GALOIS THEORY EXAMPLES

NIS–B

0. Refresh your memory, by reading either your notes from the Rings and Modules course or some other source, such as van der Waerden vol. 1, ch. 3, of the following topics: fields, polynomial rings, ideals, taking quotients of rings by ideals, principal ideal domains (PIDs), prime ideals, maximal ideals, unique factorization in PIDs.

1.(i) Let $K = \mathbb{Q}(\alpha)$ where α is the real cube root of 2. Write the inverses of $1 + \alpha$ and $1 + \alpha^2$ as polynomials in α with rational coefficients.

(ii) Put $\omega = \exp(2\pi i/3)$. Show that $\mathbb{Q}(\omega\alpha)$ is isomorphic to $\mathbb{Q}(\alpha)$.

2. Let $K = \mathbb{Q}(\alpha)$ with $\alpha^3 = 2$. Find $\mathrm{Aut}(K/\mathbb{Q})$.

3. Prove that any finite integral domain is a field. (Hint: Show that multiplication by any nonzero element is an isomorphism of sets.)

Suppose that L is an integral domain containing a field K such that L is finite dimensional as a vector space over K. Prove that L is a field. (Hint: Show that multiplication by any nonzero element is an isomorphism of vector spaces.)

4. Which of the following are fields? Which are integral domains?
   a. $\mathbb{Z}/7\mathbb{Z}$ (the integers modulo 7).
   b. $\mathbb{Z}/8\mathbb{Z}$.
   c. The ring of all continuous functions on the unit interval.
   d. The ring of all meromorphic functions on $\mathbb{C}$.
   e. $\mathbb{Z}[X]/(X^3 - 2)$.
   f. $\mathbb{Z}/2\mathbb{Z}[X]/(X^3 + X + 1)$.
   g. $\mathbb{Q}[X]/(X^4 + X^2 + 1)$.

5. Suppose that $K \hookrightarrow L$ is a field extension such that $[L : K] = 2$ (such an extension is called *quadratic*) and $\mathrm{char}\, K \neq 2$. Show that there is an element $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^2 \in K$. Prove that this extension is Galois, and describe the Galois group together with its action on L.

6. Find all irreducible polynomials over $\mathbb{F}_2$ of degree at most 4. (One method is to use the "sieve of Eratosthenes": Write out all nonconstant polynomials in order of their degree. Then repeatly add the first new uncrossed out polynomial to your list of irreducible polynomials and cross out all polynomials of larger degree divisible by it.)

7. Let α be the complex number $e^{2\pi i/5}$. Show that $\mathbb{Q}[\alpha]$ is a field of degree 4 over $\mathbb{Q}$. Show that it contains the field $\mathbb{Q}(\sqrt{5})$. (Hint: $\alpha + 1/\alpha$.)

8. Show that $\binom{p}{n}$ is divisible by p whenever p is prime and $0 < n < p$. If K is a field of characteristic p (this means that $p = 0$ in K, for example Z_p) show that

$(x+y)^p = x^p + y^p$. If f is the function such that $f(k) = k^p$ for $k \in K$ show that f is an isomorphism from the field K to a subfield of K. (It is called the Frobenius endomorphism.)

9. Find the highest common factors of the polynomials X^3-3 and X^2-4 in $\mathbb{Q}[X]$ and in $\mathbb{F}_5[X]$. In each case write the highest common factor in the form $(X^3-3)a(X)+(X^2-4)b(X)$ for polynomials $a(X)$ and $b(X)$.

10. Let I, J, and K be the matrices $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, and $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. (These are the Pauli spin matrices from quantum mechanics multiplied by $i = \sqrt{-1}$.)

Show that $I^2 = J^2 = K^2 = IJK = -1$, $IJ = -JI = K$, $JK = -KJ = I$, $KI = -IK = J$.

Define the ring $\mathbb{H}$ of quaternions to be the matrices of the form $a + bI + cJ + dK$ with a, b, c, d real. (Note that $\mathbb{H}$ is a *non-commutative* ring.) Show that the determinant of this matrix is $a^2 + b^2 + c^2 + d^2$ and deduce that every nonzero element of $\mathbb{H}$ has an inverse. (A ring such that every nonzero element has an inverse is called a *skew field* or *division ring*.) What is the inverse of $a + bI + cJ + dK$?

