Galois theory (Part II)(2015–2016)
Example Sheet 1

c.birkar@dpmms.cam.ac.uk

(1) Find the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$.

(2) Let $K \subseteq L$ be a finite field extension such that $[L : K]$ is prime. Show that any intermediate field $K \subseteq F \subseteq L$ is equal to K or equal to L.

(3) Let $K \subseteq L$ be a field extension of degree 2. Show that if the characteristic of K is not 2, then $L = K(\alpha)$ for some $\alpha \in L$ with $\alpha^2 \in K$. Show that if the characteristic is 2, then either $L = K(\alpha)$ with $\alpha^2 \in K$, or $L = K(\alpha)$ with $\alpha^2 + \alpha \in K$.

(4) Let $K \subseteq L$ be a field extension and $\alpha \in L$ an element with $[K(\alpha) : K]$ an odd number. Show that $K(\alpha) = K(\alpha^2)$.

(5) Let $K \subseteq L$ be a field 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.

(6) Let K be a field and $K(s)$ the field of rational functions in s over K, i.e. the fraction field of the polynomial ring $K[s]$. Determine all the elements of $K(s)$ which are algebraic over K.

(7) Let L be the set of all the numbers in $\mathbb{C}$ which are algebraic over $\mathbb{Q}$. Show that L is a subfield of $\mathbb{C}$ and that $[L : \mathbb{Q}]$ is infinite.

(8) Let $K \subseteq L$ be a field extension and $\varphi\colon L \to L$ a K-homomorphism. Show that φ is a K-isomorphism if L is algebraic over K.

(9) Show that the angle $\frac{\pi}{6}$ cannot be divided into three equal angles using ruler and compass. Hint: make use of the formula

$$\sin(3\theta) = 3\sin(\theta) - 4\sin(\theta)^3.$$

(10) Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Calculate $[L : \mathbb{Q}]$ and $\mathrm{Aut}_{\mathbb{Q}}(L)$. Is $\mathbb{Q} \subseteq L$ a Galois extension?

(11) Let $n \in \mathbb{N}$ and assume $f = t^{n-1} + t^{n-2} + \cdots + t + 1$ is irreducible in $\mathbb{Q}[t]$. Let $\mu = \exp(2\pi i/n)$ where $i = \sqrt{-1}$. Show that f is the minimal polynomial of μ over $\mathbb{Q}$. Next show that $\mathbb{Q} \subseteq \mathbb{Q}(\mu)$ is a Galois extension.

(12) We use the notation and assumptions of the previous problem. Show that there is a natural group isomorphism $\mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q}) \to G$ where G is the multiplicative group of the unit elements of the ring $\mathbb{Z}/\langle n \rangle$.

(13) Find a splitting field L over $\mathbb{Q}$ for each of the following polynomials, and then calculate $[L : \mathbb{Q}]$ in each case:

$$t^4 - 5t^2 + 6, \ t^8 - 1$$

(14) Let $K \subseteq L$ be a field extension and $f \in K[t]$ an irreducible polynomial of degree 2. Show that if f has a root in L, then L contains a splitting field of f over K.

(15) Let K be a field and $f \in K[t]$ a polynomial of degree n. Show that if L is a splitting field of f over K, then $[L : K] \leq n!$.

(16) Let $K \subseteq L$ be a finite field extension inside $\mathbb{C}$. Show that if $K \neq L$, then $|\operatorname{Hom}_K(L, \mathbb{C})| \geq 2$.

(17) Let K be a finite field. Write down a non-constant polynomial over K which does not have a root in K. Deduce that K cannot be algebraically closed.

(18) Let K be field and $\overline{K}$ its algebraic closure. Assume $K \subseteq L$ is a finite field extension. Show that L is K-isomorphic to some subfield of $\overline{K}$.

(19) Let K_1 and K_2 be algebraically closed fields of the same characteristic. Show that either K_1 is isomorphic to a subfield of K_2 or K_2 is isomorphic to a subfield of K_1. (Hint: use Zorn's lemma)

Galois theory (Part II)(2015–2016)
Example Sheet 2

c.birkar@dpmms.cam.ac.uk

(1) Let K be a field of characteristic $p > 0$ such that every element of K is a p-th power, i.e. for each $a \in K$ there is $b \in K$ with $a = b^p$. Show that every polynomial in $K[t]$ is separable.

