Lent Term 2016 O. Randal-Williams

IB Groups, Rings, and Modules // Example Sheet 1

1. (i) What are the orders of elements of the group S_4? How many elements are there of each order?
   (ii) How many subgroups of order 2 are there in S_4? Of order 3? How many cyclic subgroups are there of order 4?
   (iii) Find a non-cyclic subgroup $V \leq S_4$ of order 4. How many such subgroups are there?
   (iv) Find a subgroup $D \leq S_4$ of order 8. How many such subgroups are there?

2. (i) Show that A_4 has no subgroups of index 2. Exhibit a subgroup of index 3.
   (ii) Show that A_5 has no subgroups of index 2, 3, or 4. Exhibit a subgroup of index 5.
   (iii) Show that A_5 is generated by (12)(34) and (135).

3. Calculate the size of the conjugacy class of (123) as an element of S_4, as an element of S_5, and as an element of S_6. Find in each case its centraliser. Hence calculate the size of the conjugacy class of (123) in A_4, in A_5, and in A_6.

4. Suppose that $H, K \lhd G$ with $H \cap K = \{e\}$. By considering the *commutator* $[h, k] := hkh^{-1}k^{-1}$ with $h \in H$ and $k \in K$, show that any element of H commutes with any element of K. Hence show that $HK \cong H \times K$.

5. Let p be a prime number, and G be a non-abelian group of order p^3.
   (i) Show that the centre $Z(G)$ of G has order p.
   (ii) Show that if $g \notin Z(G)$ then its centraliser $C(g)$ has order p^2.
   (iii) Hence determine the sizes and numbers of conjugacy classes in G.

6. (i) For $p = 2, 3$ find a Sylow p-subgroup of S_4, and find its normaliser.
   (ii) For $p = 2, 3, 5$ find a Sylow p-subgroup of A_5, and find its normaliser.

7. Show that there are no simple groups of orders 441 or 351.

8. Let p, q, and r be prime numbers, not necessarily distinct. Show that no group of order pq is simple. Show that no group of order pq^2 is simple. Show that no group of order pqr is simple.

9. (i) Show that any group of order 15 is cyclic.
   (ii) Show that any group of order 30 has a normal subgroup of order 15.

10. Let N and H be groups, and $\phi : H \to \mathrm{Aut}(N)$ be a homomorphism. Show that we can define a group operation on the set $N \times H$ by

$$(n_1, h_1) \bullet (n_2, h_2) = (n_1 \cdot \phi(h_1)(n_2), h_1 \cdot h_2).$$

Show that the resulting group G contains copies of N and H as subgroups, that N is normal in G, that $NH = G$, and that $N \cap H = \{e\}$.

By finding an element of order 3 in $\mathrm{Aut}(C_7)$, construct a non-abelian group of order 21.

Additional Questions

11. Let p be a prime number. How many elements of order p are there in S_p? What are their centralisers? How many Sylow p-subgroups are there? What are the orders of their normalisers? If q is another prime number which divides $p-1$, show that there exists a non-abelian group of order pq.

12. Show that there are no simple groups of order 300 or 320.

13. Show that a group G of order 1001 contains normal subgroups of order 7, 11, and 13. Hence show that G is cyclic. [You may want to use Question 4.]

14. Let G be a simple group of order 60. Deduce that $G \cong A_5$, as follows. Show that G has six Sylow 5-subgroups. By considering the conjugation action of the set of Sylow 5-subgroups, show that G is isomorphic to a subgroup $G \leq A_6$ of index 6. By considering the action of A_6 on A_6/G, show that that there is an automorphism of A_6 taking G to A_5.

15. Let G be a group of order 60 which has more than one Sylow 5-subgroup. Show that G is simple.

16. Let G be a finite group with cyclic and non-trivial Sylow 2-subgroup. By considering the permutation representation of G on itself, show that G has a normal subgroup of index 2. [Show that a generator for the Sylow subgroup induces an odd permutation of G.]

17. (Frattini argument) Let $K \lhd G$ and P be a Sylow p-subgroup of K. Show that any element $g \in G$ may be written as $g = nk$ with $n \in N_G(P)$ and $k \in K$, and hence that $G = N_G(P)K$. [Observe that $g^{-1}Pg$ is also a Sylow p-subgroup of K, so is conjugate to P in K.] Deduce that $G/K \cong N_G(P)/N_K(P)$.