Show that $\mathbb{H}$ has an infinite number of automorphisms fixing every element of the subring $\mathbb{R}$ of diagonal matrices. (Hint: consider conjugation by quaternions.)

11. Suppose the roots of $X^3 - e_1X^2 + e_2X - e_3$ are α, β, and γ. Write $1/\alpha + 1/\beta + 1/\gamma$, $\alpha^2 + \beta^2 + \gamma^2$, and $\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2$ in terms of e_1, e_2, and e_3. Find a polynomial whose roots are α^2, β^2 and γ^2.

12. (Newton's identities.) Let $f(X)$ be the polynomial $X^n - e_1X^{n-1} + \ldots + (-1)^n e_n \in \mathbb{C}[X]$ with roots $\alpha_1, \ldots \alpha_n$ and let p_j be $\alpha_1^j + \ldots + \alpha_n^j$. Show that if $|X|$ is large enough then

$$\frac{Xf'(X)}{f(X)} = \sum_{1 \le k \le n} \frac{1}{1 - \alpha_k/X} = \sum_{j \ge 0} p_j X^{-j}.$$

(Hint: look at the derivative of $\log \prod_i (X - \alpha_i)$.) Use this to prove

$$\begin{aligned}
p_1 &= e_1 \\
p_2 &= p_1e_1 - 2e_2 \\
&\ldots \\
p_{n-1} &= p_{n-2}e_1 - p_{n-3}e_2 + \ldots - (-1)^n p_1 e_{n-2} + (-1)^n (n-1) e_{n-1} \\
p_k &= p_{k-1}e_1 - p_{k-2}e_2 + \ldots - (-1)^n p_{k-n} e_n \quad (k \ge n).
\end{aligned}$$

Use this to prove that all the p's can be written as polynomials in the e's. (Remark: These identities are used in group representation theory and algebraic topology to express the exterior powers e_i of a representation or vector bundle in terms of the Adams operations p_i. For example $e_2 = (e_1^2 - p_2)/2$ implies the formula $\mathrm{Tr}(g|\Lambda^2(V)) = (\mathrm{Tr}(g|V \otimes V) - \mathrm{Tr}(g^2|V))/2$ from the representation theory course.)

13. We keep the notation of question 12. Show that $\delta = \prod_{i>j}(\alpha_i - \alpha_j)$ is equal to the Vandermonde determinant

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \dots & \dots & \dots & \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix}.$$

(Hint: Show that the Vandermonde determinant is 0 whenever two of the α's are equal.) By multiplying this matrix by its transpose show that the discriminant $\Delta = \delta^2$ of f is the determinant of the matrix

$$\begin{vmatrix} p_0 & p_1 & \dots & p_{n-1} \\ p_1 & p_2 & \dots & p_n \\ \dots & \dots & \dots & \dots \\ p_{n-1} & p_n & \dots & p_{2n-2} \end{vmatrix}.$$

If α, β, γ are the roots of $X^3 - e_1X^2 + e_2X - e_3$ then express $(\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2$ in terms of e_1, e_2, and e_3.

14. We keep the notation of questions 12 and 13 with $n = 3$, so that $f(X) = X^3 - e_1X^2 + e_2X - e_3$. Let ω be a primitive cube root of 1. Express $(\alpha + \omega\beta + \omega^2\gamma)^3$ and $(\alpha + \omega^2\beta + \omega\gamma)^3$ in terms of e_1, e_2, e_3, and $\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$. Deduce that the roots of a cubic polynomial can be written explicitly in terms of the coefficients by using field operations and extraction of square and cube roots. (First show that $\alpha + \beta + \gamma$, $\alpha + \omega\beta + \omega^2\gamma$, and $\alpha + \omega^2\beta + \omega\gamma$ can be written in this form by using the result of the previous exercise to express δ in this form.) Do not try to write the roots out explicitly unless you are unusually obstinate; the expressions are very complicated!

