Example sheet 4, Galois Theory (Michaelmas 2005)

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

1. Let $K = \mathbb{Q}(\zeta)$ be the n^{th} cyclotomic field with $\zeta = e^{2\pi i/n}$. 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 $K \cap \mathbb{R} = \mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\cos 2\pi/n)$.

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

3. (i) 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?

(ii) If K contains a primitive n^{th} root of unity, then we know that $X^n - a$ is reducible over K if and only if a is a d^{th} power in K for some divisor $d > 1$ of n. Show that this need not be true if K doesn't contain a primitive n^{th} root of unity.

4. 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 $\gcd(r, m) = 1$.

5. Let f be an irreducible separable quartic, and g its resolvant cubic. Show that the discriminants of f and g are equal.

6. Let $f \in \mathbb{Q}[X]$ be an irreducible quartic polynomial whose Galois group is A_4. Show that its splitting field can be written in the form $K(\sqrt{a}, \sqrt{b})$ where $K/\mathbb{Q}$ is a Galois cubic extension and a, $b \in K$.

7. (i) Show that the Galois group of $f(X) = X^5 - 4X + 2$ over $\mathbb{Q}$ is S_5, and determine its Galois group over $\mathbb{Q}(i)$.

(ii) Find the Galois group of $f(X) = X^4 - 4X + 2$ over $\mathbb{Q}$ and over $\mathbb{Q}(i)$.

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

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

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

(iii) Show that for every $n \geq 3$, $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$. Deduce that $(\mathbb{Z}/2^n\mathbb{Z})^*$ 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 $(\mathbb{Z}/m\mathbb{Z})^*$ in general.

(v) *Dirichlet's theorem on primes in arithmetic progressions* states that if a and b are coprime positive integers, then the set $\{an + b \mid n \in \mathbb{N}\}$ contains infinitely many primes. Use this, the structure theorem for finite abelian groups, and part (iv) to show that every finite abelian group is isomorphic to a quotient of $(\mathbb{Z}/m\mathbb{Z})^*$ for suitable m. Deduce that every finite abelian group is the Galois group of some Galois extension $K/\mathbb{Q}$. [It is a long-standing unsolved problem to show this holds for an arbitrary finite group.]

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

9. Here and in question 11, $\zeta_m = e^{2\pi i/m}$ for a positive integer m.

(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 $K = \mathbb{Q}(\zeta_3, \sqrt[3]{a})$.

10. 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.

Additional assorted examples (of varying difficulty)

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

(ii) Let $\tau = \sum_{0\le n<p} \zeta_p^{n^2}$. 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 $L = \mathbb{Q}(\zeta_p)$. Show that L 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 $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$ if $m|n$. Deduce that if $0 \neq m \in \mathbb{Z}$ then $\mathbb{Q}(\sqrt{m})$ is a subfield of $\mathbb{Q}(\zeta_{4|m|})$. [This is a simple case of the *Kronecker-Weber Theorem*, which says that every abelian extension of $\mathbb{Q}$ is a subfield of a suitable $\mathbb{Q}(\zeta_m)$.]

12. Show that $\mathbb{Q}(\sqrt{2+\sqrt{2+\sqrt{2}}})$ is an abelian extension of $\mathbb{Q}$, and determine its Galois group.

13. Let $L = L(x)$ where x is transcendental over K. Show that every element of $L - K$ is transcendental over K. (An extension L/K with this property is said to be *purely transcendental*.)

Suppose further that $L = K(x, y)$, where y is algebraic over K. Show that if $y \notin K$ then L/K is not a simple extension.

14. Let L/K be an infinite algebraic extension. Show that L/K is Galois if and only if $K = L^{\mathrm{Aut}(L/K)}$. [Hint: reduce to the case of a finite extension.]

15. Let k be any field, and let $L = k(X)$. Define mappings $\sigma, \tau : L \to L$ by the formulae

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

Show that σ, τ are automorphism of L, and that they generate a subgroup $G \subset \mathrm{Aut}(L)$ isomorphic to S_3. Show that $L^H = k(g(X))$ where

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