Course 311: Academic Year 2001-02

1. Let x be an integer, and let p be a prime number. Suppose that $x^3 \equiv 1 \pmod{p}$. Prove that either $x \equiv 1 \pmod{p}$ or else $x^2 + x \equiv -1 \pmod{p}$.

2. Let x be a rational number. Suppose that x^n is an integer for some positive integer n. Explain why x must itself be an integer.

3. Find a function $f\colon \mathbb{Z}^3 \to \mathbb{Z}$ with the property that $f(x, y, z) \equiv x \pmod{3}$, $f(x, y, z) \equiv y \pmod{5}$ and $f(x, y, z) \equiv z \pmod{7}$ for all integers x, y, z.

4. Is 273 a quadratic residue or quadratic non-residue of 137?

5. Let p be a prime number. Prove that there exist integers x and y coprime to p satisfying $x^2 + y^2 \equiv 0 \pmod{p}$ if and only if $p \equiv 1 \pmod{4}$.

6. Let p be a odd prime number, and let g be a primitive root of p.

   (a) Let h is an integer satisfying $h \equiv g \pmod{p}$. Explain why the order of the congruence class of h modulo p^2 is either $p - 1$ or $p(p - 1)$. Hence or otherwise prove that h is a primitive root of p^2 if and only if $h^{p-1} \not\equiv 1 \pmod{p^2}$.

   (b) Use the result of (a) to prove that there exists a primitive root of p^2. (This primitive root will be of the form $g + kp$ for some integer k.)

   (c) Let x be an integer, and let m be a positive integer. Use the binomial theorem to prove that if $x \equiv 1 \pmod{p^m}$ and $x \not\equiv 1 \pmod{p^{m+1}}$ then $x^p \equiv 1 \pmod{p^{m+1}}$ and $x \not\equiv 1 \pmod{p^{m+2}}$

   (d) Use the results of previous parts of this question to show that any primitive root of p^2 is a primitive root of p^m for all $m \geq 2$. What does this tell you about the group of congruence classes modulo p^m of integers coprime to p?

   (e) Do the above results hold when $p = 2$ (i.e., when the prime number p is no longer required to be odd)?

7. Let G be a group. An *automorphism* of G is an isomorphism sending G onto itself. Show that the set $\mathrm{Aut}(G)$ of automorphisms of G is a group with respect to the operation of composition of automorphisms.

8. Let G be a group. The *centre* $Z(G)$ of G is defined by

$$Z(G) = \{z \in G : gz = zg \text{ for all } g \in G\}.$$

Prove that the centre $Z(G)$ of a group G is a normal subgroup of G. [In particular, you should show that $Z(G)$ is a subgroup of G.]

9. Let H be a subgroup of a group G. The *normalizer* $N(H)$ of H in G is defined by $N(H) = \{g \in G : gHg^{-1} = H\}$. Verify that $N(H)$ is a subgroup of G and H is a normal subgroup of $N(H)$.

10. (a) Show that the elements of the alternating group A_5 fall into five conjugacy classes, and calculate the number of elements in each conjugacy class. Verify that the sum of the numbers obtained equals the order of A_5.

(b) Any normal subgroup of A_5 is a union of conjugacy classes. Show how information on the sizes of the conjugacy classes of A_5 can be combined with Lagrange's Theorem to show that the group A_5 is simple.

11. (a) Show that the alternating group A_5 has 10 subgroups of order 3. Show also that any two of these subgroups are conjugate.

(b) Show that the alternating group A_5 has 5 subgroups of order 4. Show also that any two of these subgroups are conjugate.

(c) Show that the alternating group A_5 has 6 subgroups of order 5. Show also that any two of these subgroups are conjugate.

12. Use Eisenstein's criterion to verify that the following polynomials are irreducible over $\mathbb{Q}$:—

$$(i)\ t^2 - 2; \qquad (ii)\ t^3 + 9t + 3; \qquad (iii)\ t^5 + 26t + 52.$$

13. Let p be a prime number. Use the fact that the binomial coefficient $\binom{p}{k}$ is divisible by p for all integers k satisfying $0 < k < p$ to show that if $tf(t) = (t+1)^p - 1$ then the polynomial f is irreducible over $\mathbb{Q}$. The *cyclotomic polynomial* $\Phi_p(t)$ is defined by $\Phi_p(t) = 1 + t + t^2 + \cdots + t^{p-1}$ for each prime number p. Show that $t\Phi_p(t+1) = (t+1)^p - 1$, and hence show that the cyclotomic polynomial Φ_p is irreducible over $\mathbb{Q}$ for all prime numbers p.

14. The Fundamental Theorem of Algebra ensures that every non-constant polynomial with complex coefficients factors as a product of polynomials of degree one. Use this result to show that a non-constant polynomial with real coefficients is irreducible over the field $\mathbb{R}$ of real numbers if and only if it is either a polynomial of the form $at+b$ with $a \neq 0$ or a quadratic polynomial of the form $at^2 + bt + c$ with $a \neq 0$ and $b^2 < 4ac$.

