O4 Rings and Modules Lent 1996

Example sheet 1 (of 4).

All rings are commutative with 1

1. Let A be a set satisfying all the axioms for a ring with identity except for commutativity of addition. Show that this can be deduced from the other axioms.

2. Show from the ring axioms that $0 \times x = 0$.

3. (a) Let R be a ring, X a set. Show that the set R^X of all maps $f : X \to R$ is a ring under pointwise operations. When is R^X a field?

(b) Define a function $f \in R^X$ to be *of finite support* if the set $\{x \in X : f(x) \neq 0\}$ is finite. Show that the functions of finite support form a subring $R^{(X)}$ of R^X. When is it a field?

4. Which of the following sets of functions are rings under the pointwise operations?
   (a) continuous functions $(0, 1) \to [0, 1]$;
   (b) continuous functions $(0, 1) \to \mathbb{R}$;
   (c) differentiable functions $(0, 1) \to \mathbb{R}$;
   (d) analytic functions $\mathbb{C} \to \mathbb{C}$;
   (e) continuous functions $f : (0, 1) \to \mathbb{R}$ such that $1/f$ is also continuous.

5. Let A be an Abelian group (written additively) and A^A the set of all maps from A to A with pointwise addition. Define multiplication to be composition of maps.

(a) Show that this does not in general give A^A a ring structure.

(b) Let $\mathcal{E}(A)$ be the subset of A^A consisting of group homomorphisms from A to itself. Show that with multiplication defined as composition, $\mathcal{E}(A)$ satisfies all the axioms for a ring except commutativity of multiplication.

(c) Show that $\mathcal{E}(A)$ is a ring when A is a cyclic group.

6. Let $R = \mathbb{Z}[\sqrt{-d}]$ be the set of all complex numbers of the form $z = a + b\sqrt{-d}$ where a, b are integers and d is a square-free natural number. Show that R is a ring with 4 units if $d = 1$ and 2 units otherwise.
[Hint: define $N(z) = z\bar{z}$ and deduce that z is a unit iff $N(z) = 1$.]

7. Let R be a ring and $d \in R$. Define addition and multiplication on $R \times R$ by

$$(x, y) + (u, v) = (x + u, y + v)$$
$$(x, y) \cdot (u, v) = (xu + dyv, xv + yu).$$

Show that with these operations, $R \times R$ is a ring, denoted by $R[\sqrt{d}]$. What is $R[\sqrt{1}]$?

8. Let S be a non-zero subring of a ring R. Say which of the following assertions are true and which are false, giving proofs or counter-examples.
   (i) If R has no non-zero divisors of zero, then neither has S.
   (ii) If S has no non-zero divisors of zero, then neither has R.
   (iii) The characteristics of R and S are equal.

9. (a) If I, J are ideals of R, show that $I \cap J$ and $I + J$ are also ideals. Show that IJ is an ideal contained in $I \cap J$. Give an example to show that IJ may be strictly contained in $I \cap J$.

(b) If I_1, I_2, I_3 are ideals of R, show that the following laws hold:

(i) $I_1 \cap (I_2 + I_3) \supseteq (I_1 \cap I_2) \cap (I_1 \cap I_3)$;

(ii) $I_1 + (I_2 \cap I_3) \supseteq (I_1 + I_2) \cap (I_1 + I_3)$;

(iii) If $I_1 \supseteq I_2$ then $I_1 \cap (I_2 + I_3) = I_2 + (I_1 \cap I_3)$.

10. Let $R = F_1 \times F_2 \times \cdots \times F_n$, where the F_i are fields. Describe all the ideals of R and show that they are principal.

11. Suppose that $A \supseteq B$ are ideals of the ring R. Prove that A/B is an ideal of R/B and that $R/A \cong (R/B)/(A/B)$.

Prove also that if C, D are ideals in R, then the ideals $C \cap D$ and $C + D$ satisfy $C/(C \cap D) \cong (C + D)/D$.