(2) Let K be a finite field. Show that every polynomial in $K[t]$ is separable. Deduce that an extension of finite fields is separable.

(3) Let $K \subseteq L$ be an extension of fields of characteristic $p > 0$, and let $\alpha \in L$ be algebraic over K. Show that α is not separable over K if and only if $K(\alpha) \neq K(\alpha^p)$, and that if this is the case, then p divides $[K(\alpha) : K]$.

(4) Let $K \subseteq L$ be a finite extension of fields of characteristic $p > 0$ which is not separable. Show that p divides $[L : K]$.

(5) Let $K \subseteq L$ be a finite field extension. Show that there is a unique intermediate field $K \subseteq F \subseteq L$ such that $K \subseteq F$ is separable but $F \subseteq L$ is *purely inseparable*, i.e. no element $\alpha \in L \setminus F$ is separable over F. We call F the *separable closure* of K in L. Show that $|\operatorname{Hom}_F(L, E)| \leq 1$ for every extension $F \subseteq E$.

(6) Find an example of a field extension $K \subseteq L$ which is normal but not separable.

(7) Let $K \subseteq L$ be a field extension with $[L : K] = 2$. Show that the extension is normal.

(8) Find finite field extensions $K \subseteq F \subseteq L$ such that $K \subseteq F$ and $F \subseteq L$ are normal but $K \subseteq L$ is not normal.

(9) Show that $\mathbb{Q} \subseteq L = \mathbb{Q}(\sqrt{2}, \sqrt{-1})$ is a Galois extension and determine its Galois group. Write down all the subgroups of $\operatorname{Gal}(L/\mathbb{Q})$ and the corresponding subfields of L.

(10) Show that $\mathbb{Q} \subseteq L = \mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})$ is a Galois extension and that its Galois group is generated by two elements φ and ψ satisfying

$$\varphi(\sqrt[4]{2}) = \sqrt[4]{2}\sqrt{-1},\ \varphi(\sqrt{-1}) = \sqrt{-1},\ \psi(\sqrt[4]{2}) = \sqrt[4]{2},\ \psi(\sqrt{-1}) = -\sqrt{-1}$$

What is the subgroup of $\operatorname{Gal}(L/\mathbb{Q})$ corresponding to $\mathbb{Q}(\sqrt[4]{2})$? Is it a normal subgroup?

(11) Let L be the splitting field of $t^3 - 2$ over $\mathbb{Q}$. Find a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ which is not a normal subgroup.

(12) Let $K \subseteq L$ be a finite Galois extension, and F, M intermediate fields. What is the subgroup of $\mathrm{Gal}(L/K)$ corresponding to the subfield $F \cap M$? Show that if there is a K-isomorphism $F \to M$, then the subgroups $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(L/M)$ are conjugate in $\mathrm{Gal}(L/K)$.

(13) Show that for any natural number n there exists a Galois extension $K \subseteq L$ with $\mathrm{Gal}(L/K)$ isomorphic to S_n, the symmetric group of degree n. Show that for any finite group G there exists a Galois extension whose Galois group is isomorphic to G. (Hint: to prove the first claim, consider the field $L = \mathbb{Q}(s_1, \ldots, s_n)$ of rational functions in $s_1, \ldots, s_n$, then consider an action of S_n on L, etc.)

(14) Let K be a field and $f \in K[t]$ a polynomial of degree n with no repeated roots in a splitting field L of f over K. Show that $K \subseteq L$ is a Galois extension. Show that there is a (natural) injective homomorphism $\mathrm{Gal}(L/K) \to S_n$.

(15) Let K be a field and $f \in K[t]$ a polynomial with no repeated roots in a splitting field L of f over K. Show that f is irreducible iff $\mathrm{Gal}(L/K)$ acts transitively on $\mathrm{Root}_f(L)$ (that is, for any two roots α, β there is $\varphi \in \mathrm{Gal}(L/K)$ such that $\varphi(\alpha) = \beta$).