15. Find all subgroups of S_3 (the symmetric group). Let $L = \mathbb{Q}(x_1, x_2, x_3)$ be the field of rational functions in 3 variables, with S_3 acting in the obvious way by permuting the variables x_1, x_2, x_3. Recall (Newton's theorem on symmetric functions) that the fixed field under this group is $K = \mathbb{Q}(e_1, e_2, e_3)$ where the e's are defined by $(x-x_1)(x-x_2)(x-x_3) = x^3 - e_1x^2 + e_2x - e_3$. Find all the subfields of L containing K. (Hint: use the fundamental theorem of Galois theory, and look at Question 14.)

16. Is true that if $K \hookrightarrow L$ and $L \hookrightarrow M$ are Galois extensions, then $K \hookrightarrow M$ is also Galois? (Hint: consider composites of quadratic extensions.)
17. Suppose that $p_1, \dots, p_r$ are distinct prime numbers and that $K = \mathbb{Q}(\sqrt{p}_1, \dots, \sqrt{p}_r)$. Show that $K/\mathbb{Q}$ is a Galois extension, and compute its Galois group. Show also that $K = \mathbb{Q}(\sqrt{p}_1 + \dots + \sqrt{p}_r)$.

18. Let $K = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$. Show that $K/\mathbb{Q}$ is Galois and compute its Galois group.

19. Prove Eisenstein's criterion: if p is a prime number and and $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$ is a polynomial with $p|a_i$ $(0 \leq i < n)$ and p^2 does not divide a_0, then f is irreducible. If n is any positive integer, show that $(x^{p^n} - 1)/(x^{p^{n-1}} - 1) = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \ldots + x^{p^{n-1}} + 1$ is irreducible. (Hint: change x to $x + 1$ and apply Eisenstein.)

20. Let $\alpha = e^{2\pi i/p^n}$. Show that $[\mathbb{Q}[\alpha] : \mathbb{Q}] = (p-1)p^{n-1}$. Show that if m is coprime to p then there is an automorphism of $\mathbb{Q}[\alpha]$ taking α to α^m. Show that the Galois group $Gal(\mathbb{Q}[\alpha]/\mathbb{Q})$ is isomorphic to the group of units in the ring $\mathbb{Z}/(p^n)$.

21. This question shows that if x is an indeterminate, then the group $\mathrm{Aut}(K(x)/K)$ is isomorphic to $PGL_2(K) = GL_2(K)/A$, where A is the subgroup of elements of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ act on $K(x)$ by fixing K and mapping x to $(ax + b)/(cx + d)$. Show that this gives a homomorphism of groups from $PGL_2(K)$ into $\mathrm{Aut}(K(x)/K)$. Show that any homomorphism of $K(x)$ to itself fixing K maps x to $t = p(x)/q(x)$ for some coprime polynomials $p(x)$ and $q(x)$ in $K(x)$ (not both constant, $q \neq 0$), and conversely there is a homomorphism for any such pair of polynomials. Show that the polynomial $q(y)t - p(y) \in K(t)[y]$ is irreducible and is the minimal polynomial satisfied by x over the field $K(t)$. Show that $[K(x) : K(t)] = \max(\deg(p), \deg(q))$ and deduce that if the homomorphism is onto then p and q both have degree at most 1. Show that $\mathrm{Aut}(K(x)/K) = PGL_2(K)$.

22. Show that the automorphisms of $K(x)$ given by $x \to 1 - x$ and $x \to 1/x$ generate a group G of order 6 isomorphic to the symmetric group S_3. Let t be the element $(x^2 - x + 1)^3/x^2(x-1)^2$ Show that t is fixed by G, and show that $[K(x) : K(t)] \leq 6$ (by finding a polynomial of degree 6 with coefficients in $K(t)$ having x as a root). Deduce that $[K(x) : K(t)] = 6$ and that $K(t)$ is the field of all elements of $K(x)$ fixed by G. Find all the 6 subgroups of G and for each one find the subfield of $K(x)$ of elements fixed by it.

(This action of S_3 on $K(x)$ arises in the following way. Suppose that x is the cross-ratio $x = (x_4 - x_1)(x_3 - x_2)/(x_3 - x_4)(x_2 - x_1)$; this definition makes the cross-ratio of $(0, 1, \infty, \lambda)$ equal to λ. The symmetric group S_4 permutes the variables $x_1, \ldots, x_4$, and the subgroup V consisting of the identity and permutations with cycle type $(2, 2)$ leaves the cross-ratio invariant. The transposition (13) sends $x \to 1/x$ and (12) sends $x \to x - 1$, so that the quotient group $S_4/V \cong S_3$ acts as described.)

