1. (1) *Sol.* The normal field extension is an algebraic field extension $K \subset L$ such that for any irreducible polynomial $f(x) \in K[x]$ that has a root in L, $f(x)$ splits in L.

   (2) *Proof.* We assume first that $K \subset L$ is a finite normal extension. Then $L = K(a_1, a_2, ..., a_n)$ for some $a_1, ..., a_n \in L$. Let $f_i \in K[x]$ be the minimal polynomial for a_i $(i = 1, 2, ..., n)$. f_i exists since L is an algebraic extension. Consider the polynomial $f = f_1 f_2 \cdots f_n \in K[x]$. By the definition of normal extension, f_i splits in L. So f splits in L. Let R be the set of all the roots of f in L. Then we have

$$L = K(a_1, ..., a_n) \subset K(R) \subset L.$$

   Thus $L = K(R)$, which shows that L is the splitting field of $f \in K[x]$.

   Next we assume that $K \subset L$ is a finite splitting field for $f \in K[x]$. Let $g \in K[x]$ be an arbitrary polynomial such that g has a root α in L. We want to show that g splits in L. Let $h = fg \in K[x]$ and M be the splitting field of h. Since h splits in M, it can be written as the product of linear factors with coefficients in M. Then f, g can also be written in this way since $K[x]$ is a unique factorization domain, which shows that both f and g split in M. Considering f, there exists a K-homomorphism ϕ from L to M, which satisfies $\phi(L) = \phi(K)(\alpha, a_2, ..., a_n) = K(\alpha, a_2, ..., a_n) = L$ where $a_i \in L$ are the roots of f. Considering g, let $\beta \neq \alpha$ be another root of g in M (if g has only one root α, then we are done). So we just need to show that β is in L.

   By the extension lemma, there exists a ring isomorphism j from $K(\alpha)$ to $K(\beta)$, which satisfies $j(k) = k$ for any $k \in K$ and $j(\alpha) = \beta$. Regard $K(\beta)$ as a subfield of M, we can write $j : K(\alpha) \to M$. Note that L is the splitting field of $f \in K(\alpha)[x]$. To see that, the splitting field of f, regarded as a polynomial in $K(\alpha)[x]$, is $K(\alpha)(\alpha, a_2, ..., a_n) = K(\alpha, a_2, ..., a_n) = L$. Now that L is a splitting field of $K(\alpha)$, we can extend $j : K(\alpha) \to M$ to $\tilde{\phi} : L \to M$ be the extension lemma. Again by the extension lemma, $\phi = \tilde{\phi}$. So $\tilde{\phi}(L) = \phi(L) = L$, and $\beta = \tilde{\phi}(\alpha) \in L$. □

2. *Sol.*
$$\begin{aligned}x^9 - x =& x(x^8-1)\\ =& x(x^4+1)(x^2+1)(x+1)(x-1)\\ =& x(x+1)(x+2)(x^2+1)(x^4+4x^2+4-4x^2)\\ =& x(x+1)(x+2)(x^2+1)(x^2+2x+2)(x^2-2x+2).\end{aligned}$$
$$\begin{aligned}x^{27} - x =& x(x^{26}-1)\\ =& x(x^{13}+1)(x^{13}-1)\\ =& x(x+1)(x+2)(x^{12}+\cdots+x+1)(x^{12}-\cdots-x+1)\\ =& x(x+1)(x+2)(x^3-x+1)(x^3-x-1)(x^3+x^2-1)(x^3-x^2+1)\\ & (x^3+x^2+x-1)(x^3+x^2-x+1)(x^3-x^2+x+1)(x^3-x^2-x-1).\end{aligned}$$

3. *Sol.* $x^5+x+1 = (x^2+x+1)(x^3+x^2+1)$. Considering 0 and 1, both of the factors are nonzero. So they are irreducible. Thus we have $x^5+x+1 | x^{2^6}-x$ since $2|6$ and $3|6$. Note that 6 is the least common multiple of 2 and 3, so the splitting field of $x^{2^6}-x \in \mathbb{F}_2[x]$ is exactly the splitting field for $x^5+x+1 \in \mathbb{F}_2[x]$. Therefore L is the splitting field of $x^{2^6}-x \in \mathbb{F}_2[x]$, which is isomorphic to $\mathbb{F}_{2^6}$. And $|L : \mathbb{F}_2| = 6$, L has $2^6 = 64$ elements.

4. (1) *Sol.* Generators of $\mathbb{F}_{11}^*$ are $\{2, 6, 7, 8\}$.

   (2) *Sol.* The product is 10!. By Wilson's theorem, $10! \equiv -1 \equiv 10 \pmod{11}$. So the product is 10.

   (3) *Sol.* The product of all elements in $\mathbb{F}_p^*$ is $p-1$. $\mathbb{F}_p^* = \{1, 2, ..., p-1\}$. For each $i \in \{2, ..., p-2\}$, there exists a unique $a_i \in \{2, ..., p-2\}$ such that $i \cdot a_i = 1$. To see that, consider the set
$$\{i, 2i, ..., (p-2)i, (p-1)i\}.$$
   It is a complete residue system for p. Otherwise if $mi \equiv ni \pmod{p}$ for some $m \neq n \in \mathbb{F}_p^*$, then $p|(m-n)i$, which is impossible. Thus such a_i exists, and obviously not equal to 1 or $p-1$. In this way, we partition $\{2, ..., p-2\}$ into $\frac{p-3}{2}$ pairs, and in the form (i, a_i). Therefore
$$(p-1)! = 1 \cdot (p-1) \cdot 1^{(p-3)/2} = p-1.$$

5. *Proof.* Let F be a finite field of even order. Since the order must be of

the form p^k for a prime number p and a positive integer k, we have $p = 2$. The order of F then becomes 2^k. Since F is finite, $F^* = F \setminus \{0\}$ is a cyclic multiplicative group. Assume that $F^* = \langle a \rangle$. Then for any $b \in F^*$, $b = a^n$ for some $0 \neq n \neq 2^k - 2$. If n is even, then $b = (a^{n/2})^2$. If n is odd, then $b = (a^{(n+2^k-1)/2})^2$. And for 0, $0 = 0^2$. Therefore every element is a square. $\square$

6. *Proof.* Obviously, $\mathrm{Aut}_K(L) \subset \mathrm{Aut}(L)$. So it suffices to show that for any $\phi \in \mathrm{Aut}(L)$, we have $\phi(k) = k$ for any $k \in K$. Note that K is the subfield generated by $\{1\}$, so $\phi(k) = \phi(m \cdot 1) = m\phi(1) = m \cdot 1 = k$ for some positive integer m. $\square$

7. *Proof.* Since $K \subset L$ is a finite Galois extension, $|\mathrm{Aut}_K(L)| = |L : K|$. By tower theorem, $|L : K| = |L : K(\alpha)||K(\alpha) : K| = |L : K(\alpha)| \cdot \deg(p) \geq \deg(p)$. So we have $|\mathrm{Aut}_K(L)| \geq \deg(p)$. $\square$