Prof. Marc Burger

Solution 24

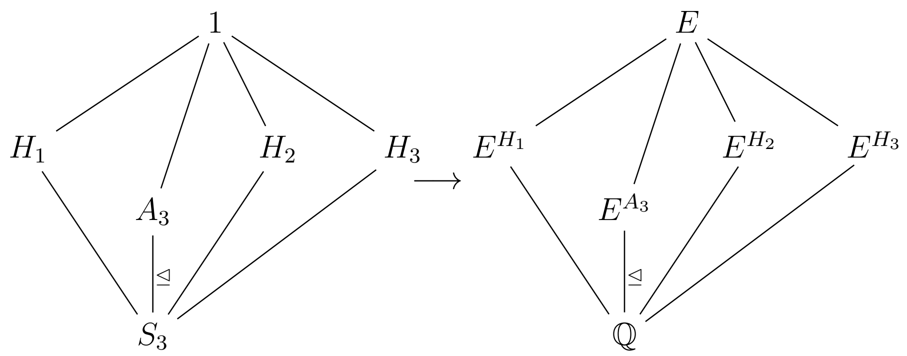
Symmetric functions. Galois correspondence.

1. Let $f = X^3 - 2 \in \mathbb{Q}[X]$ and consider its splitting field E. Recall that $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$. Write down the lattice of subgroups of S_3 and the corresponding fixed fields. Which of those are normal?

   Solution: The polynomial f has roots $z_1 = \sqrt[3]{2}$, $z_2 = \sqrt[3]{2}\omega$ and $z_3 = \sqrt[3]{2}\omega^2$, for $\omega = e^{\frac{2\pi i}{3}}$. The identification $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$ is given by $\sigma(z_i) = z_{\sigma(i)}$ for $\sigma \in S_3$. One can determine the image of ω under σ as

$$\sigma(\omega) = \frac{\sigma(z_2)}{\sigma(z_1)} = \frac{z_{\sigma(2)}}{z_{\sigma(1)}} = \omega^{\sigma(2)-\sigma(1)}.$$

   The subgroups of S_3 are given by 1, S_3 itself, $A_3 = \langle (1\ 2\ 3) \rangle$ and the three non-normal subgroups $H_i = \langle (j\ \ k) \rangle$ for each choice of $\{i, j, k\} = \{1, 2, 3\}$. The only containments are given by $1 \leqslant H_i \leqslant S_3$ and $1 \leqslant A_3 \trianglelefteq S_3$.



   By construction, we see that H_i fixes z_i for each $i \in \{1, 2, 3\}$, so that $\mathbb{Q}(z_i) \subset E^{H_i}$. Since $[E : \mathbb{Q}(z_i)] = 2 = |H_i| = [E : E^{H_i}]$, we can conclude that $E^{H_i} = \mathbb{Q}(z_i)$.

   According to the correspondence, the only intermediate Galois extension is given by $E^{A_3}/\mathbb{Q}$, which is also the unique extension of degree 2. Since $\mathbb{Q}(\omega)/\mathbb{Q}$ is a degree-2 field extension (the minimal polynomial of ω being $X^2 + X + 1 \in \mathbb{Q}[X]$), we must have $E^{A_3} = \mathbb{Q}(\omega)$. One could also directly check that A_3 fixes ω (and conclude by comparing the degrees of the extensions), if for $\tau = (1\ 2\ 3)$, a generator of A_3, one computes

$$\tau(\omega) = \omega^{\tau(2)-\tau(1)} = \omega^{3-2} = \omega.$$

2. Let k be a field with $\mathrm{char}(k) \neq 2$ and $n \geqslant 5$ an integer. Consider the field extension

$$E = k(Y_1, \dots, Y_n)/k(e_1, \dots, e_n) = K,$$

where $e_j \in k[Y_1, \dots, Y_n]$ is, for each integer $1 \leqslant j \leqslant n$, the j-th elementary symmetric polynomial, so that $\mathrm{Gal}(E/K) = S_n$. Let $E/L/K$ be the unique intermediate non-trivial Galois extension. Find a polynomial $f \in K[X]$ whose splitting field is L/K. [*Hint:* What is $\mathrm{Gal}(E/L)$? And $\deg(f)$?]