Comments or corrections to `or257@cam.ac.uk`

Lent Term 2016 O. Randal-Williams

IB Groups, Rings, and Modules // Example Sheet 2

All rings in this course are commutative and have a multiplicative identity.

1. Let $\omega = \frac{1}{2}(1+\sqrt{-3}) \in \mathbb{C}$, let $R = \{a + b\omega : \ a, b \in \mathbb{Z}\}$, and let $F = \{a + b\omega : \ a, b \in \mathbb{Q}\}$. Show that R is a subring of $\mathbb{C}$, and that F is a subfield of $\mathbb{C}$. What are the units of R?

2. *An element r of a ring R is called nilpotent if $r^n = 0$ for some n.*
   (i) What are the nilpotent elements of $\mathbb{Z}/6\mathbb{Z}$? Of $\mathbb{Z}/8\mathbb{Z}$? Of $\mathbb{Z}/24\mathbb{Z}$? Of $\mathbb{Z}/1000\mathbb{Z}$?
   (ii) Show that if r is nilpotent then r is not a unit, but $1+r$ and $1-r$ are units.
   (iii) Show that set of the nilpotent elements form an ideal N of R. What are the nilpotent elements in the quotient ring R/N?

3. Let r be an element of a ring R. Show that the polynomial $1 + rX \in R[X]$ is a unit if and only if r is nilpotent. Is it possible for the polynomial $1 + X$ to be a product of two non-units?

4. Show that if I and J are ideals in the ring R, then so is $I \cap J$, and the quotient $R/(I \cap J)$ is isomorphic to a subring of the product $R/I \times R/J$.

5. Let $I_1 \subset I_2 \subset I_3 \subset \cdots$ be ideals in a ring R. Show that the union $I = \bigcup_{n=1}^{\infty} I_n$ is also an ideal. If each I_n is proper, explain why I must be proper.

6. Write down a prime ideal in $\mathbb{Z} \times \mathbb{Z}$ that is not maximal. Explain why in a finite ring all prime ideals are maximal.

7. Explain why, for p a prime number, there is a unique ring of order p. How many rings are there of order 4?

8. Let R be an integral domain and F be its field of fractions. Suppose that $\phi : R \to K$ is an injective ring homomorphism from R to a field K. Show that ϕ extends to an injective homomorphism $\Phi : F \to K$ from F to K. What happens if we do not assume that ϕ is injective?

9. Let R be any ring. Show that the ring $R[X]$ is a principal ideal domain if and only if R is a field.

10. *An element r of a ring R is called idempotent if $r^2 = r$.*
   (i) What are the idempotent elements of $\mathbb{Z}/6\mathbb{Z}$? Of $\mathbb{Z}/8\mathbb{Z}$? Of $\mathbb{Z}/24\mathbb{Z}$? Of $\mathbb{Z}/1000\mathbb{Z}$?
   (ii) Show that if r is idempotent then so is $r' = 1 - r$, and that $rr' = 0$. Show also that the ideal (r) is naturally a ring, and that R is isomorphic to $(r) \times (r')$.

11. Let F be a field, and let $R = F[X, Y]$ be the polynomial ring in two variables.
   (i) Let I be the principal ideal $(X - Y)$ of R. Show that $R/I \cong F[X]$.
   (ii) Describe R/I when $I = (X^2 + Y)$.
   (iii) What can you say about $R/(X^2 - Y^2)$? Is it an integral domain? Does it have nilpotent or idempotent elements? ...
   (iv) Show that $\mathbb{C}[X, Y]/(X^2 + Y^2 - 1) \cong \mathbb{C}[T, T^{-1}]$. [Hint: Think about trigonometric functions.]

Additional Questions

12. Is every abelian group the additive group of some ring?

13. Let I be an ideal of the ring R and $P_1, \ldots, P_n$ be prime ideals of R. Show that if $I \subset \bigcup_{i=1}^{n} P_i$, then $I \subset P_i$ for some i.