12. Let R be a ring and $R[X_1, \ldots, X_n]$ the ring of polynomials in n (commuting) variables over R. For $p = \sum c_{i_1 \ldots i_n} X_1^{i_1} \cdots X_n^{i_n}$, not zero, define the *total degree* to be

$$d^0(p) = \max\left\{\sum_{j=1}^n i_j : c_{i_1 \ldots i_n} \neq 0\right\}.$$

Put $d^0(0) = -\infty$. Show that $d^0(pq) \leq d^0(p)d^0(q)$ and that equality holds for all p, q in $R[X_1, \ldots, X_n]$ if and only if R is an integral domain.

13. Let R be a ring and S a subring of R. The elements $r_1, \ldots, r_n$ of R are *algebraically independent* over S if, for a function $c : \mathbb{N}^n \to R$ of finite support, the condition

$$\sum_{\mathrm{i} \in \mathbb{N}^n} c(\mathrm{i}) r_1^{i_1} \cdots r_n^{i_n} = 0$$

implies c is the zero function.

Prove that, given a ring S and an integer $n \geq 1$, there exists a unique (up to isomorphism) ring $R \supset S$ such that R is generated by S and n elements which are algebraically independent over S.

14. Let A be an additive group and R a ring. Let $R^{(A)}$ be the set of functions from R to A of finite support. Define addition on $R^{(A)}$ pointwise and multiplication by *convolution*:

$$f \cdot g : b \mapsto \sum_{a \in A} f(a) g(b - a).$$

Show that this gives a ring structure on $R^{(A)}$.

Identify the ring $R(A)$ when A is (i) $\mathbb{Z}$, (ii) $\mathbb{Z}^n$.

15. Is there a ring (with identity) whose additive group is the group $\mathbb{Z}^{(\mathbb{Z})}$ of functions of finite support from $\mathbb{Z}$ to itself?

16. (a) Let R be a ring, let P denote the positive integers and $D(R)$ the functions from P to R of finite support with pointwise addition and *Dirichlet multiplication*

$$f \times g : n \mapsto \sum_{d | n} f(d) g(n/d),$$

summing over the positive disivors of n. Show that this defines a ring structure on $D(R)$.

(b) Let $\zeta : P \to R$ denote the function $\zeta : n \mapsto 1$ and let $\mu : P \to R$ the function $\mu(n) = 0$ if n has a square factor and $\mu(p_1 \cdots p_r) = (-1)^r$ when the p_i are distinct primes. Show that ζ and μ are in the multiplicative group of $D(R)$.

17. Construct an Abelian group which is not (isomorphic to) the additive group of any ring with identity.

18. (a) Suppose R is a ring with every element *idempotent*, that is, $x^2 = x$ for all x. Show that R has characteristic 2. Give examples of such rings with 2^n elements for $n = 1, 2, \ldots$.

(b) Given a set X, let $P(X)$ denote the power set of X, that is, the set of all subsets of X (including X itself and the empty set). Define addition and multiplication on $P(X)$ as follows:

$$A + B = (A \cup B) \setminus (A \cap B)$$
$$A \times B = A \cap B.$$

Show that under these operations $P(X)$ is a ring. What are the zero and unity elements? Show that every element of $P(X)$ is idempotent.

(c) Let X be an infinite set and F the collection of finite subsets of X. Show that F is a subring of $P(X)$, but that F is not isomorphic to $P(Y)$ for any set Y.

19. Suppose R is a finite non-zero ring. Show that R is made up of elements which are either units or zero-divisors but not both.

20. Let R be a ring and I, J ideals of R such that $R = I + J$. Show that R/IJ is isomorphic to the direct product of R/I and R/J.

21. Let R, S be rings. Show that the ideals of $R \times S$ are precisely the products $I \times J$ where I, J are ideals of R, S respectively. Deduce that every ideal of $\mathbb{Z} \times \mathbb{Z}$ is principal.

22. An ideal I of A is *maximal* if $I \neq A$ and whenever J is an ideal of A with $I \subseteq J \subseteq A$ then either $I = J$ or $J = A$.

(i) Show that an ideal I of A is maximal iff A/I is a field.

(ii) Show that if A is a field then $\{0\}$ and A are the only ideals.

(iii) Show that every maximal ideal is prime.

23. Does every ring have a maximal ideal?

24. Let I be a proper ideal of R. Show that R has I as unique maximal ideal iff every element of $R \setminus I$ is a unit in R.

