Part IB

Groups Rings and Modules

Year

Paper 2, Section I

1E Groups, Rings and Modules

Let R be a commutative ring. Show that the following statements are equivalent.

(i) There exists $e \in R$ with $e^2 = e$ and $e \neq 0, 1$.

(ii) $R \cong R_1 \times R_2$ for some non-trivial rings R_1 and R_2.

Let $R = \{(a, b) \in \mathbb{Z}^2 \mid a \equiv b \pmod{2}\}$. Show that R is a ring under componentwise operations. Is R an integral domain? Is R isomorphic to a product of non-trivial rings?

Paper 3, Section I

1E Groups, Rings and Modules

Let F be a finite field of order q. Let $G = \mathrm{GL}_2(F)/Z$ where $Z \leqslant \mathrm{GL}_2(F)$ is the subgroup of scalar matrices. Define an action of $\mathrm{GL}_2(F)$ on $F \cup \{\infty\}$ and use this to show that there is an injective group homomorphism

$$\phi : G \to S_{q+1}.$$

Now let $F = \mathbb{F}_2[\omega]/(\omega^2 + \omega + 1) = \{0, 1, \omega, \omega + 1\}$ be the field with $q = 4$ elements (where $\mathbb{F}_2 = \{0, 1\}$ is the field with 2 elements). Compute the order of G, find a Sylow 2-subgroup P of G, and show that $\phi(P) \leqslant A_5$.

Paper 1, Section II

9E Groups, Rings and Modules

Let R be a Noetherian integral domain with field of fractions F. Prove that the following statements are equivalent.

(i) R is a principal ideal domain.

(ii) Every pair of elements $a, b \in R$ has a greatest common divisor which can be written in the form $ra + sb$ for some $r, s \in R$.

(iii) Every finitely generated R-submodule of F is cyclic.

(iv) Every R-submodule of R^n can be generated by n elements.

Show that any integral domain that is isomorphic to $\mathbb{Z}^n$ as a group under addition is Noetherian as a ring. Find an example of such a ring that does *not* satisfy conditions (i)-(iv). Justify your answer.

Paper 2, Section II

9E Groups, Rings and Modules

(a) Let P be a Sylow p-subgroup of a group G, and let Q be any p-subgroup of G. Prove that $Q \leqslant gPg^{-1}$ for some $g \in G$. State the remaining Sylow theorems.

(b) Let G be a group acting faithfully and transitively on a set X of size 7. Suppose that

(i) for every $x \in X$ we have $\mathrm{Stab}_G(x) \cong S_4$,

(ii) for every $x, y \in X$ distinct we have $\mathrm{Stab}_G(x) \cap \mathrm{Stab}_G(y) \cong C_2 \times C_2$.

Determine the order of G and its number of Sylow p-subgroups for each prime p. [*Hint: For one of the primes p it may help to use the following fact, which you may assume. If H is a subgroup of S_p of order p then the normaliser of H in S_p has order* $p(p-1)$.]

Deduce that no proper normal subgroup of G has order divisible by 3 or order divisible by 7. Hence or otherwise prove that G is simple.

Paper 3, Section II

10E Groups, Rings and Modules

(a) Let R be a unique factorisation domain (UFD) with field of fractions F. What does it mean to say that a polynomial $f \in R[X]$ is *primitive*? Assuming that the product of two primitive polynomials is primitive, prove that for $f \in R[X]$ primitive the following implications hold.

(i) f irreducible in $R[X] \implies f$ irreducible in $F[X]$.

(ii) f prime in $F[X] \implies f$ prime in $R[X]$.

Deduce that $R[X]$ is a UFD. [You may use any standard characterisation of a UFD, provided you state it clearly.]

(b) A rational function $f \in \mathbb{C}(X, Y)$ is *symmetric* if $f(X, Y) = f(Y, X)$. Show that if $f \in \mathbb{C}(X, Y)$ is symmetric then it can be written as $f = g/h$ where $g, h \in \mathbb{C}[X, Y]$ are coprime and symmetric.

Paper 4, Section II

9E Groups, Rings and Modules

State and prove Eisenstein's criterion. Show that if p is a prime number then $f(X) = X^{p-1} + X^{p-2} + \ldots + X^2 + X + 1$ is irreducible in $\mathbb{Z}[X]$. Let $\zeta \in \mathbb{C}$ be a root of f. Prove that $\mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/(f)$. [Any form of Gauss' lemma may be quoted without proof.]

Now let $p = 3$. Show that $\mathbb{Z}[\zeta]$ is a Euclidean domain. Prove that if n is even then there is exactly one conjugacy class of matrices $A \in \mathrm{GL}_n(\mathbb{Z})$ such that $A^2 + A + I = 0$. What happens if n is odd? You should carefully state any theorems that you use.

Paper 2, Section I
1E Groups, Rings and Modules

(a) Let R be an integral domain and M an R-module. Let $T \subset M$ be the subset of torsion elements, i.e., elements $m \in M$ such that $rm = 0$ for some $0 \neq r \in R$. Show that T is an R-submodule of M.

(b) Let $\phi : M_1 \to M_2$ be a homomorphism of R-modules. Let $T_1 \leqslant M_1$ and $T_2 \leqslant M_2$ be the torsion submodules. Show that there is a homomorphism of R-modules $\Phi : M_1/T_1 \to M_2/T_2$ satisfying $\Phi(m + T_1) = \phi(m) + T_2$ for all $m \in M_1$.

Does ϕ injective imply Φ injective?

Does Φ injective imply ϕ injective?

Paper 3, Section I
1E Groups, Rings and Modules

State the first isomorphism theorem for rings.

Let R be a subring of a ring S, and let J be an ideal in S. Show that $R + J$ is a subring of S and that

$$\frac{R}{R \cap J} \cong \frac{R + J}{J}.$$

Compute the characteristics of the following rings, and determine which are fields.

$$\frac{\mathbb{Q}[X]}{(X+2)} \qquad\qquad \frac{\mathbb{Z}[X]}{(3, X^2 + X + 1)}$$

Paper 1, Section II
9E Groups, Rings and Modules

Define a *Euclidean domain.* Briefly explain how $\mathbb{Z}[i]$ satisfies this definition.

Find all the units in $\mathbb{Z}[i]$. Working in this ring, write each of the elements 2, 5 and $1 + 3i$ in the form $u\, p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ where u is a unit, and $p_1, \ldots, p_t$ are pairwise non-associate irreducibles.

Find all pairs of integers x and y satisfying $x^2 + 4 = y^3$.

Paper 2, Section II
9E Groups, Rings and Modules

Define a Sylow subgroup and state the Sylow theorems. Prove the third theorem, concerning the number of Sylow subgroups.

Quoting any general facts you need about alternating groups, show that A_n has no subgroup of index m if $1 < m < n$ and $n \geqslant 5$. Hence, or otherwise, show that there is no simple group of order 90.

Paper 3, Section II
10E Groups, Rings and Modules

Let R be a Euclidean domain. What does it mean for two matrices with entries in R to be *equivalent*? Prove that any such matrix is equivalent to a diagonal matrix. Under what further conditions is the diagonal matrix said to be in *Smith normal form*?

Let $M \leqslant \mathbb{Z}^n$ be the subgroup generated by the rows of an $n \times n$ matrix A. Show that $G = \mathbb{Z}^n/M$ is finite if and only if $\det A \neq 0$, and in that case the order of G is $|\det A|$.

Determine whether the groups G_1 and G_2 corresponding to the following matrices are isomorphic.

$$A_1 = \begin{pmatrix} 5 & 0 & 4 \\ 0 & 1 & 2 \\ 2 & 0 & 0 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 7 & 2 & -1 \\ 6 & 2 & 0 \\ 1 & 0 & 3 \end{pmatrix}$$

Paper 4, Section II
9E Groups, Rings and Modules

(a) Let R be a unique factorisation domain with field of fractions F. What does it mean for a polynomial $f \in R[X]$ to be *primitive*? Prove that the product of two primitive polynomials is primitive. Let $f, g \in R[X]$ be polynomials of positive degree. Show that if f and g are coprime in $R[X]$ then they are coprime in $F[X]$.

