Example sheet 1, Galois Theory (Michaelmas 2022)

a.j.scholl@dpmms.cam.ac.uk

This sheet covers lectures 1–6. Questions which might be more challenging are marked *.

Polynomials and symmetric polynomials

1. (i) Find the greatest common divisor of the polynomials $f = X^3 - 3$ and $g = X^2 + 1$ in $\mathbb{Q}[X]$, expressing the result in the form $af + bg$ for polynomials a, b.

(ii) Do the same for f and g in $\mathbb{F}_5[X]$. (Note that the answer is not the same as in (i).)

2. Express $\sum_{i \neq j} X_i^3 X_j$ as a polynomial in the elementary symmetric polynomials.

3. Show that if $X_1, \ldots, X_n$ are indeterminates, then

$$\begin{vmatrix} X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1} \\ X_1^{n-2} & X_2^{n-2} & \cdots & X_n^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & \cdots & X_n \\ 1 & 1 & \cdots & 1 \end{vmatrix} = \Delta = \prod_{1 \le i < j \le n} (X_i - X_j)$$

(First show that each $(X_i - X_j)$ is a factor of the determinant).

Fields and algebraic elements

4. (Quadratic extensions) Let L/K be an extension of degree 2. Show that if the characteristic of K is not 2, then $L = K(x)$ for some $x \in L$ with $x^2 \in K$.

* Show that if the characteristic is 2, then either $L = K(x)$ with $x^2 \in K$, or $L = K(x)$ with $x^2 + x \in K$.

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

6. Let $f(X) = X^3 + X^2 - 2X + 1 \in \mathbb{Q}[X]$. Use Gauss's Lemma to show that f is irreducible.

Suppose that x has minimal polynomial f over $\mathbb{Q}$, and let $y = x^4$. Find a, b, $c \in \mathbb{Q}$ such that $y = a + bx + cx^2$. Do the same for $y = (1 - x^2)^{-1}$.

7. Let L/K be an extension and $x \in L$. Show that

$$K[x] = \bigcap_{\substack{K \subset R \subset L \\ x \in R \\ R \text{ a ring}}} R \qquad \text{and} \qquad K(x) = \bigcap_{\substack{K \subset F \subset L \\ x \in F \\ F \text{ a field}}} F.$$

Tower law

8. (i) Let L/K be a finite extension whose degree is prime. Show that there is no intermediate extension $L \supsetneqq K' \supsetneqq K$.

(ii) Let x be algebraic over K of odd degree. Show that $K(x) = K(x^2)$.

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

Others

10. (i) Let K be a field, and $r = p/q \in K(X)$ 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.

11. Show that a regular 7-gon is not constructible by ruler and compass.

Additional (starred) examples for enthusiasts (of varying difficulty)

12. For I an n-tuple $I = (i_1, \dots, i_n)$ with $i_1 \geq i_2 \geq \cdots \geq i_n$, recall we have defined the monomial $X_I = \prod X_\alpha^{i_\alpha}$. Let S_I be the sum of all monomials X_J obtained from X_I by a permutation of indices. (For example, $S_{(2,1,1)} = X_1^2 X_2 X_3 + X_1 X_2^2 X_3 + X_1 X_2 X_3^2$.) Show that the elementary symmetric polynomials s_r and the power sums p_k are of the form S_I for suitable I, and that every symmetric polynomial in $\mathbb{Z}[X_1, \dots, X_n]$ can be expressed uniquely in the form $\sum_I c_I S_I$ with $c_I \in \mathbb{Z}$. Show also that for every I and J

$$S_I S_J = S_{I+J} + \sum_{K < I+J} c_K S_K$$

for integers c_K. (Here $<$ denotes lexicographical ordering.)

13. Show that an algebraic extension L/K of fields is finite if and only if it is *finitely generated*; i.e. iff $L = K(x_1, \dots, x_n)$ for some $x_i \in L$. Prove that the algebraic numbers (zeros of polynomials with rational coefficients) form a subfield of $\mathbb{C}$ which is not finitely generated over $\mathbb{Q}$.

14. 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.

15. Let K and 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 that

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

16. Suppose that L/K is an extension with $[L : K] = 3$. Show that for any $x \in L$ and $y \in L - K$ 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 L.]

17. Let L/K be an extension, and $x, y \in L$ transcendental over K. Show that x is algebraic over $K(y)$ iff y is algebraic over $K(x)$. [x, y are then said to be **algebrically dependent**.]