Example Sheet 4, Galois Theory 2018 pmhw@dpmms.cam.ac.uk

1. Let K be a field of characteristic $p > 0$. Let $a \in K$, and let $f \in K[X]$ be the polynomial $f(X) = X^p - X - a$. Show that $f(X + b) = f(X)$ for every $b \in \mathbf{F_p} \subset K$. Now suppose that f does not have a root in K, and let L/K be a splitting field for f over K. Show that $L = K(x)$ for any $x \in L$ with $f(x) = 0$, and that L/K is Galois, with Galois group isomorphic to $\mathbf{Z}/p\mathbf{Z}$.

2. Let K be a field, p a prime and $K' = K(\zeta)$ for some primitive pth root of unity ζ. Let $a \in K$. 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?

3. If K contains a primitive nth root of unit, show that $X^n - a \in K[X]$ is reducible over K if and only if a is a dth power in K for some divisor $d > 1$ of n. Show that this need not be true if K doesn't contain an nth root of unity.

4. Let K be a field containing a primitive mth root of unity for some $m > 1$. Let $a, b \in K$ such that the polynomials $f = X^m - a$, $g = X^m - b$ are irreducible. Show that f and g have the same splitting field if and only if $b = c^m a^r$ for some $c \in K$ and $r \in \mathrm{N}$ with $\gcd(r, m) = 1$.

5. Consider the polynomial $f = X^3 + 3X^2 - 1$ over $\mathbf{Q}$. Show that there exist $\delta \in \mathbf{Q}$ and $\gamma \in \mathbf{Q}(\delta^{1/2})$ such that f splits over $K = \mathbf{Q}(\delta^{1/2})(\gamma^{1/3})$.

6. For n a positive integer, write $\zeta_n = e^{2\pi i/n}$. Show that $\mathbf{Q}(\zeta_{21})$ has exactly three subfields of degree 6 over $\mathbf{Q}$. Show that one of them is $\mathbf{Q}(\zeta_7)$, one is real, and the other is a cubic extension $K = \mathbf{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})$ of $\mathbf{Q}(\zeta_3)$. Show that the minimal polynomial of $\zeta_7 + \zeta_7^{-1} = 2\cos(2\pi/7)$ over $\mathbf{Q}(\zeta_3)$ is $X^3 + X^2 - 2X - 1$. [Using the general solution of cubics from §8, it can be shown that $K = \mathbf{Q}(\zeta_3, \sqrt[3]{a})$, where $a = 7(1 + 3\sqrt{-3})/2 \in \mathbf{Q}(\zeta_3)$].

7. Let $f \in \mathbf{Q}[X]$ be an irreducible quartic polynomial whose Galois group is A_4. Show that its splitting field can be written in the form $K(\sqrt{a}, \sqrt{b})$ where $K/\mathbf{Q}$ is a Galois cubic extension and $a, b \in K$. Show that the resolvant cubic of $X^4 + 6X^2 + 8X + 9$ has Galois group C_3 (cf. Example Sheet 2, Q10) and deduce that the quartic has Galois group A_4.

8. Let $f \in k[X]$ be a quartic polynomial with distinct roots in a splitting field, and $g \in k[X]$ its resolvant cubic. Show that the discriminant of g is the same as that of f.

9. Find the Galois groups of the polynomials $X^5 - 4X + 2$ and $X^4 - 4X + 2$ over $\mathbf{Q}$. What are their Galois groups over $\mathbf{Q}(i)$?

10. Show that $X^4 + X^2 + X + 1$ is irreducible over $\mathbf{F}_3$, and find its Galois group over $\mathbf{Q}$.

11. Let $f \in k[X]$ be an irreducible (separable) quartic, with Galois group $G \subset S_4$. Let $V \subset S_4$ be the 4-group, containing pairs of transpositions. Show that $G \cap V$ is either V or a subgroup of index 2 in V. In both cases, determine the various possibilities for G.