(16) Suppose $K \subseteq L$ is a Galois extension with $G = \mathrm{Gal}(L/K)$ and let $\alpha \in L$. Show that $L = K(\alpha)$ iff the images of α under the elements of G are distinct.

(17) Show that there is at least one irreducible polynomial $f \in \mathbb{F}_5[t]$ with $\deg f = 17$.

(18) Let p be a prime number and $L = \mathbb{F}_p(s)$ be the field of rational functions in s. Let $a \in \mathbb{F}_p$ be a non-zero element, and let $\varphi \in \mathrm{Aut}_{\mathbb{F}_p}(L)$ be the automorphism determined by $\varphi(s) = as$. Determine the subgroup $G \leq \mathrm{Aut}_{\mathbb{F}_p}(L)$ generated by φ, and its fixed field L^G.

(19) Let L be the splitting field of $t^4 + t^3 + 1$ over a field K. Compute the Galois group $\mathrm{Gal}(L/K)$ for each of the following cases: $K = \mathbb{F}_2$, $K = \mathbb{F}_3$, and $K = \mathbb{F}_4$.

Galois theory (Part II)(2015–2016)
Example Sheet 3

c.birkar@dpmms.cam.ac.uk

(1) Compute $\Phi_{12} \in \mathbb{Z}[t]$, the 12-th cyclotomic polynomial.

(2) Let $K \subseteq L$ be an extension of finite fields. Show that L is the n-th cyclotomic extension of K for some n.

(3) Let L be the 7-th cyclotomic extension of $\mathbb{Q}$. Find all the intermediate fields $\mathbb{Q} \subseteq F \subseteq L$ and write each one as $\mathbb{Q}(\alpha)$ for some α. Which one of these intermediate fields is Galois over $\mathbb{Q}$?

(4) Let $\Phi_n \in \mathbb{Z}[t]$ denote the n-th cyclotomic polynomial. Show that:
(i) If $n > 1$ is odd, then $\Phi_{2n}(t) = \Phi_n(-t)$.
(ii) If p is a prime dividing n, then $\Phi_{np}(t) = \Phi_n(t^p)$.
(iii) If p and q are distinct primes, then the non-zero coefficients of Φ_{pq} are alternately $+1$ and -1. ([Hint: First show that if $1/(1-t^p)(1-t^q)$ is expanded as a power series in t, then the coefficients of t^m with $m < pq$ are either 0 or 1.)
(iv) If n is not divisible by at least three distinct odd primes, then the coefficients of Φ_n are $1, 0$ or -1.
(v) Φ_{105} has at least one coefficient which is not $1, 0$ or -1.

(5) Let $\mu = \exp(2\pi i/n)$ where $i = \sqrt{-1}$, and let $L = \mathbb{Q}(\mu)$ be the n-th cyclotomic extension of $\mathbb{Q}$. Show that the isomorphism $\mathrm{Gal}(L/\mathbb{Q}) \to (\mathbb{Z}/\langle n\rangle)^*$ sends the automorphism given by complex conjugation to the class of -1. Deduce that if $n \geq 3$, then $[L : L\cap\mathbb{R}] = 2$ and show that $L\cap\mathbb{R} = \mathbb{Q}(\mu+\mu^{-1}) = \mathbb{Q}(\cos 2\pi/n)$.