Solution: Let $H = \mathrm{Gal}(E/L)$. By Galois correspondence $L = E^H$ and $H \trianglelefteq S_n$ with $H \neq 1$ and $H \neq S_n$. Then $H \cap A_n \trianglelefteq A_n$, which is a simple group as $n \geqslant 5$, so that either $H \cap A_n = A_n$ or $H \cap A_n = 1$. In the first case, $A_n \leqslant H \leqslant G$ and since $2 = [S_n : A_n] = [S_n : H][H : A_n]$ we can conclude that either $H = A_n$ or $H = S_n$. In the second case, notice that $A_n \lhd HA_n \lhd S_n$, so that either $H = 1$ or $HA_n = S_n$ (because HA_n is properly bigger than A_n). In the latter situation, by the second isomorphism theorem for groups (or by the proof of Assignment 8, Exercise 5(b)) we conclude that $|H| = 2$, so that H contains the identity and a product of an odd number of disjoint 2-cycles. In particular, H is not normal in S_n in this case, as there are other permutations of same cycle type in S_n. The only valid possibility is $\mathrm{Gal}(E/L) = H = A_n$.

Hence $L = E^{A_n}$, so that $[E : L] = |A_n|$ and $[L : K] = |S_n|/|A_n| = 2$. Hence L/K a quadratic extension, so that it can be the splitting field of $f \in K[X]$ only if $\deg(f) = 2$.

Getting inspired by Exercise 3, we define $\Delta(f) = \prod_{i<j}(Y_i - Y_j) \in E$ and notice that $\sigma(\Delta(f)) = \mathrm{sgn}(\sigma)\Delta(f)$ for each $\sigma \in S_n$. This implies that $\Delta(f) \in E^{A_n} = L \setminus K$ and that $D(f) := \Delta(f)^2 \in K$ (since $\mathrm{char}(K) = 2$, so that $\mathrm{sgn}(\sigma) = 1$ if and only if $\sigma \in A_n$). Hence $f = X^2 - \prod_{i<j}(Y_i - Y_j)^2$ does the job.

3. Let k be a field and $f \in k[X]$ a polynomial with distinct roots and $E = \mathrm{Sf}(f)$. Write $R(f) = \{z_1, \dots, z_n\}$ to fix an embedding $\mathrm{Gal}(E/k) \subset S_n$. Define the discriminant of f as

$$D(f) = \prod_{i<j}(z_i - z_j)^2.$$

(a) Assume that $\mathrm{char}(k) \neq 2$. Prove that $D(f)$ is a square in k if and only if $\mathrm{Gal}(E/k) \subset A_n$.

(b) Show that $\mathbb{F}_4/\mathbb{F}_2$ is a counterexample in characteristic 2 to the previous part.

Solution:

(a) Let $\Delta(f) = \prod_{i<j}(z_i - z_j)$. The square roots of $D(f)$ in E are given by $\pm\Delta(f)$, so that $D(f)$ is a square in k if and only if $\Delta(f) \in k$. For $\sigma \in \mathrm{Gal}(E/k)$, we have $\sigma(\Delta(f)) = \mathrm{sgn}(\sigma)\Delta(f)$ (since the z_i's are distinct) so that $\Delta(f)$ is fixed by σ if and only if $\sigma \in A_n$ (because $\mathrm{char}(K) \neq 2$).

Since E/k is Galois, $\Delta(f)$ lies in k if and only if it is fixed by all $\sigma \in \mathrm{Gal}(E/k)$, which by what we just showed is equivalent to $\mathrm{Gal}(E/k) \subset A_n$.

(b) For $k = \mathbb{F}_2$ and $E = \mathbb{F}_4$, we have $\mathrm{Gal}(E/k) = S_2 = \langle \sigma \rangle$, where σ is the Frobenius automorphism of $\mathbb{F}_4$. We can write $E = k(\alpha)$ where α is a root of $f = X^2 + X + 1 \in k[X]$, so that $E = \mathrm{Sf}(f)$. The other root of f is $\alpha + 1$. Then $\Delta(f) = (\alpha + 1) - \alpha = 1 \in \mathbb{F}_2$, so that $D(f)$ is a square in $\mathbb{F}_2$, although $\mathrm{Gal}(E/k)$ does not lie inside A_2.

