Example sheet 4, Galois Theory, 2019.

1. (i) Let K be a field, p a prime and $K' = K(\zeta)$ for some primitive p^{th} 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?

(ii) If K contains a primitive n^{th} root of unity, then we know 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.

2. Let K be a field containing a primitive m^{th} 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 $r \in \mathbb{N}$ with $\gcd(r, m) = 1$.

3. Let f be an irreducible separable quartic, and g its resolvant cubic. Show that the discriminants of f and g are equal.

4. Let $f \in \mathbb{Q}[x]$ 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 $K/\mathbb{Q}$ is a Galois cubic extension and $a, b \in K$.

5. Show that the discriminant of $x^4 + rx + s$ is $-27r^4 + 256s^3$. [It is a symmetric polynomial of degree 12, hence a linear combination of r^4 and s^3. By making good choices for r, s, determine the coefficients.]

6. Let $f(x) = x^4 + 8x + 12 \in \mathbb{Q}[x]$. Compute the discrimininant and resolvant cubic g of f. Show f and g are both irreducible, and that the Galois group of f is A_4.

7. Determine the Galois group of the following polynomials in $\mathbb{Q}[x]$. $x^4 + 4x^2 + 2$, $x^4 + 2x^2 + 4$, $x^4 + 4x^2 - 5$, $x^4 - 2$, $x^4 + 2$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$

8. Let $\zeta = e^{2\pi i/3}$, let $\alpha = \sqrt[3]{(a + b\sqrt{2})}$ and let L be the splitting field for an irreducible polynomial for α over $\mathbb{Q}(\zeta)$. Determine the possible Galois groups of L over $\mathbb{Q}(\zeta)$.

9. Determine whether the following nested radicals can be written in terms of unnested ones, and if so, find an expression.

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

10. (i) Show that the Galois group of $f(x) = x^5 - 4x + 2$ over $\mathbb{Q}$ is S_5, and determine its Galois group over $\mathbb{Q}(i)$.

(ii) Find the Galois group of $f(x) = x^4 - 4x + 2$ over $\mathbb{Q}$ and over $\mathbb{Q}(i)$.

11. In this question we determine the structure of the groups $(\mathbb{Z}/m\mathbb{Z})^*$.

(i) Let p be an odd prime. Show that for every $n \geq 2$, $(1 + p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n}$. Deduce that $1 + p$ has order p^{n-1} in $(\mathbb{Z}/p^n\mathbb{Z})^*$.

(ii) If $b \in \mathbb{Z}$ with $(p, b) = 1$ and b has order $p - 1$ in $(\mathbb{Z}/p\mathbb{Z})^*$ and $n \geq 1$, show that $b^{p^{n-1}}$ has order $p - 1$ in $(\mathbb{Z}/p^n\mathbb{Z})^*$. Deduce that for $n \geq 1$ and p an odd prime, $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic.

(iii) Show that for every $n \geq 3$, $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$. Deduce that $(\mathbb{Z}/2^n\mathbb{Z})^*$ is generated by 5 and -1, and is isomorphic to $\mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, for any $n \geq 2$.

(iv) Use the Chinese Remainder Theorem to deduce the structure of $(\mathbb{Z}/m\mathbb{Z})^*$ in general.

(v) *Dirichlet's theorem on primes in arithmetic progressions* states that if a and b are coprime positive integers, then the set $\{an + b \mid n \in \mathbb{N}\}$ contains infinitely many primes. Use this, the structure theorem for finite abelian groups, and part (iv) to show that every finite abelian group is isomorphic to a quotient of $(\mathbb{Z}/m\mathbb{Z})^*$ for suitable m. Deduce that every finite abelian group is the Galois group of some Galois extension $K/\mathbb{Q}$. [It is a long-standing unsolved problem to show this holds for an arbitrary finite group.]

(vi) Find an explicit α for which $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois with Galois group $\mathbb{Z}/23\mathbb{Z}$.

12. Here and in the next few questions, $\zeta_m = e^{2\pi i/m}$ for a positive integer m.

(i) Find the quadratic subfields of $\mathbb{Q}(\zeta_{15})$.