(b) Let $I \subset \mathbb{C}[X, Y]$ be an ideal generated by non-zero coprime polynomials f and g. By running Euclid's algorithm in a suitable ring, or otherwise, show that $I \cap \mathbb{C}[X] \neq \{0\}$ and $I \cap \mathbb{C}[Y] \neq \{0\}$. Deduce that $\mathbb{C}[X, Y]/I$ is a finite dimensional $\mathbb{C}$-vector space.

Paper 2, Section I

1G Groups, Rings and Modules

Let M be a module over a Principal Ideal Domain R and let N be a submodule of M. Show that M is finitely generated if and only if N and M/N are finitely generated.

Paper 3, Section I

1G Groups, Rings and Modules

Let G be a finite group, and let H be a proper subgroup of G of index n.

Show that there is a normal subgroup K of G such that $|G/K|$ divides $n!$ and $|G/K| \geqslant n$.

Show that if G is non-abelian and simple, then G is isomorphic to a subgroup of A_n.

Paper 1, Section II

9G Groups, Rings and Modules

Show that a ring R is Noetherian if and only if every ideal of R is finitely generated. Show that if $\phi\colon R \to S$ is a surjective ring homomorphism and R is Noetherian, then S is Noetherian.

State and prove Hilbert's Basis Theorem.

Let $\alpha \in \mathbb{C}$. Is $\mathbb{Z}[\alpha]$ Noetherian? Justify your answer.

Give, with proof, an example of a Unique Factorization Domain that is not Noetherian.

Let R be the ring of continuous functions $\mathbb{R} \to \mathbb{R}$. Is R Noetherian? Justify your answer.

Paper 2, Section II

9G Groups, Rings and Modules

Let M be a module over a ring R and let $S \subset M$. Define what it means that S *freely generates* M. Show that this happens if and only if for every R-module N, every function $f\colon S \to N$ extends uniquely to a homomorphism $\phi\colon M \to N$.

Let M be a free module over a (non-trivial) ring R that is generated (not necessarily freely) by a subset $T \subset M$ of size m. Show that if S is a basis of M, then S is finite with $|S| \leqslant m$. Hence, or otherwise, deduce that any two bases of M have the same number of elements. Denoting this number $\mathrm{rk}M$ and by quoting any result you need, show that if R is a Euclidean Domain and N is a submodule of M, then N is free with $\mathrm{rk}N \leqslant \mathrm{rk}M$.

State the Primary Decomposition Theorem for a finitely generated module M over a Euclidean Domain R. Deduce that any finite subgroup of the multiplicative group of a field is cyclic.

Paper 3, Section II

10G Groups, Rings and Modules

Let p be a non-zero element of a Principal Ideal Domain R. Show that the following are equivalent:

(i) p is prime;

(ii) p is irreducible;

(iii) (p) is a maximal ideal of R;

(iv) $R/(p)$ is a field;

(v) $R/(p)$ is an Integral Domain.

Let R be a Principal Ideal Domain, S an Integral Domain and $\phi\colon R \to S$ a surjective ring homomorphism. Show that either ϕ is an isomorphism or S is a field.

Show that if R is a commutative ring and $R[X]$ is a Principal Ideal Domain, then R is a field.

Let R be an Integral Domain in which every two non-zero elements have a highest common factor. Show that in R every irreducible element is prime.

Paper 4, Section II

9G Groups, Rings and Modules

Let H and P be subgroups of a finite group G. Show that the sets HxP, $x \in G$, partition G. By considering the action of H on the set of left cosets of P in G by left multiplication, or otherwise, show that

$$\frac{|HxP|}{|P|} = \frac{|H|}{|H \cap xPx^{-1}|}$$

for any $x \in G$. Deduce that if G has a Sylow p-subgroup, then so does H.

Let $p, n \in \mathbb{N}$ with p a prime. Write down the order of the group $GL_n(\mathbb{Z}/p\mathbb{Z})$. Identify in $GL_n(\mathbb{Z}/p\mathbb{Z})$ a Sylow p-subgroup and a subgroup isomorphic to the symmetric group S_n. Deduce that every finite group has a Sylow p-subgroup.

State Sylow's theorem on the number of Sylow p-subgroups of a finite group.

Let G be a group of order pq, where $p > q$ are prime numbers. Show that if G is non-abelian, then $q \mid p-1$.

Paper 2, Section I

1G Groups Rings and Modules

Assume a group G acts transitively on a set Ω and that the size of Ω is a prime number. Let H be a normal subgroup of G that acts non-trivially on Ω.

Show that any two H-orbits of Ω have the same size. Deduce that the action of H on Ω is transitive.

Let $\alpha \in \Omega$ and let G_α denote the stabiliser of α in G. Show that if $H \cap G_\alpha$ is trivial, then there is a bijection $\theta\colon H \to \Omega$ under which the action of G_α on H by conjugation corresponds to the action of G_α on Ω.

Paper 1, Section II

9G Groups Rings and Modules

State the structure theorem for a finitely generated module M over a Euclidean domain R in terms of invariant factors.

Let V be a finite-dimensional vector space over a field F and let $\alpha\colon V \to V$ be a linear map. Let V_α denote the $F[X]$-module V with X acting as α. Apply the structure theorem to V_α to show the existence of a basis of V with respect to which α has the rational canonical form. Prove that the minimal polynomial and the characteristic polynomial of α can be expressed in terms of the invariant factors. [*Hint: For the characteristic polynomial apply suitable row operations.*] Deduce the Cayley–Hamilton theorem for α.

Now assume that α has matrix (a_{ij}) with respect to the basis $v_1, \ldots, v_n$ of V. Let M be the free $F[X]$-module of rank n with free basis $m_1, \ldots, m_n$ and let $\theta\colon M \to V_\alpha$ be the unique homomorphism with $\theta(m_i) = v_i$ for $1 \leqslant i \leqslant n$. Using the fact, which you need not prove, that $\ker\theta$ is generated by the elements $Xm_i - \sum_{j=1}^n a_{ji}\, m_j$, $1 \leqslant i \leqslant n$, find the invariant factors of V_α in the case that $V = \mathbb{R}^3$ and α is represented by the real matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}$$

with respect to the standard basis.

Paper 2, Section II

9G Groups Rings and Modules

State Gauss' lemma. State and prove Eisenstein's criterion.

Define the notion of an *algebraic integer*. Show that if α is an algebraic integer, then $\{f \in \mathbb{Z}[X] : f(\alpha) = 0\}$ is a principal ideal generated by a monic, irreducible polynomial.

Let $f = X^4 + 2X^3 - 3X^2 - 4X - 11$. Show that $\mathbb{Q}[X]/(f)$ is a field. Show that $\mathbb{Z}[X]/(f)$ is an integral domain, but not a field. Justify your answers.

Paper 3, Section I

1G Groups, Rings and Modules

Prove that the ideal $(2, 1+\sqrt{-13})$ in $\mathbb{Z}[\sqrt{-13}]$ is not principal.

Paper 4, Section I

2G Groups, Rings and Modules

Let G be a group and P a subgroup.

(a) Define the *normaliser* $N_G(P)$.

(b) Suppose that $K \lhd G$ and P is a Sylow p-subgroup of K. Using Sylow's second theorem, prove that $G = N_G(P)K$.

Paper 2, Section I

2G Groups, Rings and Modules

Let R be an integral domain. A module M over R is *torsion-free* if, for any $r \in R$ and $m \in M$, $rm = 0$ only if $r = 0$ or $m = 0$.

Let M be a module over R. Prove that there is a quotient

$$q : M \to M_0$$

with M_0 torsion-free and with the following property: whenever N is a torsion-free module and $f : M \to N$ is a homomorphism of modules, there is a homomorphism $f_0 : M_0 \to N$ such that $f = f_0 \circ q$.

