Example Sheet 1. **Lectures 1–6, Galois Theory Michaelmas 2010**

Rings (Preliminaries)

1.1.* 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 $\mathbb{F}_5[X]$, expressing them in the form $Q_1 P_1 + Q_2 P_2$ for polynomials Q_1, Q_2.

1.2.* 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.

Field extensions and K-homomorphisms

1.3. Let F/K be a finite extension whose degree is prime. Show that there is no intermediate extension $F \supsetneqq K' \supsetneqq K$.

1.4. (**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 field we get by adjoining the root of P to $\mathbb{Q}(\sqrt{2})$, 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 F/K be an extension of degree 2. Show that if the characteristic of K is not 2, then $F = K(x) = \{a + bx \mid a, b \in K\}$ for some $x \in F$ with $x^2 \in K$. Show that if the characteristic is 2, then either $F = K(x)$ with $x^2 \in K$, or $F = K(x)$ with $x^2 + x \in K$.

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

1.6.* Suppose that F/K is an extension with $[F : K] = 3$. Show that for any $x \in F$ and $y \in F \setminus K$ we can find $p, q, r, s \in K$ such that $x = \dfrac{p + qy}{r + sy}$.

[Hint: Consider four appropriate elements of the 3-dimensional vector space F.]

Minimal polyonomials, Algebraic extensions

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

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

1.9. Let $F = K(x, y)$, with $[K(x) : K] = m$, $[K(y) : K] = n$ and $\gcd(m, n) = 1$. Show that $[F : K] = mn$.

1.10. Let F/K be an extension and $x, y \in F$. Show that $x+y$ and xy are algebraic over K if and only if x and y are algebraic over K.

1.11. (i) Let $K(X)$ be a rational function field over a field K. Let $r = p/q \in K(X)$ be a non-constant rational function. Find a polynomial in $K(r)[T]$ which has X as a root.

(ii) Let L be a subfield of $K(X)$ containing K. Show that either $K(X)/L$ is finite, or $L = K$. Deduce that the only elements of $K(X)$ which are algebraic over K are constants.

1.12.* Show that an algebraic extension F/K of fields is finite if and only if it is **finitely generated**; i.e. if and only if $F = K(x_1, \ldots, x_n)$ for some $x_i \in F$. Prove that the algebraic numbers (roots of polynomials in $\mathbb{Q}[X]$) form a subfield of $\mathbb{C}$ which is not finitely generated over $\mathbb{Q}$.

1.13.* Let F/K be an extension, and $x, y \in F$ transcendental over K. Show that x is algebraic over $K(y)$ if and only if y is algebraic over $K(x)$. [Then x, y are said to be **algebraically dependent**.]

1.14.* 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:

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

Roots and subfields

1.15. Let $x = \sqrt{2} + \sqrt{3}$. Draw and justify the diagram of subextensions of $\mathbb{Q}(x)/\mathbb{Q}$. Write down the minimal polynomial of x over $\mathbb{Q}$, and how it factors over each subfield of $\mathbb{Q}(x)$.

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

1.17. (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 P of x over K', and show that P determines K'.]

(ii) Show that if F/K is a finite extension of infinite fields for which there exist only finitely many intermediate subfields $K \subset K' \subset F$, then $F = K(x)$ for some $x \in F$. [It is true for finite fields as well, but here we use the infiniteness.]

1.18.* Let F/K be a field extension, and $\varphi\colon F \to F$ a K-homomorphism. Show that if F/K is algebraic then φ is an isomorphism. How about when F/K is not algebraic?

(* optional)

t.yoshida@dpmms.cam.ac.uk