12. Let F, E be intermediate fields of a finite separable field extension $K \subset L$. Show that if F/K and E/K are soluble extensions, then FE/K is also soluble. (Here FE denotes the composite field of F and E as in Example Sheet 1, Q11.)

13. Let $f = X^5 + 20X + 16 \in \mathbf{Q}[X]$; show that f has four complex roots. Using Example 4.9, show that the discriminant of f is $D = 2^{16}5^6$; deduce that the reduction of f mod 2 or 5 must have repeated roots (in a splitting field). Explain why the reduction of f modulo any other prime cannot split into the product of an irreducible quadratic and an irreducible cubic. Deduce that the polynomial is irreducible over $\mathbf{F}_3$. Assuming only the fact that A_5 is simple, show that $\mathrm{Gal}(f) = A_5$. [*Hint: Reduce modulo another suitable prime. If you did Question 13 on Example Sheet 3, it might help to look at your answer.*]

---

14. Let L/K be a Galois extension with cyclic Galois group of prime order p, generated by σ.

(i) Show that for any $x \in L$, $\mathrm{Tr}_{L/K}(\sigma(x) - x) = 0$. Deduce that if $y \in L$ then $\mathrm{Tr}_{L/K}(y) = 0$ if and only if there exists $x \in L$ with $\sigma(x) - x = y$.

(ii) Suppose that K has characteristic p. Use (i) to show that any element of K can be written in the form $\sigma(x) - x$ for some $x \in L$. Show also that if $\sigma(x) - x = 1$ then $a = x^p - x \in K$. Deduce that L/K is the splitting field of polynomial of the form $X^p - X - a$. (Compare this result with Q1.)

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

16. Explain why $\cos(2\pi/17)$ may be written in terms of radicals. **Now explicitly do it!

17. (i) If $f : A_5 \to \mathrm{GL}(2, \mathbf{C})$ is a homomorphism, why must f have image in $\mathrm{SL}(2, \mathbf{C})$? Suppose $\sigma \in A_5$ is one of the 15 elements of order 2; show that $f(\sigma) = \pm I$, where I denotes the 2×2 identity matrix. Using the fact that A_5 is simple, deduce that f must be trivial.

(ii) Suppose now that $\tilde{A}_5 \subset \mathrm{SU}(2)$ denotes the binary icosahedral group and $g : \tilde{A}_5 \to \mathbf{C}^*$ a homomorphism. Show that either g is trivial, or $g(-I) = -1$. In the latter case show that there is a homomorphism $A_5 \to \mathrm{GL}(2, \mathbf{C})$, induced by $\tilde{\sigma} \mapsto g(\tilde{\sigma})\tilde{\sigma}$ for $\tilde{\sigma} \in \tilde{A}_5$, which by (i) must then be trivial. Deduce that the latter case does not occur and thus that g itself must be trivial.

18. Let $\tilde{G} \subset \mathrm{SU}(2)$ be the subgroup of order 16 generated by matrices

$$\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \quad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

where ζ is a primitive 8th root of unity. The elements $\tilde{\sigma}$ of $\tilde{G}$ act on $\mathbf{C}^2$ via matrix multiplication, and thus on the polynomial ring $R = \mathbf{C}[X_1, X_2]$ via $(\tilde{\sigma} f)(\mathbf{x}) = f(\tilde{\sigma}^{-1}\mathbf{x})$, and on the 2-sphere $\mathbf{C}_\infty$ by Möbius transformations. Find the invariant homogeneous quartics and prove that there are no invariant quadratics or sextics. *Show that any homogeneous polynomial in R corresponding to an orbit of size 8 in $\mathbf{C}_\infty$ is an invariant under the action $\tilde{G}$, and is a linear combination of $(X_1X_2)^4$ and $(X_1^4 + X_2^4)^2$. Deduce that the ring of invariants $R^{\tilde{G}}$ is a polynomial ring on two generators (to be specified).