Example sheet 3, Galois Theory (Michaelmas 2022)

a.j.scholl@dpmms.cam.ac.uk

This sheet covers lectures 13–17 (Galois groups of polynomials, finite fields, cyclotomic and Kummer extensions)

1. (i) What are the transitive subgroups of S_4? Find a monic polynomial over $\mathbb{Z}$ of degree 4 whose Galois group is $V = \{e, (12)(34), (13)(24), (14)(23)\}$.

(ii) Let $f \in \mathbb{Z}[X]$ be monic and separable of degree n. Suppose that the Galois group of f over $\mathbb{Q}$ doesn't contain an n-cycle. Prove that the reduction of f modulo p is reducible for every prime p.

(iii) Hence exhibit an irreducible polynomial over $\mathbb{Z}$ whose reduction mod p is reducible for every p.

2. (i) Let p be prime. Show that any transitive subgroup G of S_p contains a p-cycle. Show that if G also contains a transposition then $G = S_p$.

(ii) Prove that the Galois group of $X^5 + 2X + 6$ is S_5.

(iii) Show that if $f \in \mathbb{Q}[X]$ is an irreducible polynomial of degree p which has exactly two non-real roots, then its Galois group is S_p. Deduce that for $m \in \mathbb{Z}$ sufficiently large,

$$f = X^p + mp^2(X-1)(X-2)\cdots(X-p+2) - p$$

has Galois group S_p.

3. Compute the Galois group of $X^5 - 2$ over $\mathbb{Q}$.

4. (i) Let p be an odd prime, and let $x \in \mathbb{F}_{p^n}$. Show that $x \in \mathbb{F}_p$ iff $x^p = x$, and that $x + x^{-1} \in \mathbb{F}_p$ iff either $x^p = x$ or $x^p = x^{-1}$.

(ii) Apply (i) to a root of $X^2 + 1$ in a suitable extension of $\mathbb{F}_p$ to show that that -1 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$. (You have probably seen a different proof of this fact in IB GRM.)

(iii) Show that $x^4 = -1$ iff $(x + x^{-1})^2 = 2$. Deduce that 2 is a square in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod 8$.

5. Find the Galois group of $X^4 + X^3 + 1$ over each of the finite fields $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$.

6. Let L/K be Galois with group $G = \{\sigma_1, \ldots, \sigma_n\}$. Show that $(x_1, \ldots, x_n)$ is a K-basis for L iff $\det \sigma_i(x_j) \neq 0$.

7. (i) Let $f(X) = \prod_{i=1}^n (X - x_i)$. Show that $f'(x_i) = \prod_{j \neq i}(x_i - x_j)$, and deduce that $\mathrm{Disc}(f) = (-1)^{n(n-1)/2} \prod_{i=1}^n f'(x_i)$.

(ii) Let $f(X) = X^n + bX + c = \prod_{i=1}^n (X - x_i)$, with $n \geq 2$. Show that

$$x_i f'(x_i) = (n-1)b\left(\frac{-nc}{(n-1)b} - x_i\right)$$

and deduce that

$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2}\left((1-n)^{n-1}b^n + n^n c^{n-1}\right).$$

8. Let $K = \mathbb{Q}(\zeta_n)$ be the cyclotomic field with $\zeta_n = e^{2\pi i/n}$. Show that under the isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$, complex conjugation is identified with the residue class of $-1 \pmod n$. Deduce that if $n \geqslant 3$, then $[K : K \cap \mathbb{R}] = 2$ and show that $K \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos 2\pi/n)$.

9. Find all the subfields of $\mathbb{Q}(e^{2\pi i/7})$, expressing them in the form $\mathbb{Q}(x)$.

10. Let K be a field, p a prime and $K' = K(\zeta)$ for some primitive p^{th} root of unity ζ. Let $a \in K$. Show that $X^p - a$ is irreducible over K if and only if it is irreducible over K'. Is the result true if p is not assumed to be prime?

11. Let K be a field containing a primitive m^{th} root of unity for some $m > 1$. Let $a, b \in K$ such that the polynomials $f = X^m - a$, $g = X^m - b$ are irreducible. Show that f and g have the same splitting field if and only if $b = c^m a^r$ for some $c \in K$ and $r \in \mathbb{N}$ with $\gcd(r, m) = 1$.

12. (i) Find the quadratic subfields of $\mathbb{Q}(\zeta_{15})$.

(ii) Show that $\mathbb{Q}(\zeta_{21})$ has exactly three subfields of degree 6 over $\mathbb{Q}$. Show that one of them is $\mathbb{Q}(\zeta_7)$, one is real, and the other is a cyclic extension $K/\mathbb{Q}(\zeta_3)$. Use a suitable Lagrange resolvent to find $a \in \mathbb{Q}(\zeta_3)$ such that $K = \mathbb{Q}(\zeta_3, \sqrt[3]{a})$.

The next example gives an analogue of Theorem 12.3 in characteristic p.

13. Let K be a field of characteristic $p > 0$. Let $a \in K$, and let $f \in K[X]$ be the polynomial $f(X) = X^p - X - a$. Show that $f(X + b) = f(X)$ for every $b \in \mathbb{F}_p \subset K$. Now suppose that f does not have a root in K, and let L/K be a splitting field for f over K. Show that $L = K(x)$ for any $x \in L$ with $f(x) = 0$, and that L/K is Galois, with Galois group isomorphic to $\mathbb{Z}/p\mathbb{Z}$. (L/K is called an *Artin–Schreier extension.*)

Additional examples (of varying difficulty)

14. Write $a_n(q)$ for the number of irreducible monic polynomials in $\mathbb{F}_q[X]$ of degree exactly n.

(i) Show that an irreducible polynomial $f \in \mathbb{F}_q[X]$ of degree d divides $X^{q^n} - X$ if and only if d divides n.

(ii) Deduce that $X^{q^n} - X$ is the product of all irreducible monic polynomials of degree dividing n, and that

$$\sum_{d|n} d a_d(q) = q^n.$$

(iii) Calculate the number of irreducible polynomials of degree 6 over $\mathbb{F}_2$.

(iv) If you know about the Möbius function $\mu(n)$, use the Möbius inversion formula to show that

$$a_n(q) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d.$$

15. Let $\Phi_n \in \mathbb{Z}[X]$ denote the n^{th} cyclotomic polynomial. Show that:

(i) If n is odd then $\Phi_{2n}(X) = \Phi_n(-X)$.

(ii) If p is a prime dividing n then $\Phi_{np}(X) = \Phi_n(X^p)$.

(iii) If p and q are distinct primes then the nonzero coefficients of Φ_{pq} are alternately $+1$ and -1. [Hint: First show that if $1/(1 - X^p)(1 - X^q)$ is expanded as a power series in X, then the coefficients of X^m with $m < pq$ are either 0 or 1.]

(iv) If n is not divisible by at least three distinct odd primes then the coefficients of Φ_n are -1, 0 or 1.

(v) $\Phi_{3\times5\times7}$ has at least one coefficient which is not -1, 0 or 1.