14. A sequence $\{a_n\}$ of rational numbers is a *Cauchy sequence* if $|a_n - a_m| \to 0$ as $m, n \to \infty$, and $\{a_n\}$ is a *null sequence* if $a_n \to 0$ as $n \to \infty$. Quoting any standard results from Analysis, show that the set of Cauchy sequences with componentwise addition and multiplication form a ring C, and that the null sequences form a maximal ideal N.

    Deduce that C/N is a field, with a subfield which may be identified with $\mathbb{Q}$. Explain briefly why the equation $x^2 = 2$ has a solution in this field.

15. Let ϖ be a set of prime numbers. Write $\mathbb{Z}_\varpi$ for the collection of all rationals m/n (in lowest terms) such that the only prime factors of the denominator n are in ϖ.

    (i) Show that $\mathbb{Z}_\varpi$ is a subring of the field $\mathbb{Q}$ of rational numbers.

    (ii) Show that any subring R of $\mathbb{Q}$ is of the form $\mathbb{Z}_\varpi$ for some set ϖ of primes.

    (iii) Given (ii), what are the maximal subrings of $\mathbb{Q}$?

16. Show that there is no isomorphism as in Question 11 (iv) if both instances of $\mathbb{C}$ are replaced by $\mathbb{Q}$.

Comments or corrections to `or257@cam.ac.uk`

Lent Term 2016 O. Randal-Williams

IB Groups, Rings, and Modules // Example Sheet 3

All rings in this course are commutative and have a multiplicative identity.

1. Show that $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\omega]$ are Euclidean domains, where $\omega = \frac{1}{2}(1+\sqrt{-3})$. Show also that the usual Euclidean function $\phi(r) = N(r)$ does not make $\mathbb{Z}[\sqrt{-3}]$ into a Euclidean domain. Could there be some other Euclidean function ϕ making $\mathbb{Z}[\sqrt{-3}]$ into a Euclidean domain?

2. Show that the ideal $(2, 1+\sqrt{-7})$ in $\mathbb{Z}[\sqrt{-7}]$ is not principal.

3. Give an element of $\mathbb{Z}[\sqrt{-17}]$ that is a product of two irreducibles and also a product of three irreducibles.

4. Show that if R is an integral domain then a polynomial in $R[X]$ of degree d can have at most d roots. Give a quadratic polynomial in $(\mathbb{Z}/8\mathbb{Z})[X]$ that has more than two roots.

5. Determine whether or not the following rings are fields, PIDs, UFDs, integral domains:
$$\mathbb{Z}[X], \quad \mathbb{Z}[X]/(X^2+1), \quad \mathbb{Z}[X]/(2, X^2+1), \quad \mathbb{Z}[X]/(2, X^2+X+1), \quad \mathbb{Z}[X]/(3, X^3-X+1).$$

6. Determine which of the following polynomials are irreducible in $\mathbb{Q}[X]$:
$$X^4+2X+2, \quad X^4+18X^2+24, \quad X^3-9, \quad X^3+X^2+X+1, \quad X^4+1, \quad X^4+4.$$

7. Let R be an integral domain. The *greatest common divisor* (gcd) of non-zero elements a and b in R is an element d in R such that d divides both a and b, and if c divides both a and b then c divides d.
   (i) Show that the gcd of a and b, if it exists, is unique up to multiplication by a unit.
   (ii) In lectures we have seen that, if R is a UFD, the gcd of two elements exists. Give an example to show that this is not always the case in an integral domain.
   (iii) Show that if R is a PID, the gcd of elements a and b exists and can be written as $ra+sb$ for some $r, s \in R$. Give an example to show that this is not always the case in a UFD.
   (iv) Explain briefly how, if R is a Euclidean domain, the Euclidean algorithm can be used to find the gcd of any two non-zero elements. Use the algorithm to find the gcd of $11+7i$ and $18-i$ in $\mathbb{Z}[i]$.

