Chapter 8: Fields, Section 2: Multiplicity of Roots

1. *Proof.* Let F be the extension field for $p(x)$ over K. Since K is finite, it is perfect, and the roots for $p(x)$, which is irreducible, are all simple. We have shown that all roots of irreducible factors are simple, so $[F : K] = n$, implying the Galois group is $\mathbb{Z}_n$ (since we have a simple extension of a finite field). □

2. *Solution.* We can verify that $x^4 - 2$ has not roots in $\mathbb{F}_3$. Therefore it is irreducible. Since it is over a finite field, from Problem (1), the Galois group is $\boxed{\mathbb{Z}_4}$. □

3. *Solution.* $x = 1, -1$ are roots. We have $x^4 + 2 = (x - 1)(x + 1)(x^2 + 1)$. Since $(x^2 + 1)$ is irreducible, the Galois group is $\boxed{\mathbb{Z}_2}$. □

4. *Solution.* We can factor $x^6 - 1(x - 1)(x + 1)(x - 3)(x + 2)(x - 3)(x + 1)$. So the splitting field is $\mathbb{F}_7$, and the galois group is $\boxed{\{1\}}$. □

5. *Proof.* Let M be the splitting field of F. Then we have that for any polynomial $f(x) \in F[x]$ has factorization $h(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \in M[x]$. Since F is algebraic over K, we can represent $f(x)$ as a (possibly longer) polynomial $g(x) \in K[x]$. We have that $f(x) \mid g(x)$, since f's roots are at least g's roots. Since K is perfect, the irreducible factors in K only have simple roots. Since $f(x) \mid g(x)$, the irreducible factors in $f(x)$ also only have simple roots, and F is perfect. □

6. *Proof.* Consider the minimal polynomial of any $\alpha \in F$: $g(x) \in K[x]$, and $f(x) \in E[x]$. When we split these polynomials in the splitting field of F, g's roots are at least f's roots, so $f(x) \mid g(x)$. Since F is separable over K, $g(x)$ only has simple roots, and therefore $f(x)$ does too. So F is separable over E. □

7. *Proof.* Let $f, g \in K[x]$ for some field K. Let $t = \max\{\deg(f(x)), \deg(g(x))\}$, and define the polynomials as $f(x) = \sum_{k=0}^{t} a_k x^k$, $g(x) = \sum_{k=0}^{t} b_k x^k$.

$$\begin{aligned} f(x) \cdot g'(x) + f'(x) \cdot g(x) &= \sum_{k_1=0}^{t} \sum_{k_2=0}^{t} k_2 a_{k_1} b_{k_2} x^{k_1+k_2-1} + \sum_{k_1=0}^{t} \sum_{k_2=0}^{t} k_1 a_{k_1} b_{k_2} x^{k_1+k_2-1} \\ &= \sum_{k_1=0}^{t} \sum_{k_2=0}^{t} k_2 a_{k_1} b_{k_2} x^{k_1+k_2-1} + k_1 a_{k_1} b_{k_2} x^{k_1+k_2-1} \\ &= \sum_{k_1=0}^{t} \sum_{k_2=0}^{t} (k_1 + k_2) a_{k_1} b_{k_2} x^{k_1+k_2-1} \\ &= (f \cdot g)'(x). \end{aligned}$$

□

8. *Solution.* By Theorem (8.2.8), we first find the minimal polynomial for each adjoined element, $x^2 - 2$ and $x^2 + 1$. We want to find a number $a \in \mathbb{Q}$ such that

- $\sqrt{2} + ai \neq \sqrt{2} - ai$,
- $\sqrt{2} + ai \neq -\sqrt{2} - ai$.

$a = 1$ works. So the primitive element is $\sqrt{2} + ai = \boxed{\sqrt{2} + i}$. □

	$x^3 - 1$	$x^3 - 2$
Important roots	$u_i = 1, \omega, \omega^2$	$v_j = \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$

Table 1: Roots to consider for $u + av \neq u_i + av_j$

9. *Solution.* Let $u = \omega$, $v = \sqrt[3]{2}$. The roots we have to consider are the ones for $x^3 - 1$ and $x^3 - 2$, and are shown in table 1. We can see that $a = 1$ works here as well, so the primitive element is $\omega + a\sqrt[3]{2} = \boxed{\omega + \sqrt[3]{2}}$. □

10. *Proof.* Suppose some roots of f are in $\mathbb{C} \setminus \mathbb{R}$ for contraposition. Then F is a field extension of $\mathbb{Q}(i)$ as well. But then by multiplication of orders,
$$[F : \mathbb{Q}] = [F : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2[F : \mathbb{Q}(i)].$$
So $[F : \mathbb{Q}]$ is even. □

11. *Proof.* Suppose that $x = y^p$ for $y \in K(x)$. Then
$$\begin{aligned} y^p x^{-1} &= 1 \\ p \cdot y^p x^{-1} &= 0 \\ y^p &= 0 = x. \end{aligned}$$
Which is nonsensical. □

12. *Proof.* Let $f(x) = x^p - a$. If $\exists \alpha \in F$ s.t. $\alpha^p = a$, we have
$$x^p - a = x^p - \alpha^p = (x - \alpha)^p.$$
Showing that it is a pth power.

If α does not exist, let the splitting field of f be K. In other words, $\exists \beta \in K \setminus F$ such that $\beta^p = a$. Therefore in $K[x]$,
$$f(x) = (x - \beta)^p.$$
Since gcd is invariant under an extension field, we see that $\gcd(f(x), f'(x)) = (x - \beta)^{p-1}$. So $(x - \beta)^{p-1} \in F[x]$. Then
$$((x - \beta)^{p-1})^{-1}(x - \beta)^p = (x - \beta) \in F[x],$$
contradicting our assumption that $\beta \notin F$. □

If I've made any errors or you have any other comments on these solutions, message me on Mathstodon.

Notation

- I write the Galois Field $\mathrm{GF}(p^n)$ as $\mathbb{F}_{p^n}$.