25. Suppose that I is a maximal ideal of $\mathbb{Z}[X]$. Show that $I \cap \mathbb{Z} \neq \{0\}$ and deduce that $\mathbb{Z}[X]/I$ is finite.

26. Let C be the ring of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ and let

$$I = \{f \in C : f(0) = 0\}.$$

Show that I is a maximal ideal of C and identify the structure of C/I (that is, find a "well-known" ring isomorphic to it). Is the ideal I principal?

27. If A is a subring of B and I is an ideal of A, define

$$IB = \{b_1p_1 + \cdots + b_np_n : b_i \in B,\ p_i \in I\}$$

Show that

$$\frac{A[X]}{IA[X]} \cong \left(\frac{A}{I}\right)[X].$$

28. Let R be a ring, $a, b, c \in R$ and put

$$d_k = ka + bc^k, \qquad k = 0, 1, \dots .$$

Show that the ideal generated by all the d_k is finitely generated.

Let $a, b_i, c_i \in R$ for $i = 1, \dots, n$ and put

$$d_k = ka + \sum_{i=1}^{n} b_i c_i^k, \qquad k = 0, 1, \dots .$$

Show that the ideal generated by all the d_k is finitely generated.
Hint: you might find it helpful to note that if $p = \sum_{i=0}^{m} p_i X^i$ is divisible by $(X-q)^r$ then the *formal derivative* $Dp = \sum_{i=1}^{m} ip_i X^{i-1}$ is divisible by $(X-q)^{r-1}$.

29. Let I be any ideal of the ring R, and define the *radical* of I to be

$$\sqrt{I} = \{x \in R : x^n \in I \text{ for some integer } n \geq 1\}.$$

Show that $\sqrt{I}$ is an ideal of R, and that $\sqrt{\sqrt{I}} = \sqrt{I}$.

30. Let R be a ring and A, B ideals of R. Show that the set

$$(A : B) = \{x \in R : xb \in A \text{ for all } b \in B\}$$

is an ideal of R such that $(A : B)B \subseteq A \subseteq (A : B)$. Show also that $(A : B) = (A : A+B)$ and that if C is also an ideal of R then $((A : B) : C) = (A : BC)$.

31. Find the idempotent elements of the residue class rings $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$.

32. An element x of a ring R is *nilpotent* if $x^n = 0$ for some integer $n \geq 0$. Find the nilpotent elements of the residue class rings $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$.

33. Let R be a ring. Show that the set N of nilpotent elements is an ideal of R and that the quotient ring R/N has no nilpotent elements.

34. Let A denote a ring. The *nilradical* of A, $N(A)$ is the set of all nilpotent elements of A. An ideal I of A is *prime* if $I \neq A$ and whenever $xy \in I$ then $x \in I$ or $y \in I$. Prove that $N(A)$ is the intersection of all the prime ideals of A.

35. Let R be a ring and $a \in R$. Show that $1 - aX$ is a unit in $R[X]$ if and only if a is nilpotent.

36. List the units, zero-divisors, idempotent and nilpotent elements of $\mathbb{Z}/m\mathbb{Z}$ for $m = 2, \ldots, 12$. Generalise.

37. Let I be an ideal and S a subring of R. Show that $I \cap S$ is an ideal of S , that $I + S$ is a subring of R and that

$$S/(I \cap S) \cong (I + S)/I.$$

38. Show that $\mathbb{R}[X]/\langle X^2 + 1 \rangle \cong \mathbb{C}$.

39. Which of the following properties of a ring are preserved under taking (i) subrings (ii) quotient rings (iii) product rings (iv) polynomial rings ?

(a) having no non-zero divisors of zero;
(b) having no non-zero nilpotent elements;
(c) having a unique maximal ideal.

40. Let R be a ring for which $R[X]$ is a PID: show that R is a field.

41. Let R, S be rings. The Cartesian product $R \times S$ is a ring under componentwise operations. Show that there are homomorphisms from $R \times S$ to R and to S, and homomorphisms from R and from S to $R \times S$. Identify the kernels and images of these morphisms.