8. Find all ways of writing the following integers as sums of two squares: 221, 209×221, 121×221, 5×221.

9. By working in $\mathbb{Z}[\sqrt{-2}]$, show that the only integer solutions to $x^2+2=y^3$ are $x=\pm 5$, $y=3$.

10. Exhibit an integral domain R and a (non-zero, non-unit) element of R that is not a product of irreducibles.

11. Let $\mathbb{F}_q$ be a finite field of q elements.
    (i) Show that the prime subfield K (that is, the smallest subfield) of $\mathbb{F}_q$ has p elements for some prime number p. Show that $\mathbb{F}_q$ is a vector space over K and deduce that $q = p^k$, for some k.
    (ii) Show that the multiplicative group of the non-zero elements of $\mathbb{F}_q$ is cyclic.
    (Hint, recall the structure theorem for finite abelian groups, and note Question 4.)

Additional Questions

12. (a) Consider the polynomial $f = X^3Y + X^2Y^2 + Y^3 - Y^2 - X - Y + 1$ in $\mathbb{C}[X,Y]$. Write it as an element of $(\mathbb{C}[X])[Y]$, that is collect together terms in powers of Y, and then use Eisenstein's criterion to show that f is prime in $\mathbb{C}[X,Y]$.

    (b) Let F be any field. Show that the polynomial $f = X^2 + Y^2 - 1$ is irreducible in $F[X,Y]$, unless F has characteristic 2. What happens in that case?

13. Show that the subring $\mathbb{Z}[\sqrt{2}]$ of $\mathbb{R}$ is a Euclidean domain. Show that the units are $\pm(1 \pm \sqrt{2})^n$ for $n \geqslant 0$.

14. Let V be a 2-dimensional vector space over the field $\mathbb{F}_q$ of q elements, let Ω be the set of its 1-dimensional subspaces.

    (a) Show that Ω has size $q+1$ and $GL_2(\mathbb{F}_q)$ acts on it. Show that the kernel Z of this action consists of scalar matrices and the group $PGL_2(\mathbb{F}_q) = GL_2(\mathbb{F}_q)/Z$ has order $q(q^2-1)$. Show that the group $PSL_2(\mathbb{F}_q)$ obtained similarly from $SL_2(\mathbb{F}_q)$ has order $q(q^2-1)/d$ with $d = \gcd(q-1, 2)$.

    (b) Show that Ω may be identified with the set $\mathbb{F}_q \cup \{\infty\}$ in such a way that $GL_2(\mathbb{F}_q)$ acts on Ω as the group of Möbius transformations $z \mapsto \frac{az+b}{cz+d}$. Show that in this action $PSL_2(\mathbb{F}_q)$ consists of those transformations whose determinant is a square in $\mathbb{F}_q$.

15. Show that the groups $SL_2(\mathbb{F}_4)$ and $PSL_2(\mathbb{F}_5)$ defined above both have order 60. Use this and some questions from sheet 1 to show that they are both isomorphic to the alternating group A_5. Show that $SL_2(\mathbb{F}_5)$ and $PGL_2(\mathbb{F}_5)$ both have order 120, that $SL_2(\mathbb{F}_5)$ is not isomorphic to S_5, but $PGL_2(\mathbb{F}_5)$ is.

Comments or corrections to `or257@cam.ac.uk`

IB Groups, Rings, and Modules // Example Sheet 4

1. Let M be a module over a ring R, and let N be a submodule of M.
   (i) Show that if M is finitely generated then so is M/N.
   (ii) Show that if N and M/N are finitely generated then so is M.
   (iii) Show that if M/N is free, then $M \cong N \oplus M/N$.
2. We say that an R-module satisfies condition (N) if any submodule is finitely generated. Show that this condition is equivalent to condition (ACC): every increasing chain of submodules terminates.
3. Let R be a Noetherian ring. Show that the R-module R^n satisfies condition (N), and hence that any finitely generated R-module satisfies condition (N).
4. Let M be a module over an integral domain R. An element $m \in M$ is a *torsion* element if $rm = 0$ for some non-zero $r \in R$. Show that the set T of all torsion elements in M is a submodule of M, and that the quotient M/T is *torsion-free*—that is, contains no non-zero torsion elements.
5. (i) Is the abelian group $\mathbb{Q}$ torsion-free? Is it free? Is it finitely generated?
   (ii) What are the torsion elements in the abelian group $\mathbb{Q}/\mathbb{Z}$? In $\mathbb{R}/\mathbb{Z}$? In $\mathbb{R}/\mathbb{Q}$?
   (iii) Prove that $\mathbb{R}$ is not finitely generated as a module over the ring $\mathbb{Q}$.
6. Use elementary operations to bring the integer matrix $A = \begin{pmatrix} -4 & -6 & 7 \\ 2 & 2 & 4 \\ 6 & 6 & 15 \end{pmatrix}$ to Smith normal form D.