Paper 1, Section II

10G Groups, Rings and Modules

(a) Let G be a group of order p^4, for p a prime. Prove that G is not simple.

(b) State Sylow's theorems.

(c) Let G be a group of order p^2q^2, where p, q are distinct odd primes. Prove that G is not simple.

Paper 4, Section II

11G Groups, Rings and Modules

(a) Define the Smith Normal Form of a matrix. When is it guaranteed to exist?

(b) Deduce the classification of finitely generated abelian groups.

(c) How many conjugacy classes of matrices are there in $GL_{10}(\mathbb{Q})$ with minimal polynomial $X^7 - 4X^3$?

Paper 3, Section II

11G Groups, Rings and Modules

Let $\omega = \frac{1}{2}(-1 + \sqrt{-3})$.

(a) Prove that $\mathbb{Z}[\omega]$ is a Euclidean domain.

(b) Deduce that $\mathbb{Z}[\omega]$ is a unique factorisation domain, stating carefully any results from the course that you use.

(c) By working in $\mathbb{Z}[\omega]$, show that whenever $x, y \in \mathbb{Z}$ satisfy

$$x^2 - x + 1 = y^3$$

then x is not congruent to 2 modulo 3.

Paper 2, Section II

11G Groups, Rings and Modules

(a) Let k be a field and let $f(X)$ be an irreducible polynomial of degree $d > 0$ over k. Prove that there exists a field F containing k as a subfield such that

$$f(X) = (X - \alpha)g(X)\,,$$

where $\alpha \in F$ and $g(X) \in F[X]$. State carefully any results that you use.

(b) Let k be a field and let $f(X)$ be a monic polynomial of degree $d > 0$ over k, which is not necessarily irreducible. Prove that there exists a field F containing k as a subfield such that

$$f(X) = \prod_{i=1}^{d}(X - \alpha_i)\,,$$

where $\alpha_i \in F$.

(c) Let $k = \mathbb{Z}/(p)$ for p a prime, and let $f(X) = X^{p^n} - X$ for $n \geqslant 1$ an integer. For F as in part (b), let K be the set of roots of $f(X)$ in F. Prove that K is a field.

Paper 3, Section I

1G Groups, Rings and Modules

(a) Find all integer solutions to $x^2 + 5y^2 = 9$.

(b) Find all the irreducibles in $\mathbb{Z}[\sqrt{-5}]$ of norm 9.

Paper 4, Section I

2G Groups, Rings and Modules

(a) Show that every automorphism α of the dihedral group D_6 is equal to conjugation by an element of D_6; that is, there is an $h \in D_6$ such that

$$\alpha(g) = hgh^{-1}$$

for all $g \in D_6$.

(b) Give an example of a non-abelian group G with an automorphism which is not equal to conjugation by an element of G.

Paper 2, Section I

2G Groups, Rings and Modules

Let R be a principal ideal domain and x a non-zero element of R. We define a new ring R' as follows. We define an equivalence relation $\sim$ on $R \times \{x^n \mid n \in \mathbb{Z}_{\geqslant 0}\}$ by

$$(r, x^n) \sim (r', x^{n'})$$

if and only if $x^{n'}r = x^n r'$. The underlying set of R' is the set of $\sim$-equivalence classes. We define addition on R' by

$$[(r, x^n)] + [(r', x^{n'})] = [(x^{n'}r + x^n r', x^{n+n'})]$$

and multiplication by $[(r, x^n)][(r', x^{n'})] = [(rr', x^{n+n'})]$.

(a) Show that R' is a well defined ring.

(b) Prove that R' is a principal ideal domain.

Paper 1, Section II
10G Groups, Rings and Modules

(a) State Sylow's theorems.

(b) Prove Sylow's first theorem.

(c) Let G be a group of order 12. Prove that either G has a unique Sylow 3-subgroup or $G \cong A_4$.

Paper 4, Section II
11G Groups, Rings and Modules

(a) State the classification theorem for finitely generated modules over a Euclidean domain.

(b) Deduce the existence of the rational canonical form for an $n \times n$ matrix A over a field F.

(c) Compute the rational canonical form of the matrix

$$A = \begin{pmatrix} 3/2 & 1 & 0 \\ -1 & -1/2 & 0 \\ 2 & 2 & 1/2 \end{pmatrix}$$

Paper 3, Section II
11G Groups, Rings and Modules

(a) State Gauss's Lemma.

(b) State and prove Eisenstein's criterion for the irreducibility of a polynomial.

(c) Determine whether or not the polynomial

$$f(X) = 2X^3 + 19X^2 - 54X + 3$$

is irreducible over $\mathbb{Q}$.

Paper 2, Section II

11G Groups, Rings and Modules

(a) Prove that every principal ideal domain is a unique factorization domain.

(b) Consider the ring $R = \{f(X) \in \mathbb{Q}[X] \mid f(0) \in \mathbb{Z}\}$.

(i) What are the units in R?

(ii) Let $f(X) \in R$ be irreducible. Prove that either $f(X) = \pm p$, for $p \in \mathbb{Z}$ a prime, or $\deg(f) \geqslant 1$ and $f(0) = \pm 1$.

(iii) Prove that $f(X) = X$ is not expressible as a product of irreducibles.

Paper 3, Section I

1E Groups, Rings and Modules

Let R be a commutative ring and let M be an R-module. Show that M is a finitely generated R-module if and only if there exists a surjective R-module homomorphism $R^n \to M$ for some n.

Find an example of a $\mathbb{Z}$-module M such that there is no surjective $\mathbb{Z}$-module homomorphism $\mathbb{Z} \to M$ but there is a surjective $\mathbb{Z}$-module homomorphism $\mathbb{Z}^2 \to M$ which is not an isomorphism. Justify your answer.

Paper 2, Section I

2E Groups, Rings and Modules

(a) Define what is meant by a *unique factorisation domain* and by a *principal ideal domain.* State Gauss's lemma and Eisenstein's criterion, without proof.

(b) Find an example, with justification, of a ring R and a subring S such that

(i) R is a principal ideal domain, and

(ii) S is a unique factorisation domain but not a principal ideal domain.

Paper 4, Section I

2E Groups, Rings and Modules

Let G be a non-trivial finite p-group and let $Z(G)$ be its centre. Show that $|Z(G)| > 1$. Show that if $|G| = p^3$ and if G is not abelian, then $|Z(G)| = p$.

Paper 1, Section II

10E Groups, Rings and Modules

(a) State Sylow's theorem.

(b) Let G be a finite simple non-abelian group. Let p be a prime number. Show that if p divides $|G|$, then $|G|$ divides $n_p!/2$ where n_p is the number of Sylow p-subgroups of G.

(c) Let G be a group of order 48. Show that G is not simple. Find an example of G which has no normal Sylow 2-subgroup.

Paper 2, Section II
11E Groups, Rings and Modules

Let R be a commutative ring.

(a) Let N be the set of nilpotent elements of R, that is,

$$N = \{r \in R \mid r^n = 0 \text{ for some } n \in \mathbb{N}\}.$$

Show that N is an ideal of R.

(b) Assume R is Noetherian and assume $S \subset R$ is a non-empty subset such that if $s, t \in S$, then $st \in S$. Let I be an ideal of R disjoint from S. Show that there is a prime ideal P of R containing I and disjoint from S.

(c) Again assume R is Noetherian and let N be as in part (a). Let $\mathcal{P}$ be the set of all prime ideals of R. Show that

$$N = \bigcap_{P \in \mathcal{P}} P.$$

Paper 4, Section II
11E Groups, Rings and Modules

(a) State (without proof) the classification theorem for finitely generated modules over a Euclidean domain. Give the statement and the proof of the rational canonical form theorem.

(b) Let R be a principal ideal domain and let M be an R-submodule of R^n. Show that M is a free R-module.

Paper 3, Section II
11E Groups, Rings and Modules

(a) Define what is meant by a *Euclidean domain*. Show that every Euclidean domain is a principal ideal domain.