23. Find all the subfields of $\mathbb{Q}[e^{2\pi i/7}]$.

24. Suppose that p is an odd prime, and let $\tau = \sum_{0 \leq n < p} e^{2\pi i n^2/p}$. Show that $\tau\bar{\tau} = p$. If -1 is a square mod p show that τ is real, and if -1 is not a square mod p show that $\tau + \bar{\tau} = 0$, so that τ is imaginary. Show that $L = \mathbb{Q}[e^{2\pi i/p}]$ has a unique subfield K of degree 2 over $\mathbb{Q}$ (hint: $(\mathbb{Z}/p\mathbb{Z})^*$ (* denoting group of units) is cyclic). Describe K explicitly. Show that if $m|n$ then $\mathbb{Q}[e^{2\pi i/m}] \subset \mathbb{Q}[e^{2\pi i/n}]$. Show that if k is any nonzero integer then $\mathbb{Q}[\sqrt{k}]$ is contained in the field $\mathbb{Q}[e^{2\pi i/4k}]$.

(This can be done more easily using the discriminant of the ring of integers in a number field. By Vandermonde's identity (q. 13) the discriminant of $\mathcal{O}_L$ is (up to sign) a power of p, so that the discriminant of $\mathcal{O}_K$ is too. Now use the fact that K is quadratic to determine it.)

Remark A field extension is *Abelian* if it is Galois and the Galois group is Abelian. The Kronecker-Weber theorem states that any Abelian extension of $\mathbb{Q}$ is a subfield of some cyclotomic field. The proof is much deeper than anything in this course and belongs to class field theory. See e.g. "Algebraic Number Theory" (ed. Cassels and Fröhlich) or "Class Field Theory" by Artin and Tate.

25. Let L be the splitting field of $x^4 - 3$ over $\mathbb{Q}$.
    a. Show that $[L : \mathbb{Q}] = 8$ and the Galois group is the dihedral D_8 group of order 8.
    b. List all the subgroups of D_8 (there are (is?) 1 of order 1, 5 of order 2, 3 of order 4, and 1 of order 8). Draw a diagram showing which subgroups are contained in which.
    c. Find the subfields corresponding to each subgroup and draw a diagram showing their inclusions.
    d. For each subfield M work out the Galois group of L/M. Find the 6 subfields M that are Galois extensions of $\mathbb{Q}$, and for each work out the Galois group $Gal(M/\mathbb{Q})$.

26. Repeat question 25 for the (reducible) polynomial $x^4 - 4$ (except that this time $L/\mathbb{Q}$ has degree 4 and Galois group $(\mathbb{Z}/2\mathbb{Z})^2$).

27. Repeat question 25 for the polynomial $x^3 + 2x + 6$. (This time the Galois group has order 6).

28. Find the Galois group of the (splitting field of the) polynomial $x^4 + x^3 + 1$ over the finite fields $\mathbb{F}_2$, $\mathbb{F}_3$, and $\mathbb{F}_4$.
    (You should get 3 different answers. Recall that if f is any irreducible polynomial of degree n over a finite field, then the extension generated by 1 root of f is already Galois, with Galois group cyclic of order n.)

29. Show that any irreducible polynomial in $\mathbb{F}_q[x]$ of degree dividing n splits into linear factors over the field $\mathbb{F}_{q^n}$.

30.
    a. For each prime p find an irreducible polynomial of degree p with exactly two non-real roots. (Hint: try a polynomial of the form $x^p - (mp)^3 x(x-1)(x-2)\ldots(x-(p-4)) - p$ for some large integer m coprime to p. Show that for m large it has $p-2$ real roots (close to $0, 1, \ldots, p-5, p-4$, and mp), and use Eisenstein to show that it is irreducible.)
    b. Show that for each prime p there is a Galois extension of $\mathbb{Q}$ with Galois group S_p. (Recall that any subgroup of S_p of order divisible by p and containing a transposition must be S_p.)

c. Show that any finite group is a subgroup of the symmetric group S_p for some prime p. (Hint: recall that letting a group of order n act on its own elements by left multiplication makes it into a subgroup of S_n).

