Example Sheet 2. Galois Theory Michaelmas 2011

Note. You can assume that all non-finite fields are subfields of $\mathbb{C}$, as assumed in this part of the lectures. However, most proofs work without that assumption (where an *extension* L/K simply means that K is a subfield of L).

Galois extensions and Galois groups

2.1. Find the splitting field $F/\mathbb{Q}$ for each of the following polynomials (by factoring them explicitly in $\mathbb{C}[X]$), and calculate $[F:\mathbb{Q}]$ 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. Show that all subextensions of an abelian extension are abelian.

2.4. (i) Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine $[F:\mathbb{Q}]$ and $\mathrm{Aut}_{\mathbb{Q}}(F)$.

(ii) (**Biquadratic extensions**) Let $\mathbb{Q} \subset K$ (or $\mathrm{char}\, K \neq 2$). Prove that every extension F/K with $[F:K] = 4$ and $\mathrm{Aut}_K(F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is of the form $F = K(\sqrt{a}, \sqrt{b})$.

2.5. Let P be an irreducible quartic polynomial over K with $\mathbb{Q} \subset K$ (or $\mathrm{char}\, K \neq 2$), whose Galois group is A_4. Show that its splitting field can be written in the form $L(\sqrt{a}, \sqrt{b})$ where L/K is a Galois cubic extension and $a, b \in L$.

2.6. Show that $F = \mathbb{Q}(\sqrt[4]{2}, i)$ is a Galois extension of $\mathbb{Q}$, and show that $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to D_8, the dihedral group of order 8. Write down the lattice of subgroups of D_8 (be sure you have found them all!) and the corresponding subfields of F. Which subfields are Galois over $\mathbb{Q}$?

2.7. Recall (or show) that for any $n \geq 1$ there exists a Galois extension of fields F/K with $\mathrm{Gal}(F/K) \cong S_n$, the symmetric group of degree n. Show that for any finite group G there exists a Galois extension whose Galois group is isomorphic to G.

2.8. Let $n > 1$, and K be a field containing a primitive n-th root of unity. Assume that $X^n - a$ and $X^n - b$ are two irreducible polynomials in $K[X]$. Show that they have the same splitting field if and only if $b = c^n a^r$ for some $c \in K$ and $r \in \mathbb{N}$ with $\gcd(r, n) = 1$.

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

2.10. Write $\cos(2\pi/17)$ explicitly in terms of radicals.

Optional (not necessarily harder)

2.11.* 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.]

2.12.* Let $K \subset \mathbb{C}$, and F, L be two finite extensions of K, contained in $\mathbb{C}$. Let FL be the **composite field** of F and L, i.e. the extension of K generated by the elements of F, L (or, the set of all finite sums $\sum_i x_i y_i$ for $x_i \in F,\ y_i \in L$; see Problem 1.16).

(i) Assume that F/K and L/K are both Galois. Show that FL/K is Galois.

(ii) Assume that F/K and L/K are both soluble (i.e. Galois with soluble Galois groups). Show that FL/K is soluble. [Hint: recall the relation between $\mathrm{Gal}(FL/L)$ and $\mathrm{Gal}(F/K)$.]

2.13.* (i) For a group G, its **derived subgroup** G^{der} is the subgroup generated by all the elements of the form $xyx^{-1}y^{-1}$ for $x, y \in G$. Show that G^{der} is normal, and that G/G^{der} is abelian (it is the **maximal abelian quotient** of G, i.e. every group homomorphism from G to an abelian group factors through G/G^{der}).

(ii) For a finite group G, let $G_0 = G,\ G_i = (G_{i-1})^{\mathrm{der}}$ for $i \in \mathbb{N}$. Show that G is soluble if and only if there is an i such that $G_i = \{\mathrm{id}\}$.

(iii) Let G be the group of invertible $n \times n$ upper triangular matrices with entries in a finite field K. Show that G is soluble.

2.14.* Determine whether the following nested radicals can be unnested, i.e. written as $\mathbb{Q}$-linear combination of square roots of rationals; if so, find an expression:

$$\sqrt{2+\sqrt{11}},\ \sqrt{6+\sqrt{11}},\ \sqrt{11+6\sqrt{2}},\ \sqrt{11+\sqrt{6}}.$$

2.15.* Show that $\mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{2}}}\right)$ is abelian over $\mathbb{Q}$, and determine its Galois group.

2.16.* (i) Let p be a prime, and K be a field with $\mathrm{char}\, K \neq p$ and $K' := K(\boldsymbol{\mu}_p)$. For $a \in K$, 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 show 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.

October 25, 2011

t.yoshida@dpmms.cam.ac.uk