Example Sheet 3**. Galois Theory Michaelmas 2012**

Finite fields

3.1. The polyonomials $P(X) = X^3 + X + 1$, $Q(X) = X^3 + X^2 + 1$ are irreducible over $\mathbb{F}_2$. Let K be a field obtained from $\mathbb{F}_2$ by adjoining a root of P, and K' be the field obtained from $\mathbb{F}_2$ by adjoining a root of Q. Describe explicitly an isomorphism from K to K'.

3.2. Find the Galois group of $X^4 + X^3 + 1$ (that is, the Galois group of its splitting field) over each of the finite fields $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$.

3.3. Let $P \in \mathbb{F}_q[X]$ be a polynomial over a finite field. Describe the Galois group of P over $\mathbb{F}_q$ in terms of the irreducible factors of P.

Cyclotomic fields

For an integer $N \geq 1$, we denote by $K(\boldsymbol{\mu}_N)$ the N-th cyclotomic extension of K, i.e. a splitting field of $X^N - 1$ over K; when $K \subset \mathbb{C}$, we write $\zeta_N = \exp(2\pi i/N)$.

3.4. (i) Find all the subfields of $\mathbb{Q}(\boldsymbol{\mu}_7)$, expressing them in the form $\mathbb{Q}(\alpha)$. Which are Galois over $\mathbb{Q}$?

(ii) Find all the quadratic subfields of $\mathbb{Q}(\boldsymbol{\mu}_{15})$.

3.5. (i) Show that a regular 7-gon is not constructible by ruler and compass.

(ii) When the angle $2\pi/N$ is given, for which N is it possible to trisect this angle using ruler and compass? [Ruler and compass can only solve successive quadratic extensions.]

3.6. Consider $K = \mathbb{Q}(\boldsymbol{\mu}_N) \subset \mathbb{C}$. Show that under the canonical isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/(N))^\times$, the complex conjugation is identified with the residue class of $-1 \pmod N$. Deduce that if $N \geq 3$, then $[K : K \cap \mathbb{R}] = 2$ and show that $K \cap \mathbb{R} = \mathbb{Q}(\zeta_N + \zeta_N^{-1}) = \mathbb{Q}(\cos 2\pi/N)$.

3.7. Show that $\mathbb{Q}(\boldsymbol{\mu}_{21})$ has exactly three subfields of degree 6 over $\mathbb{Q}$. Show that one of them is $\mathbb{Q}(\boldsymbol{\mu}_7)$, one is real, and the other is a cyclic extension $K/\mathbb{Q}(\boldsymbol{\mu}_3)$. Use a suitable Lagrange resolvent to find $a \in \mathbb{Q}(\boldsymbol{\mu}_3)$ such that $K = \mathbb{Q}(\zeta_3, \sqrt[3]{a})$.

Function fields

3.8. (i) Let $K(X)$ be a rational function field over a field K. Let $r = p/q \in K(X)$ be a non-constant rational function. Find a polynomial in $K(r)[T]$ which has X as a root.

(ii) Let L be a subfield of $K(X)$ containing K. Show that either $K(X)/L$ is finite, or $L = K$. Deduce that the only elements of $K(X)$ which are algebraic over K are constants.

3.9. Let K be any field, and let $F = K(X)$, a rational function field over K. Define the maps $\sigma, \tau : F \to F$ by the formulae

$$\tau f(X) = f\Big(\frac{1}{X}\Big), \quad \sigma f(X) = f\Big(1 - \frac{1}{X}\Big) \quad (\forall f \in F).$$

Show that σ, τ are K-homomorphism of F, and that they generate a subgroup $G \subset \mathrm{Aut}_K(F)$ isomorphic to S_3. Show that $F^G = K(g)$, where

$$g(X) = \frac{(X^2 - X + 1)^3}{X^2(X-1)^2} \in F.$$

3.10. (i) Let L/K be an extension of degree 2. Show that if the characteristic of K is 2, then either $L = K(\alpha)$ with $\alpha^2 \in K$, or $L = K(\alpha)$ with $\alpha^2 + \alpha \in K$.

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

3.11. Let p be a prime and $F = \mathbb{F}_p(X)$, a rational function field over $\mathbb{F}_p$. Let a be an integer with $1 \le a < p$, and let $\sigma \in \mathrm{Aut}(F)$ be the unique automorphism such that $\sigma(X) = aX$. Determine the subgroup $G \subset \mathrm{Aut}(F)$ generated by σ, and its fixed field F^G.

OPTIONAL (NOT NECESSARILY HARDER)

3.12.* (i) Let p be an odd prime, and let $x \in \mathbb{F}_{p^n}^\times$. Show that $x \in \mathbb{F}_p$ if and only if $x^p = x$, and that $x + x^{-1} \in \mathbb{F}_p$ if and only if 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 $p \equiv 1 \pmod 4$.

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

3.13.* Show that the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ (cf. Problem 1.5) is reducible mod p for all primes p. (First show that for every p, one of 2, 3 or 6 is a square in $\mathbb{F}_p$.)

3.14.* Factor the polynomials: $X^9 - X \in \mathbb{F}_3[X]$, $X^{16} - X \in \mathbb{F}_4[X]$, $X^{16} - X \in \mathbb{F}_8[X]$.

3.15.* 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 $P \in \mathbb{F}_q[X]$ 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

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

3.16.* (i) Let F/K be a finite Galois extension, and H_1, H_2 subgroups of $\mathrm{Gal}(F/K)$, with fixed fields L_1, L_2. Identify the subgroup of $\mathrm{Gal}(F/K)$ corresponding to the field $L_1 \cap L_2$.