   Check your result using minors. Explain how to find invertible matrices P, Q for which $D = QAP$.
7. Work out the invariant factors of the matrices

$$\begin{pmatrix} 2X-1 & X & X-1 & 1 \\ X & 0 & 1 & 0 \\ 0 & 1 & X & X \\ 1 & X^2 & 0 & 2X-2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} X^2+2X & 0 & 0 & 0 \\ 0 & X^2+3X+2 & 0 & 0 \\ 0 & 0 & X^3+2X^2 & 0 \\ 0 & 0 & 0 & X^4+X^3 \end{pmatrix}$$

   over $\mathbb{R}[X]$.
8. Let G be the abelian group with generators a, b, c, and relations $6a + 10b = 0$, $6a + 15c = 0$, $10b + 15c = 0$. (That is, G is the free abelian group on generators a, b, c quotiented by the subgroup generated by the elements $6a + 10b$, $6a + 15c$, $10b + 15c$). Determine the structure of G as a direct sum of cyclic groups.
9. Prove that a finitely-generated abelian group G is finite if and only if $G/pG = 0$ for some prime p. Give a non-trivial abelian group G such that $G/pG = 0$ for all primes p.
10. Let A be a complex matrix with characteristic polynomial $(X+1)^6(X-2)^3$ and minimal polynomial $(X+1)^3(X-2)^2$. Write down the possible Jordan normal forms for A.
11. Find a 2×2 matrix over $\mathbb{Z}[X]$ that is not equivalent to a diagonal matrix.
12. Let M be a finitely-generated module over a Noetherian ring R, and let f be an R-module homomorphism from M to itself. Does f injective imply f surjective? Does f surjective imply f injective? What happens if R is not Noetherian?

Additional Questions

13. Write $f(n)$ for the number of distinct abelian groups of order n.

    (i) Show that if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ with the p_i distinct primes and $a_i \in \mathbb{N}$ then $f(n) = f(p_1^{a_1}) \cdots f(p_k^{a_k})$.

    (ii) Show that $f(p^a)$ equals the number $p(a)$ of partitions of a, that is, $p(a)$ is the number of ways of writing a as a sum of positive integers, where the order of summands is unimportant. (For example, $p(5) = 7$, since $5 = 4{+}1 = 3{+}2 = 3{+}1{+}1 = 2{+}2{+}1 = 2{+}1{+}1{+}1 = 1{+}1{+}1{+}1{+}1$.)

14. A real $n \times n$ matrix A satisfies the equation $A^2 + I = 0$. Show that n is even and A is similar to a block matrix $\begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix}$ with each block an $m \times m$ matrix (where $n = 2m$).

15. Show that a complex number α is an algebraic integer if and only if the additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated (i.e. $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module). Furthermore if α and β are algebraic integers show that the subring $\mathbb{Z}[\alpha, \beta]$ of $\mathbb{C}$ generated by α and β also has a finitely generated additive group and deduce that $\alpha - \beta$ and $\alpha\beta$ are algebraic integers.

    Show that the algebraic integers form a subring of $\mathbb{C}$.

16. What is the rational canonical form of a matrix?

    Show that the group $GL_2(\mathbb{F}_2)$ of non-singular 2×2 matrices over the field $\mathbb{F}_2$ of 2 elements has three conjugacy classes of elements.

    Show that the group $GL_3(\mathbb{F}_2)$ of non-singular 3×3 matrices over the field $\mathbb{F}_2$ has six conjugacy classes of elements, corresponding to minimal polynomials $X + 1, (X + 1)^2, (X + 1)^3, X^3 + 1, X^3 + X^2 + 1, X^3 + X + 1$, one each of elements of orders $1, 2, 3$ and 4, and two of elements of order 7.

Comments or corrections to `or257@cam.ac.uk`