Galois Theory Open Door Problem Set

Invariant theory

Problem 1. Let Δ be the polynomial in $r_1, \ldots, r_n$ given by

$$\Delta = \prod_{i<j} (r_i - r_j).$$

We noticed that Δ^2 is symmetric. Compute Δ^2 as a polynomial in the elementary symmetric polynomials $e_1, e_2, \ldots, e_n$ for several values of n. What is the highest power of e_k which occurs? Any conjectures? Any other thoughts about which monomials $e_1^{d_1} \cdots e_n^{d_n}$ occur?

Problem 2. (1) Let

$$V = \det \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ r_1 & r_2 & r_3 & \cdots & r_n \\ r_1^2 & r_2^2 & r_3^2 & \cdots & r_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_1^{n-1} & r_2^{n-1} & r_3^{n-1} & \cdots & r_n^{n-1} \end{bmatrix}.$$

Show that V^2 is symmetric. Show that V/Δ is symmetric. Any conjectures about the relation between V and Δ?

(2) Let $f_1(r), f_2(r), \ldots, f_n(r)$ be any n polynomials in $\mathbb{Q}[r]$. Define $A(f_1(r),\ f_2(r),\ \cdots,\ f_n(r))$ to be the determinant of the $n \times n$ matrix whose (i,j) entry is $f_i(r_j)$, so $V = A(1, r, r^2, \ldots, r^{n-1})$. Show that $A(f_1(r), f_2(r), \ldots, f_n(r))/\Delta$ is symmetric.

(3) Choose interesting examples of polynomials $(f_1(r), \ldots, f_n(r))$ for which to compute $A(f_1(r), f_2(r), \ldots, f_n(r))/\Delta$. Some good choices are $(1, r, r^2, \ldots, r^{k-1}, r^{k+1}, \ldots, r^n)$ or $(1, r, r^2, \ldots, r^{n-2}, r^k)$ for various values of k and n. Any conjectures?

Problem 3. Let L be the field $\mathbb{C}(r_1, r_2, \ldots, r_n)$. Let F be the subfield of symmetric functions. Let $x(r_1, \ldots, r_n)$ be an element of L with stabilizer subgroup $H \subset S_n$, and let K be the field of functions in L fixed by H. In this problem, we will show that $K = F[x(r_1, \ldots, r_n)]$ and will give an explicit algorithm for taking any other function $y(r_1, \ldots, r_n)$ in K and writing it in terms of $x(r_1, \ldots, r_n)$ and symmetric functions.

So, let y be some other function stabilized by H. Let $x_1, x_2, \ldots, x_N$ be the orbit of x under S_n, with $x_1 = x$. Let $y_i = gy$ where g is chosen so that $gx = x_i$, so $y_1 = y$..

(1) Set $s_j = \sum_{i=1}^N x_i^j y_i$. Show that s_j is a symmetric function.

We thus have N linear equations in the N variables $y_1, y_2, \ldots, y_N$:

$$\begin{array}{rcccc} y_1 + & y_2 + \cdots + & y_N & = & s_0 \\ x_1 y_1 + & x_2 y_2 + \cdots + & x_N y_N & = & s_1 \\ \vdots & \vdots \ \ddots & \vdots & & \vdots \\ x_1^{N-1} y_1 + & x_2^{N-1} y_2 + \cdots + & x_N^{N-1} y_N & = & s_{N-1} \end{array}$$

(2) Show that these linear equations have a unique solution.

(3) Show that, when we solve these equations for y_1, we get a formula which is symmetric in $x_2, x_3, \ldots, x_N$ (as well as involving the symmetric functions $s_0, s_1, \ldots, s_{N-1}$).

(4) Deduce that y_1 is in $F[x_1]$.

(5) Can you adapt this argument for field extensions other that $\mathbb{C}(r_1, r_2, \ldots, r_n)$ over F?

Problem 4. Let G be a group acting on 1, 2, ..., n. Let $F \subset k(x_1, \ldots, x_n)$ be the field of rational functions which are fixed by G. Compute elements of F for many cases. Some interesting examples are:

(1) G the set of maps $j \mapsto j + b \bmod n$ for $b \in \mathbb{Z}_n$, with $k = \mathbb{C}$.
(2) G the set of maps $j \mapsto aj + b$ for $a \in U_n$ and $b \in \mathbb{Z}_n$, with $k = \mathbb{C}$.
(3) G the alternating group A_n, with $k = \mathbb{C}$.
(4) G the group of order 2 switching x_i and x_{n+1-i}, with $k = \mathbb{F}_2$.

Can F be generated by finitely many rational functions? How many? Other conjectures? Can you find an example of a group G for which the field F cannot be generated by n functions?

Cyclotomic fields

Let p be a prime integer and let ζ be a primitive p-th root of unity.

Problem 5. This problem contains some lemmas, which we will use in the other problems.

(1) (**One of many results called Gauss's Lemma**) Let $x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$ be a monic polynomial with **integer** coefficients. Suppose that $f(x)$ factors as $g(x)h(x)$ where $g(x) = x^m + g_{m-1}x^{m-1} + \cdots + g_1 x + g_0$ and $h(x) = x^{n-m} + h_{n-m-1}x^{n-m-1} + \cdots + h_1 x + h_0$ are monic polynomials with **rational** coefficients. Show that $g(x)$ and $h(x)$ have **integer** coefficients.
(2) (**Eisenstein's criterion**) Let $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$ be a monic polynomial with integer coefficients. Suppose that all the f_j are 0 mod p and that f_n is **not** divisible by p^2. Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.
(3) Show that the polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$. Hint: Substitute $x = y + 1$.
(4) Show that $\mathrm{Aut}(\mathbb{Q}[\zeta]/\mathbb{Q})$ is U_p.