(6) An unsolved problem asks whether for an arbitrary finite group G there exists a Galois extension $\mathbb{Q} \subseteq L$ whose Galois group is isomorphic to G. We want to show that this holds for abelian groups.
(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 $(\mathbb{Z}/\langle p^n\rangle)^*$.
(ii) If $b \in \mathbb{Z}$ with $(p, b) = 1$ and b has order $p-1$ in $(\mathbb{Z}/\langle p\rangle)^*$ and $n \geq 1$, show that $b^{p^{n-1}}$ has order $p-1$ in $(\mathbb{Z}/\langle p^n\rangle)^*$. Deduce that for $n \geq 1$, $(\mathbb{Z}/\langle p^n\rangle)^*$ is cyclic.
(iii) Show that for every $n \geq 3$, we have $5^{2^{n-3}} \equiv 1+2^{n-1} \pmod{2^n}$. Deduce that $(\mathbb{Z}/\langle 2^n\rangle)^*$ is generated by the classes of 5 and -1, and is isomorphic to $(\mathbb{Z}/\langle 2^{n-2}\rangle) \times (\mathbb{Z}/\langle 2\rangle)$ for any $n \geq 2$.
(iv) Use the Chinese Remainder Theorem to deduce the structure of $(\mathbb{Z}/\langle m\rangle)^*$ in general.
(v) Dirichlet's theorem on primes in arithmetic progressions states that if a and b are coprime positive integers, then the set $\{an + b | n \in \mathbb{N}\}$ 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 $(\mathbb{Z}/\langle m\rangle)^*$ for suitable m. Deduce that every finite abelian group

is the Galois group of some Galois extension $\mathbb{Q} \subseteq L$.

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

(8) Let p be a prime, K be a field with char $K \neq p$, and L the p-th cyclotomic extension of K. For $a \in K$, show that $t^p - a$ is irreducible over K if and only if it is irreducible over L. Is the result true if p is not assumed to be prime?

(9) Let K be a field containing an n-th primitive root of unity. Show that $t^n - a$ 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 does not contain an n-th primitive root of unity.

(10) Let K be a field of char $K = 0$ and L the n-th cyclotomic extension of K. Show that there is a sequence of Kummer extensions $E_0 = K \subseteq E_1 \subseteq \cdots \subseteq E_r$ such that L is contained in E_r. (Hint: consider F = splitting field of $(t^n - 1)(t^{n-1} - 1) \cdots (t - 1)$ and apply induction on n)

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

(12) Let L be the splitting field of $t^3 - t - 1$ over $\mathbb{Q}$. Show that the Galois group of $\mathbb{Q} \subseteq L$ is isomorphic to S_3.

(13) Let $f \in \mathbb{Q}$ be irreducible of degree 4 and let L be its splitting field over $\mathbb{Q}$. Show that the extension $\mathbb{Q} \subseteq L$ is radical. Now assume the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to A_4. Show that L can be written in the form $F(\sqrt{a}, \sqrt{b})$ where $\mathbb{Q} \subseteq F$ is a Galois extension of degree 3 and $a, b \in F$.

(14) Consider the quartic $f = t^4 - 4t + 2$ and let L be its splitting field over $\mathbb{Q}(\sqrt{-1})$. Find the Galois group $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{-1})$.

(15) Let L be the splitting field of $t^5 - 2$ over $\mathbb{Q}$. Investigate the Galois group $\mathrm{Gal}(L/\mathbb{Q})$.

(16) Let $f = t^5 - 9t + 3 \in \mathbb{Q}[t]$ and let L be the splitting field of f over $\mathbb{Q}$. Show that $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to S_5. Let α be a root of f. Show that the extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ is not Galois by proving $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = 1$. Next show that the mentioned extension is not radical nor solvable.

(17) Let $f \in \mathbb{Q}[t]$ be irreducible of degree 4 and L its splitting field over $\mathbb{Q}$. Consider the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ as a subgroup $G \leq S_4$. Let $V = \{1, (12)(34), (13)(24), (14)(23)\}$. 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.

Galois theory (Part II)(2015–2016)
Example Sheet 4

c.birkar@dpmms.cam.ac.uk

(1) Let $K \subseteq L$ be a Galois extension of degree 10 where Char $K = 0$. Is the extension necessarily a radical extension?

(2) Express $\sum_{i \neq j} t_i^3 t_j \in K(t_1, \ldots, t_n)$ as a polynomial in the elementary symmetric polynomials.

(3) Let $L = \mathbb{Q}(x_1, \ldots, x_n)$ where x_i are variables, and let e_i be the i-th symmetric polynomial in these variables. Let $F = \mathbb{Q}(e_1, \ldots, e_n)$, $A = \mathbb{Z}[e_1, \ldots, e_n]$, $B = \mathbb{Z}[x_1, \ldots, x_n]$. Show that $A = B \cap F$.