(b) Let $p \in \mathbb{Z}$ be a prime number and let $f \in \mathbb{Z}[x]$ be a monic polynomial of positive degree. Show that the quotient ring $\mathbb{Z}[x]/(p, f)$ is finite.

(c) Let $\alpha \in \mathbb{Z}[\sqrt{-1}]$ and let P be a non-zero prime ideal of $\mathbb{Z}[\alpha]$. Show that the quotient $\mathbb{Z}[\alpha]/P$ is a finite ring.

Paper 3, Section I

1E Groups, Rings and Modules

Let G be a group of order n. Define what is meant by a *permutation representation* of G. Using such representations, show G is isomorphic to a subgroup of the symmetric group S_n. Assuming G is non-abelian simple, show G is isomorphic to a subgroup of A_n. Give an example of a permutation representation of S_3 whose kernel is A_3.

Paper 4, Section I

2E Groups, Rings and Modules

Give the statement and the proof of Eisenstein's criterion. Use this criterion to show $x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible in $\mathbb{Q}[x]$ where p is a prime.

Paper 2, Section I

2E Groups, Rings and Modules

Let R be an integral domain.

Define what is meant by the *field of fractions* F of R. [You do not need to prove the existence of F.]

Suppose that $\phi : R \to K$ is an injective ring homomorphism from R to a field K. Show that ϕ extends to an injective ring homomorphism $\Phi : F \to K$.

Give an example of R and a ring homomorphism $\psi : R \to S$ from R to a ring S such that ψ does not extend to a ring homomorphism $F \to S$.

Paper 1, Section II

10E Groups, Rings and Modules

(a) Let I be an ideal of a commutative ring R and assume $I \subseteq \bigcup_{i=1}^{n} P_i$ where the P_i are prime ideals. Show that $I \subseteq P_i$ for some i.

(b) Show that (x^2+1) is a maximal ideal of $\mathbb{R}[x]$. Show that the quotient ring $\mathbb{R}[x]/(x^2+1)$ is isomorphic to $\mathbb{C}$.

(c) For $a, b \in \mathbb{R}$, let $I_{a,b}$ be the ideal $(x-a, y-b)$ in $\mathbb{R}[x,y]$. Show that $I_{a,b}$ is a maximal ideal. Find a maximal ideal J of $\mathbb{R}[x,y]$ such that $J \neq I_{a,b}$ for any $a, b \in \mathbb{R}$. Justify your answers.

Paper 3, Section II

11E Groups, Rings and Modules

(a) Define what is meant by an *algebraic integer* α. Show that the ideal

$$I = \{h \in \mathbb{Z}[x] \mid h(\alpha) = 0\}$$

in $\mathbb{Z}[x]$ is generated by a monic irreducible polynomial f. Show that $\mathbb{Z}[\alpha]$, considered as a $\mathbb{Z}$-module, is freely generated by n elements where $n = \deg f$.

(b) Assume $\alpha \in \mathbb{C}$ satisfies $\alpha^5 + 2\alpha + 2 = 0$. Is it true that the ideal (5) in $\mathbb{Z}[\alpha]$ is a prime ideal? Is there a ring homomorphism $\mathbb{Z}[\alpha] \to \mathbb{Z}[\sqrt{-1}]$? Justify your answers.

(c) Show that the only unit elements of $\mathbb{Z}[\sqrt{-5}]$ are 1 and -1. Show that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Paper 4, Section II

11E Groups, Rings and Modules

Let R be a Noetherian ring and let M be a finitely generated R-module.

(a) Show that every submodule of M is finitely generated.

(b) Show that each maximal element of the set

$$\mathcal{A} = \{\mathrm{Ann}(m) \mid 0 \neq m \in M\}$$

is a prime ideal. [Here, maximal means maximal with respect to inclusion, and $\mathrm{Ann}(m) = \{r \in R \mid rm = 0\}$.]

(c) Show that there is a chain of submodules

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_l = M,$$

such that for each $0 < i \leqslant l$ the quotient M_i/M_{i-1} is isomorphic to R/P_i for some prime ideal P_i.

Paper 2, Section II

11E Groups, Rings and Modules

(a) State Sylow's theorems and give the proof of the second theorem which concerns conjugate subgroups.

(b) Show that there is no simple group of order 351.

(c) Let k be the finite field $\mathbb{Z}/(31)$ and let $GL_2(k)$ be the multiplicative group of invertible 2×2 matrices over k. Show that every Sylow 3-subgroup of $GL_2(k)$ is abelian.

Paper 3, Section I

1F Groups, Rings and Modules

State two equivalent conditions for a commutative ring to be *Noetherian*, and prove they are equivalent. Give an example of a ring which is not Noetherian, and explain why it is not Noetherian.

Paper 4, Section I

2F Groups, Rings and Modules

Let R be a commutative ring. Define what it means for an ideal $I \subseteq R$ to be *prime*. Show that $I \subseteq R$ is prime if and only if R/I is an integral domain.

Give an example of an integral domain R and an ideal $I \subset R$, $I \neq R$, such that R/I is not an integral domain.

Paper 2, Section I

2F Groups, Rings and Modules

Give four non-isomorphic groups of order 12, and explain why they are not isomorphic.

Paper 1, Section II

10F Groups, Rings and Modules

(i) Give the definition of a *p-Sylow subgroup* of a group.

(ii) Let G be a group of order $2835 = 3^4 \cdot 5 \cdot 7$. Show that there are at most two possibilities for the number of 3-Sylow subgroups, and give the possible numbers of 3-Sylow subgroups.

(iii) Continuing with a group G of order 2835, show that G is not simple.

Paper 4, Section II

11F Groups, Rings and Modules

Find $a \in \mathbb{Z}_7$ such that $\mathbb{Z}_7[x]/(x^3 + a)$ is a field F. Show that for your choice of a, every element of $\mathbb{Z}_7$ has a cube root in the field F.

Show that if F is a finite field, then the multiplicative group $F^\times = F \setminus \{0\}$ is cyclic.

Show that $F = \mathbb{Z}_2[x]/(x^3+x+1)$ is a field. How many elements does F have? Find a generator for $F^\times$.

Paper 3, Section II

11F Groups, Rings and Modules

Can a group of order 55 have 20 elements of order 11? If so, give an example. If not, give a proof, including the proof of any statements you need.

Let G be a group of order pq, with p and q primes, $p > q$. Suppose furthermore that q does not divide $p-1$. Show that G is cyclic.

Paper 2, Section II

11F Groups, Rings and Modules

(a) Consider the homomorphism $f : \mathbb{Z}^3 \to \mathbb{Z}^4$ given by

$$f(a,b,c) = (a + 2b + 8c, 2a - 2b + 4c, -2b + 12c, 2a - 4b + 4c).$$

Describe the image of this homomorphism as an abstract abelian group. Describe the quotient of $\mathbb{Z}^4$ by the image of this homomorphism as an abstract abelian group.

(b) Give the definition of a *Euclidean domain.*

Fix a prime p and consider the subring R of the rational numbers $\mathbb{Q}$ defined by

$$R = \{q/r \mid \gcd(p,r) = 1\},$$

where 'gcd' stands for the greatest common divisor. Show that R is a Euclidean domain.

Paper 3, Section I

1E Groups, Rings and Modules

State and prove Hilbert's Basis Theorem.

Paper 4, Section I

2E Groups, Rings and Modules

Let G be the abelian group generated by elements a, b and c subject to the relations: $3a + 6b + 3c = 0$, $9b + 9c = 0$ and $-3a + 3b + 6c = 0$. Express G as a product of cyclic groups. Hence determine the number of elements of G of order 3.

Paper 2, Section I

2E Groups, Rings and Modules

List the conjugacy classes of A_6 and determine their sizes. Hence prove that A_6 is simple.

Paper 1, Section II

10E Groups, Rings and Modules

Let G be a finite group and p a prime divisor of the order of G. Give the definition of a Sylow p-subgroup of G, and state Sylow's theorems.