42. Suppose R is a ring with characteristic p prime. Show that $\phi : R \to R$, where $\phi(r) = r^p$, is a homomorphism. Give an example for which ϕ is not injective.

43. Show that the only ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ are the zero map and the identity map.

44. Let R, R' be rings with identity elements 1_R, $1_{R'}$ S, S' subsets of R, R' respectively and $\alpha : R \to R'$ a homomorphism such that $\alpha(S) \subseteq S'$. Show that there exists a unique homomorphism $\alpha_\star : R[S^{-1}] \to R'[S'^{-1}]$ such that $\alpha_\star(a/1_R) = \alpha(a)/1_{R'}$ for all $a \in R$.

45. Let R be a principal ideal ring, S a multiplicative system in R. Show that $R[S^{-1}]$ is a principal ideal ring.

46. (i) Show that an ideal of R is prime iff R/I is an integral domain.
(ii) Is the set of continuous functions $\mathbb{R}^n \to \mathbb{R}$ an integral domain?
(iii) Show that if D is an integral domain, then so is $D[X]$.

47. (i) Show that $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.
(ii) Show that $\mathbb{Z}$ is not a field.
(iii) Show that for any ring A, the polynomial ring $A[X]$ is not a field.

48. Let R be a ring, P a prime ideal of R and S the complement of P in R. Show that $R[S^{-1}]$ has a unique maximal ideal, consisting of all elements of the form p/s for $P \in P$ and $S \in S$.

49. For which values of n is $\mathbb{Z}/n\mathbb{Z}$ a field? An integral domain? When does it have non-zero nilpotent elements? Non-trivial idempotents? Just one maximal ideal? An element which is not a square?

50. Let R_1 be the ring of rational numbers with denominator a power of a given prime p and let R_2 be the ring of rational numbers with denominator not divisible by p. Show that R_1 and R_2 are principal ideal domains, that R_1 has infinitely many prime ideals and R_2 has only two.

51. For a set ϖ of rational primes, write $\mathbb{Z}_{(\varpi)}$ for the ring of all rationals m/n such that the only prime divisors of n are in ϖ. Suppose R is a subring of $\mathbb{Q}$. Show that $R = \mathbb{Z}_{(\varpi)}$ for some set ϖ. Show further that if ϖ consists of all primes except one, then no proper subring of $\mathbb{Q}$ properly contains R.

52. Suppose $\theta : R \to S$ is a homomorphism of rings and that I is an ideal of R. Show that $\theta(I)$ is an ideal of $\theta(R)$. By considering the map $x \mapsto \theta(I) + \theta(x)$, show that $R/(I + \ker\theta) \cong \theta(R)/\theta(I)$. Deduce that if J is an ideal of R then $R/(I + J) \cong (R/J)/(J + I/J)$.

53. Suppose $\theta : R \to S$ is a homomorphism of rings. Show that every ideal of $\theta(R)$ has the form $\theta(I)$ for some ideal I of R and that there is only one such I that contains $\ker\theta$. By taking $R = \mathbb{Z}$ and $S = \mathbb{Z}/2\mathbb{Z}$, show that I need not be unique.

54. (a) Show that if $\theta : \mathbb{Z} \longrightarrow \mathbb{Q}$ is a homomorphism then $\theta n = n$ for all n in $\mathbb{Z}$.

(b) Suppose $\theta : R \longrightarrow S$ is a homomorphism from a ring R to a ring S and that x is in R. Show that if $f \in R[X]$ and θf has its obvious meaning and if $f(x) = 0$ then $\theta f(\theta x) = 0$.

(c) Show that $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\frac{1}{17}]$ are mutually non-isomorphic.

55. Let k be a field and a an element of k. Let P be the subset of $k[X]$ comprising all polynomials f such that $f(a) = 0$. Prove that $k[X]/P \cong k$ and deduce that P is a maximal ideal of $k[X]$. Suppose now that K is another field properly containing k and that a is in K but not k. What can you definitely say about P? Need P be maximal ?

56. Let P be a prime ideal of R. Prove that $P[X]$ is a prime ideal of $R[X]$. If P is a maximal ideal of R, does it follow that $P[X]$ is a maximal ideal of $R[X]$?