For $a \in U_p$, define σ_a to be the element of $\mathrm{Aut}(\mathbb{Q}[\zeta]/\mathbb{Q})$ with $\sigma_a(\zeta) = \zeta^a$.

(5) Show that ζ, ζ^2, ..., ζ^{p-1} is a basis for $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$.
(6) We consider the subring $\mathbb{Z}[\zeta]$ of $\mathbb{Q}[\zeta]$. Show that every element of $\mathbb{Z}[\zeta]$ can be written uniquely in the form $\sum_{j=1}^{p-1} c_j \zeta^j$ for **integers** c_j, and describe how σ_a acts on this representation.

Problem 6. Define the following chain of subgroups of U_{17}:

$$G_0 = U_{17} \supset G_1 = \{\pm 1, \pm 2, \pm 4, \pm 8\} \supset G_2 = \{\pm 1, \pm 4\} \supset G_3 = \{\pm 1\} \supset G_4 = \{1\}$$

Let K_i be the subfield of $\mathbb{Q}[\zeta]$ fixed by G_i, so $K_0 \subset K_1 \subset K_2 \subset K_3 \subset K_4$.

(1) Show $K_0 = \mathbb{Q}$ and $K_3 = \mathbb{Q}(\zeta) \cap \mathbb{R}$. Can you find nice descriptions of K_1 and K_2?
(2) For $1 \leq i \leq 4$, show that every element of K_i obeys a quadratic polynomial with coefficients in K_{i-1}.
(3) Show that $\cos \frac{2\pi}{17}$ is in K_3.
(4) Give formulas for $\cos \frac{2\pi}{17}$ and $\sin \frac{2\pi}{17}$ in terms of rational numbers, $+$, $-$, $\times$, $\div$ and $\sqrt{\ }$ (no higher roots, only square roots)! This is how Gauss constructed the regular 17-gon, using only a straightedge and compass.

Problem 7. Assume that the prime p is odd.

(1) Show that $a \mapsto \left(\frac{a}{p}\right)$ from U_p to $\{\pm 1\}$ is a character.
(2) Define $\gamma_1 = \sum_{b=1}^{p-1} \left(\frac{b}{p}\right) \zeta^b$. Show that, for every $a \in U_p$, we have $\sigma_a(\gamma_1) = \left(\frac{a}{p}\right) \gamma_1$.
(3) Compute γ_1^2 for $p = 3$, 5, 7, 11, 13. Any conjectures? Can you prove them?
(4) Define $\gamma_2 = \prod_{c=1}^{(p-1)/2} (\zeta^c - \zeta^{-c})$. Show that, for every $a \in U_p$, we have $\sigma_a(\gamma_2) = \left(\frac{a}{p}\right) \gamma_2$.
(5) Compute γ_2^2 for $p = 3$, 5, 7, 11, 13. Any conjectures? Can you prove them?
(6) Compute γ_1/γ_2 for $p = 3$, 5, 7, 11, 13. Any conjectures? Can you prove them?

Problem 8. Assume that the prime p is 1 mod 4.

(1) Show that there is a **surjective** character χ from U_p to $\{1, i, -1, -i\}$.
(2) Set $\gamma = \sum_{a=1}^{p-1} \chi(a) \zeta^a$; this is in $\mathbb{Q}[i, \zeta]$. Describe how $\mathrm{Aut}(\mathbb{Q}(\zeta, i)/\mathbb{Q})$ acts on γ.
(3) Compute γ^4 for $p = 5$, 13, 17. Any conjectures? Can you prove them?

Problem 9. Let p and q be distinct odd primes.

(1) Show that, for any $\beta \in \mathbb{Z}[\zeta]$, we have $\beta^q \equiv \sigma_q(\beta) \mod q$.

Let γ be the element of $\mathbb{Z}[\zeta]$ defined by whichever of the formulas γ_1 or γ_2 in Problem 7 that you like best. In that problem, you hopefully found a formula for γ^2.

(2) Use the formula
$$\sigma_q(\gamma) = \gamma^q = (\gamma^2)^{(q-1)/2} \gamma \mod q$$
to deduce a proof of Quadratic Reciprocity.

Galois theory and factorization of polynomials modulo p

Problem 10. Factor the following polynomials modulo p for all primes up to 101. We have helpfully listed the Galois group of the splitting field. Any conjectures?

(1) $x^5 - 1$. Galois group is $U_5 \cong \mathbb{Z}_4$.
(2) $x^3 - x - 1$. Galois group is S_3.
(3) $x^4 - x - 1$. Galois group is S_4.
(4) $x^3 + x^2 - 2x - 1$. Galois group is the cyclic group of order 3.
(5) $x^4 + 4x^2 + 2$. Galois group is cyclic of order 4.
(6) $x^4 - 10x^2 + 1$. Galois group is $\mathbb{Z}_2 \times \mathbb{Z}_2$.