4. (*Artin-Schreier theory*) Let k be a field of characteristic $p > 0$ and $c \in k$ be such that $c \neq y^p - y$ for every $y \in k$. Let $f = X^p - X - c \in k[X]$ and $E = \mathrm{Sf}(f)$.

(a) Let $x \in R(f)$. Prove that $x + \lambda \in R(f)$ for each $\lambda \in \mathbb{F}_p$.

(b) Deduce: f is irreducible, $E = k(x)$ and $\mathrm{Gal}(E/k)$ is cyclic of order p.

We know want to show that all p-cyclic field extensions in characteristic p are of this form. Let E/k be a finite Galois extension with $\mathrm{char}(k) = p$ and $\mathrm{Gal}(E/k) = \langle \sigma \rangle$ cyclic of order p.

(c) Show that there exists $x \in E$ such that $\sigma(x) = x + 1$ [*Hint:* Assignment 23, Exercise 2(c)]

(d) Prove that $E = k(x)$ and that there exists $c \in k$ such that $\mathrm{irr}(E/k) = X^p - X - c$. [*Hint:* Consider $\prod_{\lambda=0}^{p-1}(X - \sigma^\lambda(x))$. How can you prove that $x^p - x \in k$?]

Solution:

(a) For each $\lambda \in \mathbb{F}_p$, the equality $\lambda^p = \lambda$ holds. Hence

$$f(x + \lambda) = (x + \lambda)^p - (x + \lambda) - c = f(x) + \lambda^p - \lambda = 0.$$

(b) Notice that $x \notin k$, since f has no root in k by assumption. Since the $x + \lambda$ are p distinct elements for $\lambda \in \mathbb{F}_p$, the polynomial f factors as

$$f = \prod_{\lambda \in \mathbb{F}_p} (X - (x + \lambda)).$$

A factor g of f in $E[X]$ is given, up to a multiplicative constant, by taking a subset $S \subset \mathbb{F}_p$ and setting

$$g = \prod_{\lambda \in S} (X - (x + \lambda)).$$

The term of degree $|S| - 1$ of g has coefficient $(-1)^{|S|}(|S|x + \sum_{\lambda \in S} \lambda)$. As $\mathbb{F}_p \subset k$, this coefficient lies in k if and only if $|S|x \in k$, which is the case if and only $|S| = 0$ or $|S| = p$. This means that $g \in k[X]$ if and only if it is a unit or a constant multiple of f. Hence f is irreducible.

Clearly, $k(x)$ contains all the roots of f by part (a), so that $E = k(x)$. Hence $|\operatorname{Gal}(E/k)| = [E : k] = [k(x) : k] = p$ by irreducibility of f, so that $\operatorname{Gal}(E/k)$ is cyclic.

(c) By Assignment 23, Exercise 2(c), we know that the image of the k-linear endomorphism of E sending $x \mapsto \sigma(x) - x$ coincides with the kernel of the trace. But

$$T(1) = \sum_{\tau \in \operatorname{Gal}(E/k)} \tau(1) = \sum_{\tau \in \operatorname{Gal}(E/k)} 1 = p \cdot 1 = 0,$$

so that $1 \in \ker(T)$ can be expressed as $1 = \sigma(x) - x$ for some $x \in E$, as desired.

(d) The elements of $\operatorname{Gal}(E/k)$ are given by the powers σ^λ, for $\lambda \in \{0, \ldots, p-1\}$. By the previous part, $\sigma^\lambda(x) = x + \lambda$, so that the $\sigma^\lambda(x)$ are all distinct. Hence, Assignment 23, Exercise 1 tells us that

$$f := \prod_{\lambda=0}^{p-1} (X - \sigma^\lambda(x)) = \prod_{\lambda=0}^{p-1} (X - (x + \lambda)) \in E^{\operatorname{Gal}(E/k)}[X] = k[X]$$

This polynomial is seen to be irreducible in the same way as in part (b). Hence $f = \operatorname{irr}(x, k)$ and $[k(x) : k] = p = [E : k]$, which in turn implies that $k(x) = E$.

