Solution 17

Fixed subfield

1. Let E/k be a splitting field of $X^n - 1 \in k[X]$ and $\Gamma_n(E)$ the subgroup of $E^\times$ of n-th roots of unity. Show that

   (a) If $\mathrm{char}(k) = 0$, then $|\Gamma_n(E)| = n$.

   (b) If $\mathrm{char}(k) = p$, and $n = p^\ell m$ with $p \nmid m$, then $|\Gamma_n(E)| = m$.

   Solution: Let $f = X^n - 1$.

   (a) Suppose that $\mathrm{char}(k) = 0$. Then $f' = nX^{n-1} \neq 0$ so that each irreducible factor of f' is X (up to a multiplicative constant in $k^\times$). But $X \nmid f$, so that $\gcd(f, f') = 1$ and f has no multiple roots. Since all roots of f are in E, $|\Gamma_n(E)| = n$.

   (b) Suppose that $\mathrm{char}(k) = p$ and write $n = p^\ell m$ with $p \nmid m$. Notice that, since $\mathrm{char}(k) = p$,
   $$(X^m - 1)^p = X^{mp} - 1$$
   and iterating this process we obtain
   $$(X^m - 1)^{p^\ell} = X^{mp^\ell} - 1 = X^n - 1.$$
   Then $f = g^{p^\ell}$ for $g = X^m - 1$ and the roots of f coincide with the roots of g. Now, we see that $g' = mX^{m-1} \neq 0$ and the same reasoning done in part (a) tells us that $\gcd(g, g') = 1$, so that $|\Gamma_n(E)| = |R(g)| = m$.

2. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Recall that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. List all subgroups of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and for each subgroup H determine the subfield E^H.

   Solution: By Assignment 16, Exercise 3, the Galois groups of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ consists of the four elements $\mathrm{id}, \sigma_2, \sigma_3, \sigma_2 \circ \sigma_3$ where σ_2 maps $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{3} \mapsto -\sqrt{3}$, while σ_3 maps $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{3} \mapsto -\sqrt{3}$. Notice that $\sqrt{6} = \sqrt{2} \cdot \sqrt{3}$, so that it changes sign under the action of σ_2 and σ_3 and it is fixed by $\sigma_2 \circ \sigma_3$.

   The subgroups of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ are given by $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ itself, $\langle \sigma_2 \rangle$, $\langle \sigma_3 \rangle$, $\langle \sigma_2 \circ \sigma_3 \rangle$ and $\{\mathrm{id}\}$.

   A $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is seen to be given by $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. Hence, writing a general element $x \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ as $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, we can see when it is fixed by an element of the Galois group:

- id fixes all $x \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$;
- $\sigma_2(x) = \sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \stackrel{!}{=} x$ if and only if $b = d = 0$, that is, $x \in \mathbb{Q}(\sqrt{3})$;
- $\sigma_3(x) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \stackrel{!}{=} x$ if and only if $c = d = 0$, that is, $x \in \mathbb{Q}(\sqrt{2})$;
- $\sigma_2 \circ \sigma_3(x) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6} \stackrel{!}{=} x$ if and only if $b = c = 0$, that is, $x \in \mathbb{Q}(\sqrt{6})$.

Putting all this together, we see that

- $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\{\mathrm{id}\}} = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})$;
- $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \sigma_2 \rangle} = \mathbb{Q}(\sqrt{3})$;
- $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \sigma_3 \rangle} = \mathbb{Q}(\sqrt{2})$;
- $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \sigma_2 \circ \sigma_3 \rangle} = \mathbb{Q}(\sqrt{6})$.
- $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})} = \mathbb{Q}$.

3. Let p be a prime number and let $m \geqslant 1$. Prove that the field extension $\mathbb{F}_{p^m}/\mathbb{F}_p$ is Galois and calculate its Galois group.

   Hint. Frobenius automorphism.

   Solution: Set $q := p^m$. Recall that the Frobenius map $\mathrm{Frob}_p\colon \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^p$ is an $\mathbb{F}_p$-linear endomorphism. If $x^p = y^p$, then $0 = x^p - y^p = (x - y)^p$, hence $x = y$, so Frob_p is injective. Since it is an injective linear map from a finite-dimensional vector space to itself, it is surjective, so it is an automorphism. Its fixed field is the subfield of roots of $x^p - x$, which are precisely the p distinct elements of the base field $\mathbb{F}_p$. Its order in $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$ is precisely m, since $x^{p^r} = x$ is true for all $x \in \mathbb{F}_q$ if and only if $r \geqslant m$. From the lecture we know that

   $$[\mathbb{F}_q/\mathbb{F}_p] \geqslant |\{\mathrm{Frob}_p, \mathrm{Frob}_{p^2} = \mathrm{Frob}_p \circ \mathrm{Frob}_p, \ldots, \mathrm{Frob}_{p^{m-1}}, \mathrm{Frob}_{p^m} = \mathrm{id}_{\mathbb{F}_{p^m}}\}| = m.$$

   On the other hand, we have $[\mathbb{F}_q/\mathbb{F}_p] = m$ because $q = p^m$. It follows that $\mathbb{F}_q$ is Galois with Galois group the cyclic group generated by Frob_p.