Example Sheet 1. **Lectures 1–6, Galois Theory Michaelmas 2011**

Note. You can assume that all 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).

Field extensions, minimal polynomials

1.1. Let α be a root of $X^3 + X^2 - 2X + 1 \in \mathbb{Q}[X]$. Express $(1-\alpha^2)^{-1}$ as a $\mathbb{Q}$-linear combination of 1, α and α^2. Justify the assertion that the cubic is irreducible over $\mathbb{Q}$, using Gauss' Lemma.

1.2. (**Quadratic extensions**) (i) Let $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$. Show that $P(X) = X^2 - 5$ is irreducible in $\mathbb{Q}(\sqrt{2})[X]$. If K is the extension of $\mathbb{Q}(\sqrt{2})$ generated by a root of P, then K contains three quadratic fields over $\mathbb{Q}$. Write these fields in the form $\mathbb{Q}(\sqrt{a})$ for $a \in \mathbb{Z}$.

(ii) Let L/K be an extension of degree 2 with $\mathbb{Q} \subset K$. Show that $L = K(\alpha) = \{a + b\alpha \mid a, b \in K\}$ for some $\alpha \in F$ with $\alpha^2 \in K$.

1.3. Find the minimal polynomials over $\mathbb{Q}$ of the complex numbers $\sqrt[5]{3}$, $i + \sqrt{2}$, $\sin(2\pi/5)$ and $e^{\pi i/6} - \sqrt{3}$.

1.4. Let L/K be an extension and $\alpha, \beta \in L$. Show that $\alpha + \beta$ and $\alpha\beta$ are algebraic over K if and only if α and β are algebraic over K.

1.5. Let $\alpha = \sqrt{2} + \sqrt{3}$. Draw the diagram of subextensions of $\mathbb{Q}(\alpha)/\mathbb{Q}$. Write down the minimal polynomial of α over $\mathbb{Q}$, and how it factors over each subfield of $\mathbb{Q}(\alpha)$. Can you justify your diagram using the tower law?

Tower law

1.6. Let L/K be a finite extension whose degree is prime. Show that there is no intermediate extension $L \supsetneq K' \supsetneq K$.

1.7. Let L/K be an extension, and suppose that $\alpha \in L$ be algebraic over K of odd degree, i.e. $[K(\alpha) : K]$ is odd. Show that $K(\alpha) = K(\alpha^2)$.

1.8. Let $L = K(\alpha, \beta)$, with $[K(\alpha) : K] = m$, $[K(\beta) : K] = n$ and $\gcd(m, n) = 1$. Show that $[L : K] = mn$.

1.9. Let L/K be a finite extension and $P \in K[X]$ an irreducible polynomial of degree $d > 1$. Show that if d and $[L : K]$ are coprime, P has no roots in L.

1.10. (i) Let α be algebraic over K. Show that there is only a finite number of intermediate fields $K \subset K' \subset K(\alpha)$. [Hint: Consider the minimal polynomial P of α over K', and show that P determines K'.]

(ii) Show that if L/K is a finite extension with $\mathbb{Q} \subset K$, for which there exist only finitely many intermediate subfields $K \subset K' \subset L$, then $L = K(\alpha)$ for some $\alpha \in L$. [Hint: use the fact that, as K has infinitely many elements, a finite dimensional K-vector space is not a union of finitely many proper K-subspaces. (But in fact (ii) holds for finite fields as well.)]

Optional (not necessarily harder)

1.11.* Find the greatest common divisors of the polynomials $P_1(X) = X^3 - 3$ and $P_2(X) = X^2 - 4$ in $\mathbb{Q}[X]$ and in $\mathbb{F}_5[X]$ (if you know $\mathbb{F}_5$ already), expressing them in the form $Q_1 P_1 + Q_2 P_2$ for polynomials Q_1, Q_2.

1.12.* Let R be a ring, and K a subring of R which is a field. Show that if R is an integral domain and $\dim_K R < \infty$ then R is a field. Show that the result fails without the assumption that R is a domain.

1.13.* (**Cubic extensions**) Suppose that L/K is an extension with $[L : K] = 3$, and let $\alpha \in L \setminus K$. By considering four appropriate elements of the 3-dimensional vector space L, show that for every $\beta \in L$ we can find $a, b, c, d \in K$ such that $\beta = \dfrac{a + b\alpha}{c + d\alpha}$. (This shows $L = K(\alpha)$ without appealing to the tower law.)

1.14.* Let L/K be an extension, and $\alpha, \beta \in L$ transcendental over K. Show that α is algebraic over $K(\beta)$ if and only if β is algebraic over $K(\alpha)$. [Then α, β are said to be **algebraically dependent**.]

1.15.* Let L/K be a field extension, and $\tau \colon L \to L$ a K-homomorphism. Show that if L/K is algebraic then τ is an isomorphism. How about when L/K is not algebraic?

1.16.* Let K, L be subfields of a field M such that M/K is finite. Denote by KL the set of all finite sums $\sum x_i y_i$ with $x_i \in K$ and $y_i \in L$. Show that KL is a subfield of M, and:

$$[KL : K] \leq [L : K \cap L].$$

October 13, 2011

t.yoshida@dpmms.cam.ac.uk