Let p and q be distinct primes. Prove that a group of order p^2q is not simple.

Let G be a finite group, H a normal subgroup of G and P a Sylow p-subgroup of H. Let $N_G(P)$ denote the normaliser of P in G. Prove that if $g \in G$ then there exist $k \in N_G(P)$ and $h \in H$ such that $g = kh$.

Paper 4, Section II

11E Groups, Rings and Modules

(a) Consider the four following types of rings: Principal Ideal Domains, Integral Domains, Fields, and Unique Factorisation Domains. Arrange them in the form $A \implies B \implies C \implies D$ (where $A \implies B$ means if a ring is of type A then it is of type B).

Prove that these implications hold. [You may assume that irreducibles in a Principal Ideal Domain are prime.] Provide examples, with brief justification, to show that these implications cannot be reversed.

(b) Let R be a ring with ideals I and J satisfying $I \subseteq J$. Define K to be the set $\{r \in R : rJ \subseteq I\}$. Prove that K is an ideal of R. If J and K are principal, prove that I is principal.

Paper 3, Section II

11E Groups, Rings and Modules

Let R be a ring, M an R-module and $S = \{m_1, \ldots, m_k\}$ a subset of M. Define what it means to say S *spans* M. Define what it means to say S is an *independent* set.

We say S is a *basis* for M if S spans M and S is an independent set. Prove that the following two statements are equivalent.

1. S is a basis for M.
2. Every element of M is uniquely expressible in the form $r_1 m_1 + \cdots + r_k m_k$ for some $r_1, \ldots, r_k \in R$.

We say S *generates* M *freely* if S spans M and any map $\Phi : S \to N$, where N is an R-module, can be extended to an R-module homomorphism $\Theta : M \to N$. Prove that S generates M freely if and only if S is a basis for M.

Let M be an R-module. Are the following statements true or false? Give reasons.

(i) If S spans M then S necessarily contains an independent spanning set for M.

(ii) If S is an independent subset of M then S can always be extended to a basis for M.

Paper 2, Section II

11E Groups, Rings and Modules

Prove that every finite integral domain is a field.

Let F be a field and f an irreducible polynomial in the polynomial ring $F[X]$. Prove that $F[X]/(f)$ is a field, where (f) denotes the ideal generated by f.

Hence construct a field of 4 elements, and write down its multiplication table.

Construct a field of order 9.

Paper 3, Section I

1G Groups, Rings and Modules

Define the notion of a free module over a ring. When R is a PID, show that every ideal of R is free as an R-module.

Paper 4, Section I

2G Groups, Rings and Modules

Let p be a prime number, and G be a non-trivial finite group whose order is a power of p. Show that the size of every conjugacy class in G is a power of p. Deduce that the centre Z of G has order at least p.

Paper 2, Section I

2G Groups, Rings and Modules

Show that every Euclidean domain is a PID. Define the notion of a Noetherian ring, and show that $\mathbb{Z}[i]$ is Noetherian by using the fact that it is a Euclidean domain.

Paper 1, Section II

10G Groups, Rings and Modules

(i) Consider the group $G = GL_2(\mathbb{R})$ of all 2 by 2 matrices with entries in $\mathbb{R}$ and non-zero determinant. Let T be its subgroup consisting of all diagonal matrices, and N be the normaliser of T in G. Show that N is generated by T and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and determine the quotient group N/T.

(ii) Now let p be a prime number, and F be the field of integers modulo p. Consider the group $G = GL_2(F)$ as above but with entries in F, and define T and N similarly. Find the order of the group N.

Paper 4, Section II
11G Groups, Rings and Modules

Let R be an integral domain, and M be a finitely generated R-module.

(i) Let S be a finite subset of M which generates M as an R-module. Let T be a maximal linearly independent subset of S, and let N be the R-submodule of M generated by T. Show that there exists a non-zero $r \in R$ such that $rx \in N$ for every $x \in M$.

(ii) Now assume M is *torsion-free*, i.e. $rx = 0$ for $r \in R$ and $x \in M$ implies $r = 0$ or $x = 0$. By considering the map $M \to N$ mapping x to rx for r as in (i), show that every torsion-free finitely generated R-module is isomorphic to an R-submodule of a finitely generated free R-module.

Paper 3, Section II
11G Groups, Rings and Modules

Let $R = \mathbb{C}[X, Y]$ be the polynomial ring in two variables over the complex numbers, and consider the principal ideal $I = (X^3 - Y^2)$ of R.

(i) Using the fact that R is a UFD, show that I is a prime ideal of R. [*Hint: Elements in* $\mathbb{C}[X, Y]$ *are polynomials in* Y *with coefficients in* $\mathbb{C}[X]$.]

(ii) Show that I is not a maximal ideal of R, and that it is contained in infinitely many distinct proper ideals in R.

Paper 2, Section II
11G Groups, Rings and Modules

(i) State the structure theorem for finitely generated modules over Euclidean domains.

(ii) Let $\mathbb{C}[X]$ be the polynomial ring over the complex numbers. Let M be a $\mathbb{C}[X]$-module which is 4-dimensional as a $\mathbb{C}$-vector space and such that $(X - 2)^4 \cdot x = 0$ for all $x \in M$. Find all possible forms we obtain when we write $M \cong \bigoplus_{i=1}^{m} \mathbb{C}[X]/(P_i^{n_i})$ for irreducible $P_i \in \mathbb{C}[X]$ and $n_i \geqslant 1$.

(iii) Consider the quotient ring $M = \mathbb{C}[X]/(X^3 + X)$ as a $\mathbb{C}[X]$-module. Show that M is isomorphic as a $\mathbb{C}[X]$-module to the direct sum of three copies of $\mathbb{C}$. Give the isomorphism and its inverse explicitly.

Paper 3, Section I
1G Groups, Rings and Modules

What is a *Euclidean domain*?

Giving careful statements of any general results you use, show that in the ring $\mathbb{Z}[\sqrt{-3}]$, 2 is irreducible but not prime.

Paper 2, Section I
2G Groups, Rings and Modules

What does it mean to say that the finite group G *acts* on the set Ω?

By considering an action of the symmetry group of a regular tetrahedron on a set of pairs of edges, show there is a surjective homomorphism $S_4 \to S_3$.

[You may assume that the symmetric group S_n is generated by transpositions.]

Paper 4, Section I
2G Groups, Rings and Modules

An *idempotent* element of a ring R is an element e satisfying $e^2 = e$. A *nilpotent* element is an element e satisfying $e^N = 0$ for some $N \geqslant 0$.

Let $r \in R$ be non-zero. In the ring $R[X]$, can the polynomial $1 + rX$ be (i) an idempotent, (ii) a nilpotent? Can $1 + rX$ satisfy the equation $(1 + rX)^3 = (1 + rX)$? Justify your answers.

Paper 1, Section II
10G Groups, Rings and Modules

Let G be a finite group. What is a *Sylow p-subgroup* of G ?

Assuming that a Sylow p-subgroup H exists, and that the number of conjugates of H is congruent to 1 mod p, prove that all Sylow p-subgroups are conjugate. If n_p denotes the number of Sylow p-subgroups, deduce that

$$n_p \equiv 1 \mod p \qquad \text{and} \qquad n_p \mid |G| .$$

If furthermore G is simple prove that either $G = H$ or

$$|G| \mid n_p!$$

Deduce that a group of order $1,000,000$ cannot be simple.

Paper 2, Section II

11G Groups, Rings and Modules

State Gauss's Lemma. State Eisenstein's irreducibility criterion.

(i) By considering a suitable substitution, show that the polynomial $1 + X^3 + X^6$ is irreducible over $\mathbb{Q}$.

(ii) By working in $\mathbb{Z}_2[X]$, show that the polynomial $1 - X^2 + X^5$ is irreducible over $\mathbb{Q}$.

