Lent 2026 **GROUPS, RINGS & MODULES – SHEET 1** G. Taylor

Questions with bracketed numbers are optional.

1. For each d dividing 24, how many subgroups of order d does S_4 have?

2. (i) Show that A_5 is generated by (12)(34) and (135).

   (ii) Show that A_5 has no subgroup of index 2, 3 or 4, and that any subgroup of index 5 is isomorphic to A_4.

3. Let $n \geqslant 5$. Find the centraliser of (12345) in S_n, and find the size of its conjugacy class in A_n.

4. Let p be a prime number, and G be a non-abelian group of order p^3.

   Show that the centre $Z(G)$ of G has order p, and that if $g \notin Z(G)$ then its centraliser $C(g)$ has order p^2. Hence determine the number of conjugacy classes in G.

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

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

6. Show that any group of order 15 is cyclic, and that any group of order 30 has a subgroup of order 15.

7. Show that any group of order 1001 is cyclic.

8. Show that there are no simple groups of order 441 or 351 or 112.

9. Let p, q, r be distinct prime numbers. Show that no group of order pq or pq^2 or pqr is simple.

10. Let p be prime. How many elements of order p are there in S_p? What are their centralisers? How many Sylow p-subgroups are there? What is the order of their normalisers?

    If q is a prime which divides $p - 1$, show that there exists a non-abelian group of order pq.

11. Let N and H be groups, and $\phi : H \to \text{Aut}(N)$ 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 $N \cap H = \{e\}$.

    Use this to construct a non-abelian group of order 21.

12. Let G be a simple group of order 60. By considering the conjugation action of G on the set of its Sylow 5-subgroups, show that G is isomorphic to a subgroup of A_6 of index 6. Then, by considering the coset action of A_6, show that that G is isomorphic to A_5.

(13) Let G be a group of order 60 with more than one Sylow 5-subgroup. Show that G is simple.

(14) Let G be a finite simple group with a (non-trivial) cyclic Sylow 2-subgroup. Show that $G \cong C_2$.

Lent 2026 **GROUPS, RINGS & MODULES – SHEET 2** G. Taylor

All rings are commutative and have a multiplicative identity.

1. Let $\omega = \frac{1}{2}(1+\sqrt{-3})$ and let $R = \{a + b\omega : a, b \in \mathbb{Z}\}$. Show that R is a subring 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 $\mathbb{Z}/180\mathbb{Z}$?
   (ii) Show that if r is nilpotent then r is not a unit, but $1 + r$ is a unit.
   (iii) Show that the nilpotent elements of R form an ideal N of R. What are the nilpotent elements in the quotient R/N?

3. Let r be an element of a ring R. Show that, in $R[X]$, the polynomial $1 + rX$ 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. Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ 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.

5. 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 $R/I \times R/J$. Show further that if there exist $x \in I$ and $y \in J$ with $x + y = 1$ then $R/(I \cap J) \cong R/I \times R/J$. What does this result say when $R = \mathbb{Z}$?

6. Give an example of a monic quadratic polynomial in $(\mathbb{Z}/8\mathbb{Z})[X]$ that has more than two roots.

   Now let R be an integral domain. Show that a polynomial in $R[X]$ of degree d can have at most d roots. Deduce that the natural ring homomorphism from $R[X]$ to the ring of all functions from R to R is injective if and only if R is infinite.

7. Find an ideal in $\mathbb{Z} \times \mathbb{Z}$ that is prime but not maximal.

8. How many rings are there of order 7? How many rings are there of order 4?

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

10. Show that the set $\mathcal{P}(S)$ of all subsets of a set S is a ring with respect to the operations of symmetric difference and intersection. What is the ideal (A)? What is the ideal (A, B)?

11. 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 $\mathbb{Z}/24\mathbb{Z}$? How many are there in $\mathbb{Z}/180\mathbb{Z}$?
    (ii) Show that if r is idempotent then so is $1 - r$. Show that the ideal (r) is naturally a ring, and that R is isomorphic to $(r) \times (1 - r)$.

12. A ring R is called *Boolean* if every element of R is idempotent.

    Prove that every finite Boolean ring is isomorphic to a power-set ring $\mathcal{P}(S)$ for some set S. Give an example to show that this need not remain true for infinite Boolean rings.

(13) Find an abelian group which is not the additive group of any ring. Is every abelian group the additive group of some ideal in some ring?