57. Let k be a field and let $R = k[X, Y]$ be the polynomial ring. Let I be the ideal of R generated by $X + Y$. Show that $R/I \cong k[X]$.

58. Show that the following conditions on a ring A are equivalent

(N1) Every ideal I of A is finitely generated;

(N2) Given any chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$, there exists an N such that $I_n = I_N$ for all $n \geq N$;

(N3) Every non-empty set of ideals in A has a maximal element (with respect to $\subseteq$).

Such a ring is *Noetherian.*

The questions on these example sheets are intended to provide a choice for the student and supervisor. Many are easy: most are straight-forward. A possible selection might be 2, 3, 5, 6, 9(a), 16, 18, 20 or 21, 22, 29, 42, 49; with a further selection from 25, 28, 30, 33, 43, 59 for those who want something a little harder.

Comments to R.G.E. Pinch at DPMMS or email `rgep@dpmms.cam.ac.uk`

O4 Rings and Modules Lent 1996

Example sheet 2.

All rings are commutative with 1

1. Let a be an element of a ring R. Show that the kernel of the evaluation map $f(X) \mapsto f(a)$ from $R[X]$ to R is the principal ideal $\langle X - a \rangle$.

2. Show that if $d < -1$ the unit group of $\mathbb{Z}[\sqrt{d}]$ is $\{\pm 1\}$. Show that $U(\mathbb{Z}[\sqrt{2}]) \supseteq \{\pm(1+\sqrt{2})^m : m \in \mathbb{Z}\}$. Is this the whole group?

3. Define a map $\lambda : \mathbb{Z}[\sqrt{d}] \to \mathbb{R}^2$ by $\lambda : (a + b\sqrt{d}) \mapsto \left(a + b\sqrt{d}, a - b\sqrt{d}\right)$. Show that the image of λ is discrete and deduce that the unit group of $\mathbb{Z}[\sqrt{d}]$ is of the form $\{\pm\alpha^n : n \in \mathbb{Z}\}$ for some α.

4. Show that 2 is irreducible in $\mathbb{Z}[\sqrt{10}]$. Is 2 prime in this ring ?

5. By considering the elements $n + \mathrm{i}\sqrt{n}$ and $1 + \mathrm{i}\sqrt{n}$, show that $\mathbb{Z}[\mathrm{i}\sqrt{n}]$ is not a UFD for $n \geq 3$.

6. In $\mathbb{Z}[\sqrt{6}]$, it is clear that $6 = (\sqrt{6})^2 = 3.2$. Does this show that $\mathbb{Z}[\sqrt{6}]$ is not Euclidean?

7. By considering the ideal of $\mathbb{Z}[\sqrt{-5}]$ generated by 3 and $2 + \sqrt{-5}$, show that $\mathbb{Z}[\sqrt{-5}]$ is not a PID. Show further that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

8. Factorise the following elements into products of primes:
   (a) $11 + 7\mathrm{i}$ in $\mathbb{Z}[\mathrm{i}]$;
   (b) $4 + 7\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$;
   (c) $4 - \sqrt{-3}$ in $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

9. Let R be a UFD and K its field of fractions. Suppose a/b is a non-zero element of K with a, b relatively prime in R. Show that if a/b is a root of $a_0 + a_1X + \cdots + a_nX^n$ (where $a_i \in R$, $0 \leq i \leq n$) then $a \mid a_0$ and $b \mid a_n$.
   What are the rational roots of $2x^4 - 2x^3 + x^2 + 6x - 7$?

10. Let R be an integral domain. Show that the remainder after dividing $X^m - 1$ by $X^d - 1$ (in $R[X]$) is $X^r - 1$, where $m = qd + r$, $0 \leq r < d$. Show that an *h.c.f.* of $X^m - 1$ and $X^n - 1$ is $X^d - 1$, where d is the *h.c.f.* of m and n. Show further that for a positive integer l, $(l^m - 1, l^n - 1) = l^{(m,n)} - 1$.

11. Let d be a positive integer, not divisible by any square, and suppose that $\mathbb{Z}[\sqrt{-d}]$ is a principal ideal domain. Show that d is prime.