(ii) Show that $\mathbb{Q}(\zeta_{21})$ has exactly three subfields of degree 6 over $\mathbb{Q}$. Show that one of them is $\mathbb{Q}(\zeta_7)$, one is real, and the other is a cyclic extension $K/\mathbb{Q}(\zeta_3)$. Find an explicit $a \in \mathbb{Q}(\zeta_3)$ such that $K = \mathbb{Q}(\zeta_3, \sqrt[3]{a})$.

13. Compute the discriminant of $x^{p^n} - 1$.

14. Show $\mathbb{Q}(\zeta_m).\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$ if m and n are relatively prime.

15. In this question you will construct the quadratic subfield of $\mathbb{Q}(\zeta_p)$ using the first method sketched in lectures.

(i) Let p be an odd prime. Show that if $r \in \mathbb{Z}$ then $\sum_{0\le s<p} \zeta_p^{rs}$ equals p if $r \equiv 0 \pmod{p}$ and equals 0 otherwise.

(ii) Let $\tau = \sum_{0\le n<p} \zeta_p^{n^2}$. Show that $\tau\overline{\tau} = p$. Show also that τ is real if -1 is a square mod p, and otherwise τ is purely imaginary (i.e. $\tau/i \in \mathbb{R}$).

(iii) Let $L = \mathbb{Q}(\zeta_p)$. Show that L has a unique subfield K which is quadratic over $\mathbb{Q}$, and that $K = \mathbb{Q}(\sqrt{\varepsilon p})$ where $\varepsilon = (-1)^{(p-1)/2}$.

(iv) Show that $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$ if $m|n$. Deduce that if $0 \ne m \in \mathbb{Z}$ then $\mathbb{Q}(\sqrt{m})$ is a subfield of $\mathbb{Q}(\zeta_{4|m|})$. [This is a simple case of the *Kronecker-Weber Theorem*, which says that every abelian extension of $\mathbb{Q}$ is a subfield of a suitable $\mathbb{Q}(\zeta_m)$.]

16. For which $n \in \mathbb{N}$ is it possible to trisect an angle of size $2\pi/n$ using only straightedge and compass?

17. (i) Let G be a finite group, and N a normal subgroup. Show that G is solvable if and only if N and G/N are solvable.

(ii) For a group G, the *derived subgroup* G^{der} is the subgroup generated by all elements $\{xyx^{-1}y^{-1} \mid x, y \in G\}$. Show that G^{der} is normal, and that G/G^{der} is abelian.

Show that if G is a simple group, then $G = G^{der}$. [The converse is not true.]

Let $G_0 = G$, and for $i > 0$, set $G_i = (G_{i-1})^{der}$. Show that G is solvable if and only if there is an i such that $G_i = 1$.

iii) Let G be the group of invertible n by n upper triangular matrices, with coefficients in a finite field K. Show that G is solvable.

18. (i) Let D_{2n} be the dihedral group of order $2n$, and $N = \mathbb{Z}/n\mathbb{Z}$ its cyclic subgroup of rotations. Show that D_{2n} is isomorphic to a semidirect product of N and $\mathbb{Z}/2\mathbb{Z}$.

(ii) Let $G = D_8$, $V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Show V is a normal subgroup of G, with quotient $\mathbb{Z}/2\mathbb{Z}$. Is G a semidirect product of V and $\mathbb{Z}/2\mathbb{Z}$?

(iii) Let G be a group with normal subgroup N. Show that G is isomorphic to a semidirect product of G and G/N if and only if there is a subgroup H of G isomorphic to G/N such that $H \cap N = 1$, $HN = G$.

19. Show that $\mathbb{Q}(\sqrt{2+\sqrt{2+\sqrt{2}}})$ is an abelian extension of $\mathbb{Q}$, and determine its Galois group.

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

21. Show that for any $n > 1$ the polynomial $x^n + x + 3$ is irreducible over $\mathbb{Q}$. Determine its Galois group for $n \le 5$.