d. Show that for any finite group G, there are finite extensions $M \subset L$ of $\mathbb{Q}$ such that L/M is Galois with Galois group G. (Hint: recall that if $\mathbb{Q} \subset M \subset L$ and $\mathbb{Q} \subset L$ is Galois, then $M \subset L$ is Galois with Galois group equal to the subgroup of G corresponding to M.) The "inverse problem" of Galois theory asks whether for any finite group G there is an extension $L/\mathbb{Q}$ of $\mathbb{Q}$ which is Galois with Galois group G; it is an extremely difficult unsolved problem. See Serre's "Topics in Galois Theory" (1992) for a statement (complete up to about 1990) of what is known, together with a description of various techniques, mostly from algebraic geometry and number theory.

31. This question shows that it is not possible to trisect an angle or duplicate a cube using ruler and compass. A complex number is called Euclidean if it can be obtained from rational numbers using the usual field operations and taking square roots.

a. Show that a number is Euclidean if and only if its real and imaginary parts are both constructible by ruler and compass from a line segment of length 1. (This is long but straightforward and can be missed out. In one direction show that the coordinates of the point of intersection of (say) two circles can be written in terms of their centers and radii using the operations above. In the other direction you need to find constructions for the product of two constructible numbers and the square root of a constructible number and so on.)

b. Show that a is a Euclidean number if and only if there is a finite tower of fields $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$ such that $[K_n : K_{n-1}] = 2$ and $a \in K_n$.

c. Show that the irreducible polynomial satisfied by any Euclidean number has degree a power of 2. (Hint: $[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}[a]][\mathbb{Q}[a] : \mathbb{Q}]$.)

d. Show that it is not possible to construct $2^{1/3}$ with ruler and compass (in other words, duplicate the cube).

e. Find an irreducible polynomial of degree 3 satisfied by $\cos(2\pi/9)$ and deduce that it is not possible to trisect an angle of $\pi/3$ using ruler and compass. (Hint: $\cos(2\pi/9) = (\alpha + \alpha^{-1})/2$ where α is a root of $(x^9 - 1)/(x^3 - 1)$.)
It is not possible to square the circle because π s transcendental, but this is much more difficult to prove. (See chapter 6 of Stewart's book for a proof.)

32. Let F_q be the finite field of prime power order q. This exercise finds the number of irreducible polynomials of some degree in $F_q[x]$.

a. Show that an irreducible polynomial in $F_q[x]$ of degree m divides $x^{q^n} - x$ if and only if $m|n$. (Hint: use that fact that the splitting field F_{q^n} of $x^{q^n} - x$ contains F_{q^m} if and only if $m|n$.)

b. Show that $x^{q^n} - x$ is the product of all irreducible polynomials in $F_q[x]$ of degree dividing n which have leading coefficient 1. Check this explicitly for $q = 2$, $n = 4$ using the list of irreducible polynomials over F_2 in example sheet 1.

c. If $a_n(q)$ is the number of irreducible polynomials of degree n over F_q with leading coefficient 1 then show (by looking at the degree of $x^{q^n} - x$) that

$$\sum_{d|n} d\, a_d(q) = q^n.$$

d. Use this to calculate the number of irreducible polynomials of degree 6 over F_2.

e. If you know about the Möbius function $\mu(n)$ then use the Möbius inversion formula to show that

$$a_n(q) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d.$$

33. Show that any irreducible polynomial in $F_q[x]$ of degree dividing n splits into linear factors over the field F_{q^n}. (Hint: either use the previous question, or use the fact that any two finite fields of order q^n are isomorphic.)

34. Recall that any finite separable extension is generated by a single element, and has only a finite number of intermediate fields. In this exercise we show that this is not always true for non separable extensions. Let L be the field $F_p(x, y)$ of rational functions in two variables, and let K be the subfield $F_p(x^p, y^p)$.
    a. Show that $[L : K] = p^2$. (Hint: look at $K \subset K[x] \subset L$.)
    b. Show that the Frobenius endomorphism is an isomorphism from L onto K.
    c. Show that every element of L not in K generates and extension of degree p of K. (Hint: show that it is a root of an equation of the form $t^p - a \in K[t]$.)
    d. Show that there are an infinite number of extensions of K contained in L, and that L is not generated over K by any single element.

