

Example Sheet 2. Lectures 7–12, Galois Theory Michaelmas 2010

FIELD EXTENSIONS, SPLITTING FIELDS

2.1. Find a splitting field K/\mathbb{Q} for each of the following polynomials, and calculate $[K : \mathbb{Q}]$ in each case:

$$X^4 - 5X^2 + 6, \quad X^4 - 7, \quad X^8 - 1, \quad X^3 - 2, \quad X^4 + 4.$$

2.2. Show that if F is a splitting field over K for $P \in K[X]$ of degree n , then $[F : K] \leq n!$.

2.3.* 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.]

2.4.* (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 $\text{Aut}(K(X)/K) \cong PGL_2(K)$.

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

CHARACTERISTIC p , FINITE FIELDS

2.5. Let K be a 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 $F = K(x)$ for any $x \in F$ with $P(x) = 0$, and that F/K is Galois, with Galois group isomorphic to $\mathbb{Z}/p\mathbb{Z}$. [These cyclic extensions are called **Artin-Schreier extensions**.]

2.6. Let $F = \mathbb{F}_p(X, Y)$ 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 $f \in F$ one has $f^p \in K$, and deduce that F/K is not a simple extension.

2.7. The polynomials $P(X) = X^3 + X + 1$, $Q(X) = X^3 + X^2 + 1$ 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' .

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

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \xrightarrow[\cong]{\varphi_n} & \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \\ \downarrow & & \downarrow \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow[\cong]{\varphi_m} & \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \end{array}$$

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

2.9. 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 $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$.

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

2.11.* (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 -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 $p \equiv \pm 1 \pmod{8}$.

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

2.13.* Show that the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over \mathbb{Q} (cf. Problem 1.15) 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 .)

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

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

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

2.15. (i) Find all the subfields of $\mathbb{Q}(\mu_7)$, expressing them in the form $\mathbb{Q}(x)$. Which are Galois over \mathbb{Q} ?

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

2.16. (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? [Ruler and compass can only solve successive quadratic extensions.]

2.17. Let $K = \mathbb{Q}(\mu_n)$ be the n -th cyclotomic field, considered as a subfield of \mathbb{C} . Show that under the canonical isomorphism $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$, 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 $K \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos 2\pi/n)$.

2.18.* (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 $\tau\bar{\tau} = p$. 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 $F = \mathbb{Q}(\mu_p)$. 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 $\mathbb{Q}(\mu_m) \subset \mathbb{Q}(\mu_n)$ if $m|n$. Deduce that if $0 \neq m \in \mathbb{Z}$ then $\mathbb{Q}(\sqrt{m})$ is a subfield of $\mathbb{Q}(\mu_{4|m})$. [This is a simple case of the **Kronecker-Weber Theorem**.]

2.19.* 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 $1/(1-X^p)(1-X^q)$ 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.

2.20.* 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.

(* optional)

November 5, 2010
t.yoshida@dpmmms.cam.ac.uk