(14) Find all subrings of the ring $\mathbb{Q}$.

Lent 2026 **GROUPS, RINGS & MODULES – SHEET 3** G. Taylor

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

4. Determine whether or not the following rings are fields, PIDs, UFDs, integral domains:

$$\mathbb{Z}[X],\quad \mathbb{Z}[X]/(X^2+1),\quad \mathbb{Z}[X]/(2,X^2+1),\quad \mathbb{Z}[X]/(2,X^2+X+1),\quad \mathbb{Z}[X]/(3,X^3-X+1).$$

5. Determine which of the following polynomials are irreducible in $\mathbb{Q}[X]$:

$$X^4+2X+2,\quad X^4+18X^2+24,\quad X^3-9,\quad X^3+X^2+X+1,\quad X^4+1,\quad X^4+4.$$

6. Find all irreducible polynomials of degree 5 in $(\mathbb{Z}/2\mathbb{Z})[X]$.

   Does $(\mathbb{Z}/2\mathbb{Z})[X]$ contain irreducible polynomials of arbitrarily large degree?

7. (i) From lectures we know that, in a UFD, the highest common factor (hcf) of two elements exists. Give an example to show that this is not always the case in an integral domain.

   (ii) Show that, in a PID, the hcf 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.

   (iii) Use the Euclidean algorithm to find the hcf of $11+7i$ and $18-i$ in $\mathbb{Z}[i]$.

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

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

10. Let F be a field. Show that the ideal (X,Y) in $F[X,Y]$ is not principal. Can the ideal (X^2, XY, Y^2) be generated by two elements?

    Show that $F[X,Y]/(X-Y) \cong F[X]$.

    Is $F[X,Y]/(X^2-Y^2)$ an integral domain? Does it have nilpotent or idempotent elements?

11. If a UFD has at least one irreducible, must it have infinitely many (non-associate) irreducibles?

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

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

(14) Let the set $\mathbb{Z}$ be given a ring structure such that the multiplication is the same as the usual multiplication on $\mathbb{Z}$. Must its addition be the same as the usual addition on $\mathbb{Z}$?

Lent 2026 **GROUPS, RINGS & MODULES – SHEET 4** G. Taylor

All rings are commutative and have a multiplicative identity.

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 is equivalent to condition (ACC): every increasing chain of submodules terminates.

   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).

3. 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 $r \in R$.

   (i) Show that the torsion elements of M form a submodule T of M. What are the torsion elements in the quotient M/T?

   (ii) What are the torsion elements in the $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$? In $\mathbb{R}/\mathbb{Z}$? In $\mathbb{R}/\mathbb{Q}$?

   (iii) Is the $\mathbb{Z}$-module $\mathbb{Q}$ torsion-free? Is it free? Is it finitely generated?

4. Find the Smith normal form of the following matrices over $\mathbb{Z}$ and $\mathbb{Q}[X]$, respectively.

$$\begin{pmatrix} -4 & -6 & 7 \\ 2 & 2 & 4 \\ 6 & 6 & 15 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} X^2+2X & 0 & 0 & 0 \\ 0 & X^2+3X+2 & 0 & 0 \\ 0 & 0 & X^3+2X^2 & 0 \\ 0 & 0 & 0 & X^4+X^3 \end{pmatrix}$$

5. Find a 2×2 matrix over $\mathbb{Z}[X]$ that is not equivalent to a diagonal matrix.

6. How many abelian groups are there of order 6? Of order 60? Of order 6000?

7. Let G be the abelian group with generators a, b, c, and relations $6a + 10b = 0$, $6a + 15c = 0$, $10b + 15c = 0$. Determine the structure of G as a direct sum of cyclic groups.

8. 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.

9. Let A be a complex matrix with characteristic polynomial $(X+1)^6(X-2)^3$ and minimal polynomial $(X+1)^3(X-2)^2$. What are the possible Jordan normal forms for A? What are the invariant factors of the corresponding $\mathbb{C}[X]$-modules?

10. 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 $n = 2m$).

11. 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 if R is not Noetherian?)

(12) Show that a complex number α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ 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 is also finitely-generated $\mathbb{Z}$-module and deduce that $\alpha - \beta$ and $\alpha\beta$ are algebraic integers. Show that the algebraic integers form a subring of $\mathbb{C}$.

(13) Let R be a ring. Show that if the R-modules R^m and R^n are isomorphic then $m = n$.