Solution 22

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 $p > 2$ be a prime number and $\zeta := e^{\frac{2\pi i}{p}}$. Let $E = \mathbb{Q}(\zeta)$. Recall that $\mathrm{Gal}(E/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

   (a) Show that there exists a unique subgroup H of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ of order 2. What is its generator? [*Hint:* It is an element of order 2]

   (b) Prove that $\mathbb{Q}(\zeta + \zeta^{-1}) \subseteq E^H$ and that $[E : \mathbb{Q}(\zeta + \zeta^{-1})] \leqslant 2$.

   (c) Deduce that $E^H = \mathbb{Q}(\zeta + \zeta^{-1})$.

   Solution: By Assignment 16, Exercise 2, an isomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is given by $k + p\mathbb{Z} \mapsto (\zeta \mapsto \zeta^k)$ for each $k \in \mathbb{Z}$. Recall that an automorphism of $\mathbb{Q}(\zeta)$ (fixing $\mathbb{Q}$) is indeed uniquely determined by the image of ζ, which in turn needs to be another root of $\mathrm{irr}(\zeta, \mathbb{Q}) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$.

   (a) By Algebra I, we know that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$ because $\mathbb{Z}/p\mathbb{Z}$ is a finite field. $p - 1$ is divisible by 2 since p is odd. Hence $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ has a unique subgroup of order 2. It is generated by the $\frac{p-1}{2}$-th power of a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Only one element $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ can have order 2, because two distinct such elements generate distinct subgroups of order 2.

   We also know that complex conjugation $\sigma : x \mapsto \overline{x}$ belongs to $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ which clearly has order 2, so that $H = \langle \sigma \rangle$.

   (b) As $|\zeta| = 1$, we see that $\zeta^{-1} = \overline{\zeta}$, so that σ actually corresponds to the class of $-1 \in (\mathbb{Z}/p\mathbb{Z})^\times$.

   At any rate,

$$\sigma(\zeta + \zeta^{-1}) = \sigma(\zeta) + \sigma(\zeta^{-1}) = \zeta^{-1} + \zeta,$$

so that $\zeta + \zeta^{-1} \in E^H$. As E^H is a subfield of E, we can conclude that $\mathbb{Q}(\zeta + \zeta^{-1}) \subset E$.

Notice that ζ is a root of $(X - \zeta)(X - \zeta^{-1}) = X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[X]$, so that $[E : \mathbb{Q}(\zeta + \zeta^{-1}] \leqslant 2$.

(c) By Proposition IV.9, $[E : E^H] = |H| = 2$. Hence we know that

$$2 \cdot [E^H : \mathbb{Q}(\zeta + \zeta^{-1})] = [E : \mathbb{Q}(\zeta + \zeta^{-1})] \leqslant 2$$

so that $[E^H : \mathbb{Q}(\zeta + \zeta^{-1})] = 1$, meaning that $E^H = \mathbb{Q}(\zeta + \zeta^{-1})$.