Paper 3, Section II

11G Groups, Rings and Modules

For each of the following assertions, provide either a proof or a counterexample as appropriate:

(i) The ring $\mathbb{Z}_2[X]/\langle X^2 + X + 1\rangle$ is a field.

(ii) The ring $\mathbb{Z}_3[X]/\langle X^2 + X + 1\rangle$ is a field.

(iii) If F is a finite field, the ring $F[X]$ contains irreducible polynomials of arbitrarily large degree.

(iv) If R is the ring $C[0,1]$ of continuous real-valued functions on the interval $[0,1]$, and the non-zero elements $f, g \in R$ satisfy $f \mid g$ and $g \mid f$, then there is some unit $u \in R$ with $f = u \cdot g$.

Paper 4, Section II

11G Groups, Rings and Modules

Let R be a commutative ring with unit 1. Prove that an R-module is finitely generated if and only if it is a quotient of a free module R^n, for some $n > 0$.

Let M be a finitely generated R-module. Suppose now I is an ideal of R, and ϕ is an R-homomorphism from M to M with the property that

$$\phi(M) \subset I \cdot M \ = \{m \in M \,|\, m = rm' \quad \text{with} \quad r \in I\,,\ m' \in M\}\,.$$

Prove that ϕ satisfies an equation

$$\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_1\phi + a_0 = 0$$

where each $a_j \in I$. [You may assume that if T is a matrix over R, then $\operatorname{adj}(T)\,T = \det T\,(\mathrm{id})$, with id the identity matrix.]

Deduce that if M satisfies $I \cdot M = M$, then there is some $a \in R$ satisfying

$$a - 1 \in I \quad \text{and} \quad aM = 0\,.$$

Give an example of a finitely generated $\mathbb{Z}$-module M and a proper ideal I of $\mathbb{Z}$ satisfying the hypothesis $I \cdot M = M$, and for your example, give an explicit such element a.

Paper 2, Section I

2F Groups, Rings and Modules

Show that the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, with $ij = k = -ji$, $i^2 = j^2 = k^2 = -1$, is not isomorphic to the symmetry group D_8 of the square.

Paper 3, Section I

1F Groups, Rings and Modules

Suppose that A is an integral domain containing a field K and that A is finite-dimensional as a K-vector space. Prove that A is a field.

Paper 4, Section I

2F Groups, Rings and Modules

A ring R satisfies the descending chain condition (DCC) on ideals if, for every sequence $I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$ of ideals in R, there exists n with $I_n = I_{n+1} = I_{n+2} = \ldots$. Show that $\mathbb{Z}$ does not satisfy the DCC on ideals.

Paper 1, Section II

10F Groups, Rings and Modules

(i) Suppose that G is a finite group of order $p^n r$, where p is prime and does not divide r. Prove the first Sylow theorem, that G has at least one subgroup of order p^n, and state the remaining Sylow theorems without proof.

(ii) Suppose that p, q are distinct primes. Show that there is no simple group of order pq.

Paper 2, Section II

11F Groups, Rings and Modules

Define the notion of a Euclidean domain and show that $\mathbb{Z}[i]$ is Euclidean.

Is $4 + i$ prime in $\mathbb{Z}[i]$?

Paper 3, Section II

11F Groups, Rings and Modules

Suppose that A is a matrix over $\mathbb{Z}$. What does it mean to say that A can be brought to Smith normal form?

Show that the structure theorem for finitely generated modules over $\mathbb{Z}$ (which you should state) follows from the existence of Smith normal forms for matrices over $\mathbb{Z}$.

Bring the matrix $\begin{pmatrix} -4 & -6 \\ 2 & 2 \end{pmatrix}$ to Smith normal form.

Suppose that M is the $\mathbb{Z}$-module with generators e_1, e_2, subject to the relations

$$-4e_1 + 2e_2 = -6e_1 + 2e_2 = 0\,.$$

Describe M in terms of the structure theorem.

Paper 4, Section II

11F Groups, Rings and Modules

State and prove the Hilbert Basis Theorem.

Is every ring Noetherian? Justify your answer.

Paper 2, Section I

2H Groups Rings and Modules

Give the definition of conjugacy classes in a group G. How many conjugacy classes are there in the symmetric group S_4 on four letters? Briefly justify your answer.

Paper 3, Section I

1H Groups Rings and Modules

Let A be the ring of integers $\mathbb{Z}$ or the polynomial ring $\mathbb{C}[X]$. In each case, give an example of an ideal I of A such that the quotient ring $R = A/I$ has a non-trivial idempotent (an element $x \in R$ with $x \neq 0, 1$ and $x^2 = x$) and a non-trivial nilpotent element (an element $x \in R$ with $x \neq 0$ and $x^n = 0$ for some positive integer n). Exhibit these elements and justify your answer.

Paper 4, Section I

2H Groups Rings and Modules

Let M be a free $\mathbb{Z}$-module generated by e_1 and e_2. Let a, b be two non-zero integers, and N be the submodule of M generated by $ae_1 + be_2$. Prove that the quotient module M/N is free if and only if a, b are coprime.

Paper 1, Section II

10H Groups Rings and Modules

Prove that the kernel of a group homomorphism $f : G \to H$ is a normal subgroup of the group G.

Show that the dihedral group D_8 of order 8 has a non-normal subgroup of order 2. Conclude that, for a group G, a normal subgroup of a normal subgroup of G is not necessarily a normal subgroup of G.

Paper 2, Section II

11H Groups Rings and Modules

For ideals I, J of a ring R, their *product* IJ is defined as the ideal of R generated by the elements of the form xy where $x \in I$ and $y \in J$.

(1) Prove that, if a prime ideal P of R contains IJ, then P contains either I or J.

(2) Give an example of R, I and J such that the two ideals IJ and $I \cap J$ are different from each other.

(3) Prove that there is a natural bijection between the prime ideals of R/IJ and the prime ideals of $R/(I \cap J)$.

Paper 3, Section II

11H Groups Rings and Modules

Let R be an integral domain and $R^{\times}$ its group of units. An element of $S = R \setminus (R^{\times} \cup \{0\})$ is *irreducible* if it is not a product of two elements in S. When R is Noetherian, show that every element of S is a product of finitely many irreducible elements of S.

Paper 4, Section II

11H Groups Rings and Modules

Let $V = (\mathbb{Z}/3\mathbb{Z})^2$, a 2-dimensional vector space over the field $\mathbb{Z}/3\mathbb{Z}$, and let $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in V$.

(1) List all 1-dimensional subspaces of V in terms of e_1, e_2. (For example, there is a subspace $\langle e_1 \rangle$ generated by e_1.)

(2) Consider the action of the matrix group

$$G = GL_2(\mathbb{Z}/3\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,\, b,\, c,\, d \in \mathbb{Z}/3\mathbb{Z}\,,\ ad - bc \neq 0 \right\}$$

on the finite set X of all 1-dimensional subspaces of V. Describe the stabiliser group K of $\langle e_1 \rangle \in X$. What is the order of K? What is the order of G?

(3) Let $H \subset G$ be the subgroup of all elements of G which act trivially on X. Describe H, and prove that G/H is isomorphic to S_4, the symmetric group on four letters.

Paper 2, Section I

2F Groups, Rings and Modules

State Sylow's theorems. Use them to show that a group of order 56 must have either a normal subgroup of order 7 or a normal subgroup of order 8.

Paper 3, Section I

1F Groups, Rings and Modules

Let F be a field. Show that the polynomial ring $F[X]$ is a principal ideal domain. Give, with justification, an example of an ideal in $F[X, Y]$ which is not principal.

Paper 4, Section I

2F Groups, Rings and Modules

Let M be a module over an integral domain R. An element $m \in M$ is said to be torsion if there exists a nonzero $r \in R$ with $rm = 0$; M is said to be torsion-free if its only torsion element is 0. Show that there exists a unique submodule N of M such that (a) all elements of N are torsion and (b) the quotient module M/N is torsion-free.