15. Let $f_1, f_2, \ldots, f_k$ be non-constant polynomials with coefficients in a field K, and let $g = f_1 f_2 \cdots f_k + 1$. Show that g is not divisible by $f_1, f_2, \ldots, f_k$. Use this result to show that there are infinitely many irreducible polynomials with coefficients in a field K.

16. A complex number z is said to be *algebraic* if there $f(z) = 0$ for some non-zero polynomial f with rational coefficients. Show that $z \in \mathbb{C}$ is algebraic if and only if $\mathbb{Q}(z){:}\,\mathbb{Q}$ is a finite extension Then use the Tower Law to prove that the set of all algebraic numbers is a subfield of $\mathbb{C}$.

17. Let K, L and M be fields satisfying $K \subset L \subset M$. Suppose that the field extensions $M{:}\,L$ and $L{:}\,K$ are algebraic (but not necessarily finite). Prove that the extension $M{:}\,K$ is algebraic.

18. Let L be a splitting field for a polynomial of degree n with coefficients in K. Prove that $[L{:}\,K] \leq n!$.

19. (a) Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and $[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}] = 4$. What is the degree of the minimum polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$?

    (b) Show that $\sqrt{2}+\sqrt{3}$ is a root of the polynomial $t^4 - 10t^2 + 1$, and thus show that this polynomial is an irreducible polynomial whose splitting field over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

    (c) Find all $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, and show that they constitute a group of order 4 isomorphic to a direct product of two cyclic groups of order 2.

20. Let K be a field of characteristic p, where p is prime.

    (a) Show that $f \in K[t]$ satisfies $Df = 0$ if and only if $f(t) = g(t^p)$ for some $g \in K[t]$.

    (b) Let $h(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$, where $a_0, a_1, \ldots, a_n \in K$. Show that $(h(t))^p = g(t^p)$, where $g(t) = a_0^p + a_1^p t + a_2^p t^2 + \cdots + a_n^p t^n$.

(c) Now suppose that Frobenius monomorphism of K is an automorphism of K. Show that $f \in K[t]$ satisfies $Df = 0$ if and only if $f(t) = (h(t))^p$ for some $h \in K[t]$. Hence show that $Df \neq 0$ for any irreducible polynomial f in $K[t]$.

(d) Use these results to show that every algebraic extension $L\colon K$ of a finite field K is separable.

21. A field K is said to be *algebraically closed* if every non-constant polynomial with coefficients in K splits over K. Use the fact that the number of irreducible polynomials with coefficients in a given field K is infinite to prove that any algebraically closed field must be infinite.

22. For each positive integer n, let ω_n be the primitive nth root of unity in $\mathbb{C}$ given by $\omega_n = \exp(2\pi i/n)$, where $i = \sqrt{-1}$.

    (a) Show that the field extensions $\mathbb{Q}(\omega_n)\colon \mathbb{Q}$ and $\mathbb{Q}(\omega_n, i)\colon \mathbb{Q}$ are normal field extensions for all positive integers n.

    (b) Show that the minimum polynomial of ω_p over $\mathbb{Q}$ is the *cyclotomic polynomial* $\Phi_p(t)$ given by $\Phi_p(t) = 1 + t + t^2 + \cdots + t^{p-1}$. Hence show that $[\mathbb{Q}(\omega_p)\colon \mathbb{Q}] = p - 1$ if p is prime.

    (c) Let p be prime and let $\alpha_k = \omega_{p^2}\omega_p^k = \exp(2\pi i(1 + kp)/p^2)$ for all integers k. Note that $\alpha_0 = \omega_{p^2}$ and $\alpha_k = \alpha_l$ if and only if $k \equiv l \bmod p$. Show that if θ is an automorphism of $\mathbb{Q}(\omega_{p^2})$ which fixes $\mathbb{Q}(\omega_p)$ then there exists some integer m such that $\theta(\alpha_k) = \alpha_{k+m}$ for all integers k. Hence show that $\alpha_0, \alpha_1, \ldots, \alpha_{p-1}$ all belong to the orbit of ω_{p^2} under the action of the Galois group $\Gamma(\mathbb{Q}(\omega_{p^2})\colon \mathbb{Q}(\omega_p))$. Use this result to show that $[\mathbb{Q}(\omega_{p^2})\colon \mathbb{Q}(\omega_p)] = p$ and $[\mathbb{Q}(\omega_{p^2})\colon \mathbb{Q}] = p(p-1)$.

23. Show that the field $\mathbb{Q}(\xi, \omega)$ is a splitting field for the polynomial $t^5 - 2$ over $\mathbb{Q}$, where $\omega = \omega_5 = \exp(2\pi i/5)$ and $\xi = \sqrt[5]{2}$. Show that $[\mathbb{Q}(\xi, \omega)\colon \mathbb{Q}] = 20$ and the Galois $\Gamma(\mathbb{Q}(\xi, \omega)\colon \mathbb{Q})$ consists of the automorphisms $\theta_{r,s}$ for $r = 1, 2, 3, 4$ and $s = 0, 1, 2, 3, 4$, where $\theta_{r,s}(\omega) = \omega^r$ and $\theta_{r,s}(\xi) = \omega^s \xi$.