35 (i) Consider the action of the symmetric group S_n on the field $L = \mathbb{Q}(X_1, \ldots, X_n)$. Show that the field L^{A_n} of invariants under the alternating group is $\mathbb{Q}(\sigma_1, \ldots, \sigma_n, \delta)$, where $\delta = \prod_{i>j}(X_i - X_j)$ is the square root of the discriminant and $\sigma_1, \ldots, \sigma_n$ are the elementary symmetric functions.
(ii) An element $f \in \mathbb{Z}[X_1, \ldots, X_n]$ is *anti-invariant* if $\tau(f) = \mathrm{sgn}(\tau) f$ for all $\tau \in S_n$, where $\mathrm{sgn}(\tau)$ is the signature of τ. Show that if f is anti-invariant, then it is divisible by δ. (That is, f/δ is a symmetric polynomial.)
(Remark: (ii) has applications in the representation theory of compact Lie groups, notably to proving the Weyl denominator formula.)

36 Suppose that f is an irreducible polynomial over $\mathbb{Q}$ of degree n. Show that the Galois group of f is a subgroup of the alternating group A_n if and only if the discriminant of f is a square in $\mathbb{Q}$.

37 Suppose that f is an irreducible cubic polynomial over $\mathbb{Q}$ with just one real root. Show that the Galois group of f is S_3.

38 This question describes a technique involving reduction modulo p for finding various kinds of elements in Galois groups of splitting fields.

The result is this: suppose that $f \in \mathbb{Z}[X]$ is a polynomial of degree n with leading coefficient a_n and that f has no repeated roots. Suppose that p is a prime number such that a_n is prime to p and that $\bar{f}$, the reduction of f modulo p, also has no repeated roots. Let $\bar{f} = \phi_1 \ldots . \phi_r$ be the prime factorization of $\bar{f}$ in $\mathbb{F}_p[X]$. Say $\deg \phi_i = n_i$. Then $\mathrm{Gal}(f)$, regarded as a subgroup of the symmetric group S_n, has an element whose cycle type is $(n_1, \ldots, n_r)$.

The rest of this question is concerned with proving this; the following questions give examples of its use.

Fix some notation: K is a field, $f \in K[x]$ is of degree n and has no repeated factors, L is a splitting field for f over K, $G = \mathrm{Gal}(f) = \mathrm{Gal}(L/K)$, which we regard as a subgroup of the symmetric group S_n, and $\rho_1, \ldots, \rho_n \in L$ are the roots of f. $Y_1, \ldots, Y_n$ are independent indeterminates and for any $s \in S_n$ we put

$$H_s = (x - (\rho_{s(1)}Y_1 + \cdots + \rho_{s(n)}Y_n)) \in L(Y_1, \ldots, Y_n)[x].$$

We then set $F = \prod_{s \in S_n} H_s$. Notice that also $F = \prod_{s \in S_n}(x - (\rho_1 Y_{s(1)} + \cdots + \rho_n Y_{s(n)})$.
(i) Show that $F \in K[Y_1, \ldots, Y_n][x]$.
(ii) Suppose that the prime factorization of F in $K(Y_1, \ldots, Y_n)[x]$ is $F = F_1 \ldots . F_r$. By Gauss' lemma, we can assume that $F_i \in K[Y_1, \ldots, Y_n][x]$ for all i. Choose one of the factors $H_s = H$, say, of F_1. By considering $\prod_{g \in G} g(H)$, show that the degree of F_1 is the order of G. Also, consider the permutation action of S_n on the given linear factors H_s of F, and show that G is precisely the subgroup of S_n that preserves each factor F_i.
(iii) Now assume that $f \in \mathbb{Z}[x]$ and that f is monic. Suppose that p is a prime number not dividing the discriminant of f; notice that this is equivalent to the reduction $\bar{f} \in \mathbb{F}_p[x]$ of f having non-zero discriminant. Let k be a splitting field for $\bar{f}$ over $\mathbb{F}_p$, with Galois group $\mathrm{Gal}(k/\mathbb{F}_p) = \mathrm{Gal}(\bar{f})$.

Show that $F_i \in \mathbb{Z}[Y_1, \ldots, Y_n][x]$, and let $\bar{F}_i$ denote the reduction of F_i mod p, so that $\bar{F} = \bar{F}_1 \ldots . \bar{F}_r$. Of course, it is quite possible that some or all of the $\bar{F}_i$ will factorize further; say $\bar{F}_i = \prod_j \Phi_{i,j}$.