(ii) Show that the fixed field of $H_1 \cap H_2$ is the composite field (see Problem 2.12 for the definition) $L_1 L_2$ of L_1, L_2.

(iii) Show $\mathbb{Q}(\boldsymbol{\mu}_M) \cdot \mathbb{Q}(\boldsymbol{\mu}_N) = \mathbb{Q}(\boldsymbol{\mu}_{MN})$ if $M, N \geq 1$ are relatively prime.

3.17.* (i) Let $f \in K(X)$. Show that $K(X) = K(f)$ if and only if $f = (aX+b)/(cX+d)$ for some a, b, c, $d \in K$ with $ad - bc \neq 0$. (ii) Show that $\mathrm{Aut}(K(X)/K) \xrightarrow{\cong} PGL_2(K)$.

[Hint: For $f = p(X)/q(X)$, use Gauss' Lemma for $p(T) - fq(T) \in K(f)[T]$.]

3.18.* Let K be any field and $F = K(X)$ the field of rational functions over K.

(i) Show that for every $a \in K$ there is a unique $\sigma_a \in \mathrm{Aut}_K(F)$ with $\sigma_a(X) = X + a$.

(ii) Let $G = \{\sigma_a \mid a \in K\}$. Show that G is a subgroup of $\mathrm{Aut}_K(F)$, isomorphic to the additive group of K. Show that if K is infinite, then $F^G = K$.

(iii) Assume that K has characteristic $p > 0$, and let $H = \{\sigma_a \mid a \in \mathbb{F}_p\}$. Show that $F^H = K(Y)$ with $Y = X^p - X$. [See also Problem 3.10.]

More on cyclotomic fields

3.19.* (i) Let p be an odd prime. Show that if $r \in \mathbb{Z}$ then $\sum_{0 \leq s < p} \zeta_p^{rs}$ equals p if $r \equiv 0 \pmod{p}$ and equals 0 otherwise.

(ii) Let $\tau = \sum_{0 \leq n < p} \zeta_p^{n^2}$ (the **Gauss sum**). Show that $\tau\overline{\tau} = p$. Show also that τ is real if -1 is a square mod p, and otherwise τ is purely imaginary (i.e. $\tau/i \in \mathbb{R}$).

(iii) Let $F = \mathbb{Q}(\boldsymbol{\mu}_p)$. Show that F has a unique subfield K which is quadratic over $\mathbb{Q}$, and that $K = \mathbb{Q}(\sqrt{\varepsilon p})$ where $\varepsilon = (-1)^{(p-1)/2}$.

(iv) Show that $\mathbb{Q}(\boldsymbol{\mu}_M) \subset \mathbb{Q}(\boldsymbol{\mu}_N)$ if $M|N$. Deduce that if $0 \neq m \in \mathbb{Z}$ then $\mathbb{Q}(\sqrt{m})$ is a subfield of $\mathbb{Q}(\boldsymbol{\mu}_{4|m|})$. [This is a simple case of the **Kronecker-Weber Theorem**.]

3.20.* Let $\Phi_N \in \mathbb{Z}[X]$ denote the N-th cyclotomic polynomial. Show that:

(i) If N is odd and $N \neq 1$ 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) $\Phi_{3\times 5\times 7}$ has at least one coefficient which is not -1, 0 or 1.

3.21.* In this question we determine the structure of the groups $(\mathbb{Z}/(N))^\times$.

(i) Let p be an odd prime. Show that $(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n}$ for every $n \geq 2$. Deduce that $1+p$ has order p^{n-1} in $(\mathbb{Z}/(p^n))^\times$.

(ii) If $b \in \mathbb{Z}$ with $(p, b) = 1$ and b has order $p-1$ in $(\mathbb{Z}/(p))^\times$ and $n \geq 1$, show that $b^{p^{n-1}}$ has order $p-1$ in $(\mathbb{Z}/(p^n))^\times$. Deduce that $(\mathbb{Z}/(p^n))^\times$ is cyclic for $n \geq 1$ and p an odd prime.

(iii) Show that $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$ for every $n \geq 3$. Deduce that $(\mathbb{Z}/(2^n))^\times$ is generated by 5 and -1, and is isomorphic to $\mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, for any $n \geq 2$.

(iv) Use the Chinese Remainder Theorem to deduce the structure of $(\mathbb{Z}/(N))^\times$ in general.

3.22.* Use (1) the structure of $(\mathbb{Z}/(N))^\times$ (Problem 3.21), (2) the **Dirichlet's theorem on primes in arithmetic progressions**, stating that if a and b are coprime positive integers, then the set $\{an+b \mid n \in \mathbb{N}\}$ contains infinitely many primes, and (3) the structure theorem for finite abelian groups to show that every finite abelian group is isomorphic to a quotient of $(\mathbb{Z}/(N))^\times$ for suitable N.

Deduce that every finite abelian group is the Galois group of some Galois extension $K/\mathbb{Q}$. [It is a long-standing unsolved problem (**inverse Galois problem**) to show this holds for an arbitrary finite group.]

Find an explicit $\alpha \in \mathbb{C}$ for which $\mathbb{Q}(\alpha)/\mathbb{Q}$ is abelian with Galois group $\mathbb{Z}/23\mathbb{Z}$.

---

6 November, 2012

t.yoshida@dpmms.cam.ac.uk