24. Let f be a monic polynomial of degree n with coefficients in a field K. Then

    $$f(t) = (t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_n),$$

    where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of f in some splitting field L for f over K. The *discriminant* of the polynomial f is the quantity δ^2, where

δ is the product $\prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)$ of the quantities $\alpha_j - \alpha_i$ taken over all pairs of integers i and j satisfying $1 \le i < j \le n$.

Show that the quantity δ changes sign whenever α_i is interchanged with α_{i+1} for some i between 1 and $n-1$. Hence show that $\theta(\delta) = \delta$ for all automorphisms θ in the Galois group $\Gamma(L{:}\,K)$ that induce even permutations of the roots of f, and $\theta(\delta) = -\delta$ for all automorphisms θ in $\Gamma(L{:}\,K)$ that induce odd permutations of the roots. Then apply the Galois correspondence to show that the discriminant δ^2 of the polynomial f belongs to the field K containing the coefficients of f, and the field $K(\delta)$ is the fixed field of the subgroup of $\Gamma(L{:}\,K)$ consisting of those automorphisms in $\Gamma(L{:}\,K)$ that induce even permutations of the roots of f. Hence show that $\delta \in K$ if and only if all automorphisms in the Galois group $\Gamma(L{:}\,K)$ induce even permutations of the roots of f.

25. (a) Show that the discriminant of the quadratic polynomial $t^2 + bt + c$ is $b^2 - 4c$.

    (b) Show that the discriminant of the cubic polynomial $t^3 - pt - q$ is $4p^2 - 27q^2$.

26. Let $f(t) = t^3 - pt - q$ be a cubic polynomial with complex coefficients p and q, and let the complex numbers α, β and γ be the roots of f.

    (a) Give formulae for the coefficients p and q of f in terms of the roots α, β and γ of f, and verify that $\alpha + \beta + \gamma = 0$ and

$$\alpha^3 + \beta^3 + \gamma^3 = 3\alpha\beta\gamma = 3q$$

    (b) Let $\lambda = \alpha + \omega\beta + \omega^2\gamma$ and $\mu = \alpha + \omega^2\beta + \omega\gamma$, where ω is the complex cube root of unity given by $\omega = \frac{1}{2}(-1 + \sqrt{3}i)$. Verify that $1 + \omega + \omega^2 = 0$, and use this result to show that

$$\alpha = \frac{1}{3}(\lambda + \mu), \qquad \beta = \frac{1}{3}(\omega^2\lambda + \omega\mu), \qquad \gamma = \frac{1}{3}(\omega\lambda + \omega^2\mu).$$

    (c) Let K be the subfield $\mathbb{Q}(p, q)$ of $\mathbb{C}$ generated by the coefficients of the polynomial f, and let M be a splitting field for the polynomial f over $K(\omega)$. Show that the extension $M{:}\,K$ is normal, and is thus a Galois extension. Show that any automorphism in the Galois group $\Gamma(M{:}\,K)$ permutes the roots α, β and γ of f and either fixes ω or else sends ω to ω^2.

(d) Let $\theta \in \Gamma(M\colon K)$ be a K-automorphism of M. Suppose that

$$\theta(\alpha) = \beta, \quad \theta(\beta) = \gamma, \quad \theta(\gamma) = \alpha.$$

Show that if $\theta(\omega) = \omega$ then $\theta(\lambda) = \omega^2\lambda$ and $\theta(\mu) = \omega\mu$. Show also that if $\theta(\omega) = \omega^2$ then $\theta(\lambda) = \omega\mu$ and $\theta(\mu) = \omega^2\lambda$. Hence show that $\lambda\mu$ and $\lambda^3 + \mu^3$ are fixed by any automorphism in $\Gamma(M\colon K)$ that cyclically permutes α, β, γ. Show also that the quantities $\lambda\mu$ and $\lambda^3 + \mu^3$ are also fixed by any automorphism in $\Gamma(M\colon K)$ that interchanges two of the roots of f whilst leaving the third root fixed. Hence prove that $\lambda\mu$ and $\lambda^3 + \mu^3$ belong to the field K generated by the coefficients of f and can therefore be expressed as rational functions of p and q.

(e) Show by direct calculation that $\lambda\mu = 3p$ and $\lambda^3 + \mu^3 = 27q$. Hence show that λ^3 and μ^3 are roots of the quadratic polynomial $t^2 - 27qt + 27p^3$. Use this result to verify that the roots of the cubic polynomial $t^3 - pt - q$ are of the form

$$\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}}$$

where the two cube roots must be chosen so as to ensure that their product is equal to $\frac{1}{3}p$.