Deduce from (ii) that $\mathrm{Gal}(\bar{f})$ is the subgroup of S_n that preserves each factor in the factorization $\bar{F} = \prod_{i,j} \Phi_{i,j}$, and deduce from this that $\mathrm{Gal}(\bar{f})$ is a subgroup of $\mathrm{Gal}(f)$.

[The idea is that you should use (ii) twice, first with $K = \mathbb{Q}$ and secondly with $K = \mathbb{F}_p$, and by comparing what you get, deduce that $\mathrm{Gal}(\bar{f})$ is a subgroup of $\mathrm{Gal}(f)$.]
(iv) Suppose that f, p and $\bar{f}$ are as in (iii), and that the prime factorization of $\bar{f}$ is $\bar{f} = \phi_1 \ldots . \phi_r$, where $\deg \phi_i = n_i$. Use the fact that $\mathrm{Gal}(\bar{f})$ is cyclic (why?) to deduce that $\mathrm{Gal}(f)$ has an element s that is a product of disjoint cycles of lengths $n_1, \ldots, n_r$ respectively.

39 Compute the Galois group of $f = X^4 + X^2 + X + 1$ over $\mathbb{Q}$.

[Hint: test the factorization of f and of its cubic resolvent by reduction modulo small primes. Alternatively use the mod p method described above.]

40 By using Vandermonde's determinant (q. 13) show that the discriminant of $x^n + px + q$ is $(-1)^{n+\eta(n)-1}(n-1)^{n-1}p^n + (-1)^{n+\eta(n-1)-1}n^n q^{n-1}$, where $\eta(n) = 0$ if $n \equiv 0$ or $1 \pmod 4$ and $\eta(n) = 1$ if $n \equiv 3$ or $4 \pmod 4$.

41 Compute the Galois group over $\mathbb{Q}$ of $X^5 + 3X + 1$.

42 (i) Work out the cyclotomic polynomial $\Phi_n(x)$ for $1 \leq n \leq 10$.
(ii) Show that $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ if p is prime.
(iii) If n is odd show that $\Phi_{2n}(x) = \Phi_n(-x)$. (Hint: z is a primitive n'th root of 1 if and only if $-z$ is a primitive $2n$'th root of 1.)
(iv) If p is prime and $p|n$ then show that $\Phi_{pn}(x) = \Phi_n(x^p)$. (Hint: Show that z is a primitive pn'th root of 1 if and only if z^p is a primitive n'th root of 1.)
(v) If p and q are distinct primes show that the nonzero coefficients of $\Phi_{pq}(x)$ are alternately $+1$ and -1. (Hint: First show that if $1/(1-x^p)(1-x^q)$ is expanded in a power series in x, than the coefficient of x^m for $m < pq$ is 0 or 1.)
(vi) If n is not divisible by at least 3 distinct odd primes show that all coefficients of $\Phi_n(x)$ are -1, 0, or 1.
(vii) Work out $\Phi_{3\times5\times7}(x)$.

43 A theorem of Wedderburn says that every finite division ring ("possibly noncommutative ring such that every nonzero element has an inverse") is commutative. (Cf. the ring $\mathbb{H}$ of quaternions.) In this exercise we will use cyclotomic polynomials to prove this. (This argument is due to Witt and can be found on p. 1 of Weil's "Basic Number Theory".)

Let L be a finite division ring, and let K be the centre of L (that is, the set of elements of L that commute with all elements of L). We can suppose by induction that every division ring of order less than that of L is commutative.

(i) Show that K is a field of order q for some prime power q, and L is a vector space over K of dimension n for some integer n, and that the multiplicative group L^* of non-zero elements in L is a group of order $q^n - 1$.
(ii) Show that any subring of L is a division ring (so that by the induction hypothesis any proper subring of L is a field).
(iii) If $a \in L^*$ and is not in the centre of L, then show that the elements of L that commute with a form a field of order q^m for some $m|n$.
(iv) Show that the number of conjugates of a in L^* is of the form $(q^n-1)/(q^m-1)$ for some m dividing n. (Recall that if a is an element of some group G, then the number of conjugates of a is (order of G)/(order of centralizer of a).)
(v) By counting the number of elements in each conjugacy class of L^* show that

$$\#(L^*) = q^n - 1 = q - 1 + \sum_{a_i} (q^n - 1)/(q^{m_i} - 1)$$

where the sum is over a set of representatives a_i of the conjugacy classes of the group L^* which are not in the centre, and the centralizer of a_i is a field of order q^{m_i} $(m_i|n, m_i < n)$. (The term $q-1$ is the number of elements in the centre of L^*.)

