \gamma = \beta^q - \beta$ with $\beta, \gamma \in F \Rightarrow \beta^q - \gamma^q = (\beta - \gamma)^q = \beta - \gamma$
 and thus $\beta - \gamma \in K = \mathbb{F}_q$.

$$\text{Assume } \beta - \gamma \in \mathbb{F}_q \Rightarrow (\beta - \gamma)^q = \beta^q - \gamma^q = \beta - \gamma \Rightarrow \alpha = \beta^q - \beta = \gamma^q - \gamma.$$

4. $N_{F/K}(\alpha) = \alpha^{\frac{q^m - 1}{q - 1}}$

If $\alpha = \beta^{q-1}$ for some $\beta \in F$ then $N_{F/K}(\alpha) = \alpha^{\frac{q^m - 1}{q - 1}} = \beta^{q^m - 1} = 1$.

~~Let $N_{F/K}(\alpha) = 1$, that is: $\alpha \cdot \alpha^q \cdot \alpha^{q^2} \cdots \alpha^{q^{m-1}} = 1 \Rightarrow \alpha =$~~

$N_{F/K}$ is a surjective group hom. from F^* to K^* , both are cyclic groups of orders $q^m - 1$ and $q - 1$ respectively. Let γ be a primitive root of F^* then $N_{F/K}(\gamma)$ is a primitive root of K^* since $N_{F/K}$ is surjective. Thus γ^{q-1} generates the kernel, $\langle \gamma^{q-1} \rangle$ is the subgroup

of elements of F^* which are $(q-1)$ -st powers.

5. There are $q^m - 1$ possible values for the first vector b_1 in a basis (has to be $\neq 0$). The second must not lie in the \mathbb{F}_q -span of b_1 , thus for every b_1 there are $q^m - q$ choices for the second basis vector b_2 . For the i -th basis vector to be linearly independent from the first $i-1$ vectors, it must not lie in their \mathbb{F}_q -span. That leaves $q^m - q^{i-1}$ choices for b_i for every choice of (b_1, \dots, b_{i-1}) . The result follows.

NOTE: A vector space of dimension k over \mathbb{F}_q has q^k elements.