(4) Let $f = t^5 + 2t + 6 \in \mathbb{Q}[t]$ and let L be a splitting field of f over $\mathbb{Q}$. Considering the reduction $\bar{f} \in \mathbb{F}_3[t]$ show that $\mathrm{Gal}(L/\mathbb{Q})$ contains a transpose when considered as a subgroup of S_5.

(5) Show that $t^4 + 1$ is reducible over every finite field $\mathbb{F}_q$. Let p be an odd prime. By considering the splitting field of $t^2 + 1$ over $\mathbb{F}_p$, show that -1 is a quadratic residue mod p iff $p \equiv 1 \bmod 4$. If ζ a root of $t^4 + 1$, show that $(\zeta + \zeta^{-1})^2 = 2$. Hence show that 2 is a quadratic residue mod p iff $p \equiv \pm 1 \bmod 8$.

(6) Show that the minimal polynomial of $\sqrt{3} + \sqrt{5}$ over $\mathbb{Q}$ is reducible modulo p for all primes p.

(7) Describe the function $\mathrm{tr}_{\mathbb{C}/\mathbb{R}}$, $\mathrm{N}_{\mathbb{C}/\mathbb{R}}$, $\mathrm{tr}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}$, and $\mathrm{N}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}$ where $m \in \mathbb{Z}$.

(8) Let $f = t^8 - 2 \in \mathbb{Q}[t]$ and let L be a splitting field of f over $\mathbb{Q}$. Let $\alpha = \sqrt[8]{2}$. Calculate $\mathrm{tr}_{L/\mathbb{Q}}(\alpha)$, $\mathrm{N}_{L/\mathbb{Q}}(\alpha)$, $\mathrm{tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$, and $\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$.

(9) Suppose p is an odd prime, $\mu = \exp(2\pi i/p)$ where $i = \sqrt{-1}$, and let $L = \mathbb{Q}(\mu)$. If f denotes the corresponding cyclotomic polynomial Φ_p, show that $f'(\mu) = p\mu^{p-1}/(\mu - 1)$. Prove that the norm $\mathrm{N}_{L/\mathbb{Q}}(f'(\mu)) = p^{p-2}$.

(10) Let $K \subseteq F \subseteq L$ be finite separable extensions. Show that the formula $\mathrm{N}_{L/K}(\alpha) = \mathrm{N}_{F/K}(\mathrm{N}_{L/F}(\alpha))$ holds for every $\alpha \in L$.

(11) *Hilbert's theorem 90.* Let $K \subseteq L$ be a cyclic extension and let φ be a generator of $\mathrm{Gal}(L/K)$. Show that for $\alpha \in$ Ł, we have: $\alpha = \frac{\beta}{\varphi(\beta)}$ for some $\beta \in L$ iff $\mathrm{N}_{L/K}(\alpha) = 1$.

(12) Let f be an irreducible cubic polynomial over a field K with char $K \neq 2, 3$, and let α be a square root of the discriminant of f. Show that f remains irreducible over $K(\alpha)$.

(13) Assume $f = t^n + at + b \in K[t]$ is irreducible and separable. Calculate the discriminant D_f in terms of the coefficients a, b.

(14) Let $f = t^5 + 20t + 16 \in \mathbb{Q}[t]$ and let L be a splitting field of f over $\mathbb{Q}$. Show that $\mathrm{Gal}(L/K)$ is isomorphic to A_5. [Hint: use discriminants, reduction mod primes, etc. Also you may assume that A_5 has no proper subgroup of index $2, 3$, or 4.]

(15) Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a Galois extension of $\mathbb{Q}$ and find its Galois group.

(16) Optional: Let $p_1, p_2, \ldots, p_n$ denote the first n primes, and let $L = \mathbb{Q}(\sqrt{p}_1, \sqrt{p}_2, \ldots, \sqrt{p}_n)$. Show that this is a Galois extension of degree 2^n with Galois group isomorphic to $(\mathbb{Z}/\langle 2\rangle)^n$.