# EXAMPLE SHEET 2 (LECTURES 7–12)
# GALOIS THEORY MICHAELMAS 2009

## Fields and automorphisms

**1.** Let $K$ be a field of characteristic $p > 0$. Let $a \in K$, and let $P \in K[X]$ be the polynomial $P(X) = X^p - X - a$. 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 $L/K$ be a splitting field for $P$ over $K$. Show that $L = K(x)$ for any $x \in L$ with $P(x) = 0$, and that $L/K$ is Galois, with Galois group isomorphic to $\mathbb{Z}/p\mathbb{Z}$. (These cyclic extensions are called **Artin-Schreier extensions**.)

**2.** Let $K$ be a field and $c \in K$. If $m, n \in \mathbb{Z}_{>0}$ are coprime, show that $X^{mn} - c$ is irreducible if and only if both $X^m - c$ and $X^n - c$ are irreducible. (Use the Tower Law.)

**3.** (i) Let $x$ be algebraic over $K$. Show that there is only a finite number of intermediate fields $K \subset K' \subset K(x)$. [Hint: Consider the minimal polynomial of $x$ over $K'$.]

(ii) Show that if $L/K$ is a finite extension of infinite fields for which there exist only finitely many intermediate subfields $K \subset K' \subset L$, then $L = K(x)$ for some $x \in L$.

**4.** Let $L = \mathbb{F}_p(X, Y)$ be the field of rational functions in two variables (i.e. the field of fractions of $\mathbb{F}_p[X, Y]$) and $K$ the subfield $\mathbb{F}_p(X^p, Y^p)$. Show that for any $f \in L$ one has $f^p \in K$, and deduce that $L/K$ is not a simple extension.

**5.** (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 $\mathrm{Aut}(K(X)/K) \simeq PGL_2(K)$.

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

## Finite fields

**7.** 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 $L$ be the field obtained from $\mathbb{F}_2$ by adjoining a root of $Q$. Describe explicitly an isomorphism from $K$ to $L$.

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

---

*Date*: November 11, 2009.

**9.** (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 $p \equiv \pm 1 \pmod 8$.

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

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

**12.** Recall the definition of the canonical isomorphism $\varphi_n : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. For every $m, n$ with $m \mid n$, show that the following is a commutative diagram:

$$\begin{tikzcd}
\mathbb{Z}/n\mathbb{Z} \arrow[r, "\varphi_n", "\cong"'] \arrow[d] & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \arrow[d] \\
\mathbb{Z}/m\mathbb{Z} \arrow[r, "\varphi_m", "\cong"'] & \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)
\end{tikzcd}$$

where the right vertical map is the natural restriction $\sigma \longmapsto \sigma|_{\mathbb{F}_{q^m}}$ and the left vertical map is the natural surjection $a \bmod n \longmapsto a \bmod m$.

**13.** 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

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

## Cyclotomic fields

For $n \in \mathbb{Z}_{>0}$, we denote by $K(\boldsymbol{\mu}_n)$ the $n$-th cyclotomic extension of $K$, the splitting field of $X^n - 1$ over $K$. We denote by $\zeta_n$ a primitive $n$-th root of unity for $n \in \mathbb{Z}_{>0}$.

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

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

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

(ii) For which $n \in \mathbb{N}$ is it possible to trisect an angle of size $2\pi/n$ using only ruler and compass?

**16.** Let $K = \mathbb{Q}(\boldsymbol{\mu}_n)$ be the $n$-th cyclotomic field, considered as a subfield of $\mathbb{C}$. 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 $K \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos 2\pi/n)$.

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

(iii) Let $L = \mathbb{Q}(\boldsymbol{\mu}_p)$. 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 $\mathbb{Q}(\boldsymbol{\mu}_m) \subset \mathbb{Q}(\boldsymbol{\mu}_n)$ 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**.]

**18.** 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 $\Phi_{pq}$ 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 $\Phi_n$ are $-1$, 0 or 1.

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

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

(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 $(\mathbb{Z}/(m))^\times$ in general.

*E-mail address*: `t.yoshida@dpmms.cam.ac.uk`