Lent Term 2004 J. Saxl

IB Groups, Rings and Modules: Some Past Tripos Questions

On each IB paper, there will be one GRM question in Section 1 and one in Section 2. The questions in Section 2 carry twice as much weight as those in Section 1. On this sheet, there are six plus seven random questions of approximately right difficulty taken (and sometimes slightly adjusted) from various past papers. Unless otherwise indicated, they come from IIA questions on some old course.

SECTION 1

1. (02/1/4(i)) What is a Sylow subgroup? State Sylow's theorems. Show that any group of order 33 is cyclic.

2. (00/1/4(i)) What are the orders of the conjugacy classes in S_5 of $(12)(34), (123)$ and (12345)? Identify the corresponding centralizers. Give the orders of the conjugacy classes in A_5. Show that the alternating group A_5 is simple.

3. (01/2/4(i)) Show that the ring $k = \mathbb{F}_2[x]/(x^2 + x + 1)$ is a field. How many elements does it have?

4. (02/3/4(i)) A ring is Noetherian if all its ideals are finitely generated. State Hilbert's Basis Theorem. Give an example of a Noetherian ring which is an integral domain but not a principal ideal domain.

5. (96/2/3(i)) State the structure theorem for finitely generated modules over a Euclidean domain.
The subgroup G of $\mathbb{Z}^3$ is generated by the row vectors $(6, -8, 6)$ and $(8, -12, 7)$. Describe the structure of G and of the quotient $\mathbb{Z}^3/G$.

6. (94/3/4(i)) Let V be the vector space of all complex polynomials of degree not exceeding n. The endomorphism $\Delta : V \to V$ is defined by
$$(\Delta p)(x) = p(x + 1) - p(x).$$
What is the Jordan normal form of Δ?

SECTION 2

7. (01/2/4(ii)) Let $k = \mathbb{F}_4$ be the field of 4 elements. By considering what happens to a chosen basis of the vector space k^2, or otherwise, find the order of the groups $GL_2(k)$ and $SL_2(k)$.
By considering the set of lines in k^2, or otherwise, show that $SL_2(k)$ is a subgroup of the symmetric group S_5 and identify this subgroup.

8. (00/1/4(ii)) What is a Sylow p-subgroup of a finite group? State Sylow's Theorems on the number of Sylow p-subgroups of a finite group. Let $\mathcal{P}$ be the set of Sylow p-subgroups of a finite group G and let $Q \leq G$ be an arbitrary p-subgroup. By considering the conjugacy action of Q on $\mathcal{P}$, or otherwise, show that $Q \leq P$ for some Sylow p-subgroup P.
How many Sylow 5-subgroups has A_5? How many Sylow 3-subgroups? How many Sylow 2-subgroups?

9. (03/2/4(ii)) State and prove the Eisenstein criterion for irreducibility of polynomials with integer coefficients.
Show that if p is a prime, the polynomial

$$1 + x + \cdots + x^{p-1}$$

is irreducible over $\mathbb{Z}$.

10. (00/4/4) Let R be a unique factorization domain. What is a primitive polynomial in $R[x]$? Prove that the product of two primitive polynomials in $R[x]$ is primitive. Identify the primes in $R[x]$.
Factorize the polynomials $x^{11} - 1$ and $x^{10} - 1$ in $\mathbb{Z}[x]$ into irreducibles. Briefly justify why the factors you give are irreducible.

11. (02/2/4(ii)) What are the units in $\mathbb{Z}[i]$? What are the primes in $\mathbb{Z}[i]$? Justify your answers.
Factorize $11 + 7i$ into primes in $\mathbb{Z}[i]$.

12. (94/3/3) State the structure theorem for modules over a Euclidean domain.
Let V be a vector space of dimension n over a field k and α an endomorphism of V with minimal polynomial μ and characteristic polynomial ρ. Explain how, using α, we may regard V as a $k[x]$-module. Show that if V is cyclic then $\mu = \rho$. Using the structure theorem, deduce that in general μ divides ρ, and ρ divides μ^t for some t.

13. (IB87/2/4) Let A be a finitely generated abelian group which is the direct sum of g copies of $\mathbb{Z}$ and a finite abelian group of order n.
(a) For each integer $m \geq 1$, let $mA = \{mx : x \in A\}$. Prove that mA is a subgroup of finite index in A.
(b) Prove that the index $(A : mA)$ of mA in A satisfies $(A : mA) \geq m^g$, with equality if and only if m is coprime to n.
(c) Let ψ be a homomorphism from A into another abelian group. By considering a composite map

$$A \to \psi(A) \to \psi(A)/m\psi(A),$$

or otherwise, prove that if m is coprime to n and if $\psi(A)$ has also summand $\mathbb{Z}^g$, then

$$(\psi(A) : m\psi(A)) = (A : mA).$$

Comments and corrections should be sent to `j.saxl@dpmms.cam.ac.uk`.