Paper 1, Section II

10F Groups, Rings and Modules

Prove that a principal ideal domain is a unique factorization domain.

Give, with justification, an example of an element of $\mathbb{Z}[\sqrt{-3}]$ which does not have a unique factorization as a product of irreducibles. Show how $\mathbb{Z}[\sqrt{-3}]$ may be embedded as a subring of index 2 in a ring R (that is, such that the additive quotient group $R/\mathbb{Z}[\sqrt{-3}]$ has order 2) which is a principal ideal domain. [*You should explain why R is a principal ideal domain, but detailed proofs are not required.*]

Paper 2, Section II

11F Groups, Rings and Modules

Define the centre of a group, and prove that a group of prime-power order has a nontrivial centre. Show also that if the quotient group $G/Z(G)$ is cyclic, where $Z(G)$ is the centre of G, then it is trivial. Deduce that a non-abelian group of order p^3, where p is prime, has centre of order p.

Let F be the field of p elements, and let G be the group of 3×3 matrices over F of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} .$$

Identify the centre of G.

Paper 3, Section II

11F Groups, Rings and Modules

Let S be a multiplicatively closed subset of a ring R, and let I be an ideal of R which is maximal among ideals disjoint from S. Show that I is prime.

If R is an integral domain, explain briefly how one may construct a field F together with an injective ring homomorphism $R \to F$.

Deduce that if R is an arbitrary ring, I an ideal of R, and S a multiplicatively closed subset disjoint from I, then there exists a ring homomorphism $f : R \to F$, where F is a field, such that $f(x) = 0$ for all $x \in I$ and $f(y) \neq 0$ for all $y \in S$.

[*You may assume that if T is a multiplicatively closed subset of a ring, and $0 \notin T$, then there exists an ideal which is maximal among ideals disjoint from T.*]

Paper 4, Section II

11F Groups, Rings and Modules

Let R be a principal ideal domain. Prove that any submodule of a finitely-generated free module over R is free.

An R-module P is said to be projective if, whenever we have module homomorphisms $f : M \to N$ and $g : P \to N$ with f surjective, there exists a homomorphism $h : P \to M$ with $f \circ h = g$. Show that any free module (over an arbitrary ring) is projective. Show also that a finitely-generated projective module over a principal ideal domain is free.

1/II/10G Groups, Rings and Modules

(i) Show that A_4 is not simple.

(ii) Show that the group $\mathrm{Rot}(D)$ of rotational symmetries of a regular dodecahedron is a simple group of order 60.

(iii) Show that $\mathrm{Rot}(D)$ is isomorphic to A_5.

2/I/2G Groups, Rings and Modules

What does it means to say that a complex number α is algebraic over $\mathbb{Q}$? Define the minimal polynomial of α.

Suppose that α satisfies a nonconstant polynomial $f \in \mathbb{Z}[X]$ which is irreducible over $\mathbb{Z}$. Show that there is an isomorphism $\mathbb{Z}[X]/(f) \cong \mathbb{Z}[\alpha]$.

[*You may assume standard results about unique factorisation, including Gauss's lemma.*]

2/II/11G Groups, Rings and Modules

Let F be a field. Prove that every ideal of the ring $F[X_1, \ldots, X_n]$ is finitely generated.

Consider the set

$$R = \left\{ p(X,Y) = \sum c_{ij} X^i Y^j \in F[X,Y] \;\middle|\; c_{0j} = c_{j0} = 0 \text{ whenever } j > 0 \right\}.$$

Show that R is a subring of $F[X,Y]$ which is not Noetherian.

3/I/1G Groups, Rings and Modules

Let G be the abelian group generated by elements a, b, c, d subject to the relations

$$4a - 2b + 2c + 12d = 0, \quad -2b + 2c = 0, \quad 2b + 2c = 0, \quad 8a + 4c + 24d = 0\,.$$

Express G as a product of cyclic groups, and find the number of elements of G of order 2.

3/II/11G **Groups, Rings and Modules**

What is a Euclidean domain? Show that a Euclidean domain is a principal ideal domain.

Show that $\mathbb{Z}[\sqrt{-7}]$ is not a Euclidean domain (for any choice of norm), but that the ring

$$\mathbb{Z}\Big[\frac{1+\sqrt{-7}}{2}\Big]$$

is Euclidean for the norm function $N(z) = z\bar{z}$.

4/I/2G **Groups, Rings and Modules**

Let $n \geq 2$ be an integer. Show that the polynomial $(X^n - 1)/(X - 1)$ is irreducible over $\mathbb{Z}$ if and only if n is prime.

[*You may use Eisenstein's criterion without proof.*]

4/II/11G **Groups, Rings and Modules**

Let R be a ring and M an R-module. What does it mean to say that M is a free R-module? Show that M is free if there exists a submodule $N \subseteq M$ such that both N and M/N are free.

Let M and M' be R-modules, and $N \subseteq M$, $N' \subseteq M'$ submodules. Suppose that $N \cong N'$ and $M/N \cong M'/N'$. Determine (by proof or counterexample) which of the following statements holds:

(1) If N is free then $M \cong M'$.

(2) If M/N is free then $M \cong M'$.

1/II/10G Groups, Rings and Modules

(i) State a structure theorem for finitely generated abelian groups.

(ii) If K is a field and f a polynomial of degree n in one variable over K, what is the maximal number of zeroes of f? Justify your answer in terms of unique factorization in some polynomial ring, or otherwise.

(iii) Show that any finite subgroup of the multiplicative group of non-zero elements of a field is cyclic. Is this true if the subgroup is allowed to be infinite?

2/I/2G Groups, Rings and Modules

Define the term *Euclidean domain*.

Show that the ring of integers $\mathbb{Z}$ is a Euclidean domain.

2/II/11G Groups, Rings and Modules

(i) Give an example of a Noetherian ring and of a ring that is not Noetherian. Justify your answers.

(ii) State and prove Hilbert's basis theorem.

3/I/1G Groups, Rings and Modules

What are the orders of the groups $GL_2(\mathbb{F}_p)$ and $SL_2(\mathbb{F}_p)$ where $\mathbb{F}_p$ is the field of p elements?

3/II/11G Groups, Rings and Modules

(i) State the Sylow theorems for Sylow p-subgroups of a finite group.

(ii) Write down one Sylow 3-subgroup of the symmetric group S_5 on 5 letters. Calculate the number of Sylow 3-subgroups of S_5.

4/I/2G Groups, Rings and Modules

If p is a prime, how many abelian groups of order p^4 are there, up to isomorphism?

4/II/11G **Groups, Rings and Modules**

A regular icosahedron has 20 faces, 12 vertices and 30 edges. The group G of its rotations acts transitively on the set of faces, on the set of vertices and on the set of edges.

(i) List the conjugacy classes in G and give the size of each.

(ii) Find the order of G and list its normal subgroups.

[*A normal subgroup of* G *is a union of conjugacy classes in* G.]

1/II/10E **Groups, Rings and Modules**

Find all subgroups of indices 2, 3, 4 and 5 in the alternating group A_5 on 5 letters. You may use any general result that you choose, provided that you state it clearly, but you must justify your answers.

[*You may take for granted the fact that A_4 has no subgroup of index 2.*]

2/I/2E **Groups, Rings and Modules**

(i) Give the definition of a Euclidean domain and, with justification, an example of a Euclidean domain that is not a field.

(ii) State the structure theorem for finitely generated modules over a Euclidean domain.

(iii) In terms of your answer to (ii), describe the structure of the $\mathbb{Z}$-module M with generators $\{m_1, m_2, m_3\}$ and relations $2m_3 = 2m_2$, $4m_2 = 0$.

2/II/11E **Groups, Rings and Modules**

(i) Prove the first Sylow theorem, that a finite group of order $p^n r$ with p prime and p not dividing the integer r has a subgroup of order p^n.

(ii) State the remaining Sylow theorems.

(iii) Show that if p and q are distinct primes then no group of order pq is simple.