In order to conclude, let $c = x^p - x$, so that x is a root of $X^p - X - c$. In order to conclude, it is enough to show that $c \in k = E^{\operatorname{Gal}(E/k)}$, which can be done by checking that $\sigma(c) = c$, since σ is a generator of $\operatorname{Gal}(E/k)$. This is an easy computation:

$$\sigma(c) = \sigma(x^p - x) = \sigma(x)^p - \sigma(x) = (x+1)^p - (x+1) = x^p - x = c$$

5. Let L/k be a finite field extension and fix an embedding $L \subset \overline{k}$.

(a) Show: there exists a minimal normal finite field extension E/k containing L.

(b) Show: if L/k is separable, then E/k is Galois (it is called the *Galois closure of* L/k).

Solution:

(a) Since L/k is a finite extension, it is finitely generated. Write $L = k(x_1, \ldots, x_n)$ and let $f_i = \operatorname{irr}(x_i, k)$. Let $E = \operatorname{Sf}(\prod f_i)$. This is a finite normal extension of k containing L. Moreover, by Assignment 19, Exercise 4, we know that a normal extension of k containing x_i must contain all roots of $\operatorname{irr}(x_i, k)$ as well, so that E is minimal by construction.

(b) The polynomials f_i in part (a), and hence their product $\prod f_i$, are separable. Hence $E = \mathrm{Sf}(\prod f_i)$ is a Galois extension of k.

6. We say that a field extension L/k is *simple* if there exists $x \in L$ such that $L = k(x)$. In this exercise we want to prove the following result:

Lemma. A finite field extensions L/k is simple if and only if there are finitely many intermediate field extensions $L/F/k$.

(a) Suppose that $L = k(x)$ for some $x \in L$ and let $L/F/k$ be an intermediate extension. Let $f = \mathrm{irr}(x, F)$ and $F_0 \subset F$ the extension of k generated by the coefficients of f. Prove that $F = F_0$. [*Hint:* Notice that $F(x) = F_0(x)$ and compare degrees]

(b) Conclude that if L/k is simple, then it contains only finitely many intermediate subextensions [*Hint:* In part (a), f divides $\mathrm{irr}(x, k)$]

(c) Let k be an infinite field and V a k-vector space. Suppose that $V_1, \dots, V_m$ are finitely many vector subspaces of V, with $V_i \neq V$ for each i. Show that $\bigcup_{i=1}^m V_i \neq V$ [*Hint:* Induction on n]

(d) Suppose that a finite field extension L/k contains only finitely many intermediate extensions. Prove that L/k is simple.

Solution:

(a) The polynomial f is irreducible in $F[X]$, hence also in $F_0[X]$. This means that $[F(x) : F] = \deg(f) = [F_0(x) : F_0]$. But

$$L = k(x) \subset F_0(x) \subset F(x) \subset L$$

implies that $F_0(x) = F(x)$, so that

$$[F : F_0] = \frac{[F(x) : F_0]}{[F(x) : F]} = \frac{[F_0(x) : F_0]}{[F(x) : F]} = 1.$$

(b) By part (a), if $L = k(x)/F/k$ is an intermediate extension, then F is generated by the coefficients of the $\mathrm{irr}(x, F)$, which is a proper monic factor of $\mathrm{irr}(x, k)$ in $L[X]$. Since $\mathrm{irr}(x, k)$ has only finitely many proper monic factors, there are only finitely many intermediate extensions $L/F/k$.

(c) (See also Chambert-Loir, *A Field Guide to Algebra*, Lemma 3.3.4). This is proved by induction on n, the case $n = 1$ being trivial. We may suppose that $V \neq \bigcup_{i=1}^{n-1} V_i$ and take $x \in V \setminus \bigcup_{i=1}^{n-1} V_i$. If $x \notin V_n$, we are done. Else, let $y \in V \setminus V_n$. We want to prove that there exists $t \in k$ such that $x + ty \notin \bigcup_{i=1}^{n} V_i$.