(vi) Show that $\Phi_n(q)|(q^n-1)/(q^{m_i}-1)$ for each i and $\Phi_n(q)|q^n-1$, and deduce that $\Phi_n(q)|q-1$. (Φ_n is the n'th cyclotomic polynomial.)
(vii) Show that if $n>1$ then $\Phi_n(q)>q-1$ (using $\Phi_n(x)=\prod_{i\in(Z/nZ)^*}(q-\zeta^i)$) and deduce that $n=1$, so that $L=K$ and is commutative.

44 (i) Show that if p and q are primes and $a^q\equiv 1 \bmod p$ for some integer a then a has order 1 or q in the group $(\mathbb{Z}/p\mathbb{Z})^*$, and deduce that $a\equiv 1 \bmod p$ or $p\equiv 1 \bmod q$.
(ii) If $p\neq q$ and p divides $(a^q-1)/(a-1)=\Phi_q(a)$ show that $p\equiv 1 \bmod q$.
(iii) Deduce that there are an infinite number of primes congruent to 1 mod q. (Hint: If $p_1,\ldots,p_i$ are some set of such primes, consider prime divisors of $\Phi_q(p_1p_2\ldots p_iq)$.)

45 In this exercise we use cyclotomic polynomials to prove the special case $n=1$ of Dirichlet's theorem that any arithmetic progression $mx+n$ with m, n coprime positive integers contains an infinite number of primes.
(i) Show that if m is not divisible by the prime p then the roots of $x^m-1\in\mathbb{F}_p[x]$ are all distinct, and each root has order m. (Recall that f has no multiple roots if f is coprime to f'.)
(ii) Deduce that if neither m nor n are divisible by p and $m\neq n$ then $\Phi_m(x)$ and $\Phi_n(x)$ are coprime in $\mathbb{F}_p[x]$.
(iii) Show that if m, n are integers with m not divisible by p then $\Phi_m(n)\equiv 0 \bmod p$ if and only if m is the smallest integer such that $a^m\equiv 1 \bmod p$.
(iv) Show that if a prime p divides $\Phi_m(n)$ for any positive integers m, n, then either p divides m or $p\equiv 1 \bmod m$. (Use part (iii), and recall that $a^{p-1}\equiv 1 \bmod p$ for any integer a coprime to the prime p.)
(v) Use (iv) to show that there are an infinite number of primes congruent to 1 mod m. (Hint: if $p_1,\ldots p_i$ are any finite set of primes 1 mod m then show that not all prime divisors of $\Phi_m(p_1p_2\ldots p_im+1)$ can divide m, and show that none of them can be $p_1,\ldots,p_i$.)

46 In this question, assume the result of the previous question, that given any integer a there are an infinite number of primes congruent to 1 modulo a.
(i) Show that any finite abelian group G is a quotient group of $(\mathbb{Z}/m\mathbb{Z})^*$ for some integer m. (Hint: recall that any finite abelian group is a product of cyclic groups of order a_i for some integers a_i. Take a set of distinct primes p_i with $p_i\equiv 1 \bmod a_i$, take m to be the product of the p_i's, and use the fact that $(\mathbb{Z}/m\mathbb{Z})^*$ is the product of the groups $(\mathbb{Z}/p_i\mathbb{Z})^*$.)
(ii) Deduce that any finite abelian group G is the Galois group of $L/\mathbb{Q}$ for some finite extension L of the rationals. (Hint: Take L to be a subfield of the field generated by the m'th roots of 1 (with Galois group $(\mathbb{Z}/m\mathbb{Z})^*$), for some suitable m.)
(iii) Find an explicit real number α (written using the cos function) such that $\mathbb{Q}(\alpha)$ is a Galois extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}/23\mathbb{Z}$.