3/I/1E **Groups, Rings and Modules**

(i) Give an example of an integral domain that is not a unique factorization domain.

(ii) For which integers n is $\mathbb{Z}/n\mathbb{Z}$ an integral domain?

3/II/11E **Groups, Rings and Modules**

Suppose that R is a ring. Prove that $R[X]$ is Noetherian if and only if R is Noetherian.

4/I/2E **Groups, Rings and Modules**

How many elements does the ring $\mathbb{Z}[X]/(3, X^2 + X + 1)$ have?

Is this ring an integral domain?

Briefly justify your answers.

4/II/11E **Groups, Rings and Modules**

(a) Suppose that R is a commutative ring, M an R-module generated by $m_1, \ldots, m_n$ and $\phi \in End_R(M)$. Show that, if $A = (a_{ij})$ is an $n \times n$ matrix with entries in R that represents ϕ with respect to this generating set, then in the sub-ring $R[\phi]$ of $End_R(M)$ we have $\det(a_{ij} - \phi\delta_{ij}) = 0$.

[Hint: A is a matrix such that $\phi(m_i) = \sum a_{ij} m_j$ with $a_{ij} \in R$. Consider the matrix $C = (a_{ij} - \phi\delta_{ij})$ with entries in $R[\phi]$ and use the fact that for any $n \times n$ matrix N over any commutative ring, there is a matrix N' such that $N'N = (\det N)1_n$.]

(b) Suppose that k is a field, V a finite-dimensional k-vector space and that $\phi \in End_k(V)$. Show that if A is the matrix of ϕ with respect to some basis of V then ϕ satisfies the characteristic equation $\det(A - \lambda 1) = 0$ of A.

1/II/10C **Groups, Rings and Modules**

Let G be a group, and H a subgroup of finite index. By considering an appropriate action of G on the set of left cosets of H, prove that H always contains a normal subgroup K of G such that the index of K in G is finite and divides $n!$, where n is the index of H in G.

Now assume that G is a finite group of order pq, where p and q are prime numbers with $p < q$. Prove that the subgroup of G generated by any element of order q is necessarily normal.

2/I/2C **Groups, Rings and Modules**

Define an automorphism of a group G, and the natural group law on the set $\mathrm{Aut}(G)$ of all automorphisms of G. For each fixed h in G, put $\psi(h)(g) = hgh^{-1}$ for all g in G. Prove that $\psi(h)$ is an automorphism of G, and that ψ defines a homomorphism from G into $\mathrm{Aut}(G)$.

2/II/11C **Groups, Rings and Modules**

Let A be the abelian group generated by two elements x, y, subject to the relation $6x + 9y = 0$. Give a rigorous explanation of this statement by defining A as an appropriate quotient of a free abelian group of rank 2. Prove that A itself is not a free abelian group, and determine the exact structure of A.

3/I/1C **Groups, Rings and Modules**

Define what is meant by two elements of a group G being conjugate, and prove that this defines an equivalence relation on G. If G is finite, sketch the proof that the cardinality of each conjugacy class divides the order of G.

3/II/11C **Groups, Rings and Modules**

(i) Define a primitive polynomial in $\mathbb{Z}[x]$, and prove that the product of two primitive polynomials is primitive. Deduce that $\mathbb{Z}[x]$ is a unique factorization domain.

(ii) Prove that

$$\mathbb{Q}[x]/(x^5 - 4x + 2)$$

is a field. Show, on the other hand, that

$$\mathbb{Z}[x]/(x^5 - 4x + 2)$$

is an integral domain, but is not a field.

4/I/2C **Groups, Rings and Modules**

State Eisenstein's irreducibility criterion. Let n be an integer > 1. Prove that $1 + x + \ldots + x^{n-1}$ is irreducible in $\mathbb{Z}[x]$ if and only if n is a prime number.

4/II/11C **Groups, Rings and Modules**

Let R be the ring of Gaussian integers $\mathbb{Z}[i]$, where $i^2 = -1$, which you may assume to be a unique factorization domain. Prove that every prime element of R divides precisely one positive prime number in $\mathbb{Z}$. List, without proof, the prime elements of R, up to associates.

Let p be a prime number in $\mathbb{Z}$. Prove that R/pR has cardinality p^2. Prove that $R/2R$ is not a field. If $p \equiv 3 \bmod 4$, show that R/pR is a field. If $p \equiv 1 \bmod 4$, decide whether R/pR is a field or not, justifying your answer.

1/I/2F Groups, Rings and Modules

Let G be a finite group of order n. Let H be a subgroup of G. Define the normalizer $N(H)$ of H, and prove that the number of distinct conjugates of H is equal to the index of $N(H)$ in G. If p is a prime dividing n, deduce that the number of Sylow p-subgroups of G must divide n.

[*You may assume the existence and conjugacy of Sylow subgroups.*]

Prove that any group of order 72 must have either 1 or 4 Sylow 3-subgroups.

1/II/13F Groups, Rings and Modules

State the structure theorem for finitely generated abelian groups. Prove that a finitely generated abelian group A is finite if and only if there exists a prime p such that $A/pA = 0$.

Show that there exist abelian groups $A \neq 0$ such that $A/pA = 0$ for all primes p. Prove directly that your example of such an A is not finitely generated.

2/I/2F Groups, Rings and Modules

Prove that the alternating group A_5 is simple.

2/II/13F Groups, Rings and Modules

Let K be a subgroup of a group G. Prove that K is normal if and only if there is a group H and a homomorphism $\phi : G \to H$ such that

$$K = \{g \in G \ : \ \phi(g) = 1\}\,.$$

Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with a, b, c, d in $\mathbb{Z}$ and $ad - bc = 1$. Let p be a prime number, and take K to be the subset of G consisting of all $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a \equiv d \equiv 1 \,(\mathrm{mod}\ p)$ and $c \equiv b \equiv 0 \,(\mathrm{mod}\ p)$. Prove that K is a normal subgroup of G.

3/I/2F Groups, Rings and Modules

Let R be the subring of all z in $\mathbb{C}$ of the form

$$z = \frac{a + b\sqrt{-3}}{2}$$

where a and b are in $\mathbb{Z}$ and $a \equiv b \,(\mathrm{mod}\ 2)$. Prove that $N(z) = z\bar{z}$ is a non-negative element of $\mathbb{Z}$, for all z in R. Prove that the multiplicative group of units of R has order 6. Prove that $7R$ is the intersection of two prime ideals of R.

[*You may assume that R is a unique factorization domain.*]

3/II/14F Groups, Rings and Modules

Let L be the group $\mathbb{Z}^3$ consisting of 3-dimensional row vectors with integer components. Let M be the subgroup of L generated by the three vectors

$$u = (1,2,3),\ v = (2,3,1),\ w = (3,1,2)\,.$$

(i) What is the index of M in L?

(ii) Prove that M is not a direct summand of L.

(iii) Is the subgroup N generated by u and v a direct summand of L?

(iv) What is the structure of the quotient group L/M?

4/I/2F Groups, Rings and Modules

State Gauss's lemma and Eisenstein's irreducibility criterion. Prove that the following polynomials are irreducible in $\mathbb{Q}\,[x]$:

(i) $x^5 + 5x + 5$;

(ii) $x^3 - 4x + 1$;

(iii) $x^{p-1} + x^{p-2} + \ldots + x + 1,$ where p is any prime number.

4/II/12F Groups, Rings and Modules

Answer the following questions, fully justifying your answer in each case.

(i) Give an example of a ring in which some non-zero prime ideal is not maximal.

(ii) Prove that $\mathbb{Z}[x]$ is not a principal ideal domain.

(iii) Does there exist a field K such that the polynomial $f(x) = 1 + x + x^3 + x^4$ is irreducible in $K[x]$?

(iv) Is the ring $\mathbb{Q}[x]/(x^3 - 1)$ an integral domain?

(v) Determine all ring homomorphisms $\phi : \mathbb{Q}[x]/(x^3 - 1) \to \mathbb{C}$.