Suppose that $x + ty$ and $x + t'y$ belong to the same V_i, for $t \neq t'$. Then $y \in V_i$ and $x = (x + ty) - ty \in V_i$ as well. For every i, one of those conclusions contradicts the assumptions (as $x \notin \bigcup_{i=1}^{n-1} V_i$ and $y \notin V_n$). Hence $x + ty$ belongs to V_i for at most one value of $t \in k$, implying that $x + ty \in \bigcup_{i=1}^{n-1} V_i$ for at most n values of $t \in k$. As k is infinite, there exists $t \in k$ such that $x + ty \notin \bigcup_{i=1}^{n-1} V_i$, which concludes the proof.

(d) Suppose that k is finite. Then L is finite, too. By Algebra I, we know that $L^\times$ is a cyclic group, so that for x a generator of $L^\times$, we know that $k(x)$ contains the whole $L^\times$, implying that $L = k(x)$.

From now on, we suppose that L/k is an infinite extension. Since there are only finitely many intermediate extensions, there are finitely many intermediate simple extensions L_i/k for some index $i \in I$. As each $u \in L$ lies in the simple extension $k(u)$, we know that $L = \cup_{i \in I} L_i$. Then, by part (c), we must have $L = L_i$ for some $i \in I$, so that L/k is itself a simple extension.

7. (*Primitive Element Theorem*) Let L/k be a finite separable field extension. Prove that there exists $x \in L$ such that $L = k(x)$.

Solution: By Exercise 5, L/k is contained into a finite Galois extension E/k. By the Galois correspondence, the intermediate field extensions of E/k are parametrized by the subgroups of the finite group $\mathrm{Gal}(E/k)$, so that they are finitely many. This implies that L/k has only finitely many intermediate field extensions, too. By Exercise 6, L/k is a simple field extension, that is, there exists $x \in L$ such that $L = k(x)$.

8. Prove that the field extension $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t^p)$, where s and t are formal variables, contains infinitely many intermediate extensions.

Solution: We have a tower of field extensions $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t)/\mathbb{F}_p(s^p,t^p)$. Notice that $\mathbb{F}_p(s,t) = \mathbb{F}_p(s^p,t)(s)$ and that s is a root of the polynomial $(X-s)^p = X^p - s^p \in \mathbb{F}_p(s^p,t)[X]$, which in turn is irreducible because its monic proper factors in $\mathbb{F}_p(s,t)[X]$ have constant term not lying in $\mathbb{F}_p(s^p,t)$, we obtain $[\mathbb{F}_p(s,t) : \mathbb{F}_p(s^p,t)] = p$. Similarly, we see that $X^p - t^p$ is the minimal polynomial of t over $\mathbb{F}_p(s^p,t^p)$, so that $[\mathbb{F}_p(s^p,t) : \mathbb{F}_p(s^p,t^p)] = p$. All in all we obtain

$$[\mathbb{F}_p(s,t) : \mathbb{F}_p(s^p,t^p)] = [\mathbb{F}_p(s,t) : \mathbb{F}_p(s^p,t)][\mathbb{F}_p(s^p,t) : \mathbb{F}_p(s^p,t^p)] = p^2.$$

We prove that $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t^p)$ is not simple. Suppose by contradiction that $\mathbb{F}_p(s,t) = \mathbb{F}_p(s^p,t^p)(f)$ for some $f \in \mathbb{F}_p(s,t)$. As the Frobenius map $x \mapsto x^p$ is a field endomorphism of $\mathbb{F}_p(s,t)$, we realise that $f^p \in \mathbb{F}_p(s^p,t^p)$. Hence $\mathrm{irr}(f, \mathbb{F}_p(s^p,t^p)) | X^p - f^p$, so that

$$p^2 = [\mathbb{F}_p(s,t) : \mathbb{F}_p(s^p,t^p)] = [\mathbb{F}_p(s^p,t^p)(f) : \mathbb{F}_p(s^p,t^p)] \leqslant p,$$

a contradiction. Hence $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t^p)$ is not simple.

By Exercise 6, $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t^p)$ contains infinitely many intermediate field extensions.