12. Show that a field is its own field of fractions.

13. Let $\mathbb{Z}[\omega]$ be the set of complex numbers of the form $a + b\sqrt{-3}$ where a and b are either both integers or both half odd integers. Show that $\mathbb{Z}[\omega]$ is a ED with respect to the function $\mathcal{N}(a + b\sqrt{-3}) = a^2 + 3b^2$. What is the group of units of this ring?

14. (a) Show by direct verification that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field.

(b) Let $\omega = \exp(2\pi i/3)$. Show that $\mathbb{Q}(\omega) = \{a + b\omega : a, b \in \mathbb{Q}\}$ a subfield of $\mathbb{C}$.

(c) In each case, give yet another proof that the object in question is a field.

15. Let D be an ID with infinitely many elements, of which only finitely many are irreducible. Suppose every non-unit has an irreducible factor. Show that D has infinitely many units.

16. Recall that an integer a is a *quadratic residue* modulo a prime p if the equation $x^2 \equiv a \bmod p$ holds for some integer x, otherwise a is a *quadratic non-residue.* The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined to be 0 if $a \equiv 0 \bmod p$, otherwise $+1$ for a quadratic residue and -1 for a non-residue. Assume $p \neq 2$.

(a) Show that the map $x \mapsto x^2$ is exactly two-to-one on the unit group $(\mathbb{Z}/p)^*$.

(b) Show that the quadratic residues form a subgroup of $(\mathbb{Z}/p)^*$.

(c) Show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(d) Show that $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p$.

17. Show that if $p \equiv 1 \bmod 4$ then -1 is a quadratic residue of p. Deduce that p is not an irreducible element of $\mathbb{Z}[i]$. Hence determine the irreducible elements of $\mathbb{Z}[i]$.

18. Show that every prime $p \not\equiv 3 \bmod 4$ is a sum of two squares: $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$. Deduce that an integer is a sum of two squares if and only if every prime factor which is $\equiv 3 \bmod 4$ occurs to an even power in the prime factorisation.

Express 2210 as the sum of two squares in four different ways.

19. Give a complete description of the integer solutions to the equation $x^2 + y^2 = z^2$.

20. Let D be an ID. Show that $D[X]$ is an ID, and that it is a PID if and only if D is a field.

21. Exhibit a UFD which is not a PID.

22. Let D be a UFD with field of fractions F. Let $f(X) = a_n X^n + \cdots + a_0 \in D[X]$ with degree $n \geq 1$. Suppose there is a prime element p in D such that $p \mid a_i$ for $1 \leq i \leq n-1$ and that $p \nmid a_n$, $p^2 \nmid a_0$. Prove that $f(X)$ is irreducible in $F[X]$.

Suppose that $f(c) = 0$ for some $c \in F$. Show that $c \in D$ and that $c \mid a_0$.

24. Given a ring R, let $R[\![X]\!]$ denote the ring of formal power series in X over R. Show that if K is a field, then $K[\![X]\!]$ is a PID. What are the units of $K[\![X]\!]$? What are the primes?

25. Prove that a finite integral domain is a field.

26. Show that the ring of Gaussian integers $\mathbb{Z}[i]$ is isomorphic to the quotient ring $\mathbb{Z}[X]/\langle X^2 + 1\rangle$. Show that the principal ideals $\langle 3\rangle$, $\langle 1 + i\rangle$ and $\langle 2 + i\rangle$ are prime, but that $\langle 2\rangle$ and $\langle 5\rangle$ are not.

27. Let R be a commutative principal ideal ring, S a multiplicative system in R. Show that $R[S^{-1}]$ is a principal ideal ring.

28. A ring R is *simple* if R has no ideal other than 0 and R itself, and the multiplication in R is not always zero. Prove that a (commutative) simple ring is a field.

29. (i) Let K be a finite field and let ϕ be a mapping of K into K. Show that there is a polynomial $f(x)$ such that $f(a) = \phi(a)$ for every $a \in K$.

(ii) Give an example to show that the finiteness condition in (i) cannot be dropped.

(iii) Let $f \in \mathbb{C}[X]$ be a polynomial of degree m and let $a_1, \ldots, a_{m+1}$ be distinct rational numbers such that $f(a_i)$ is a rational number. Show that the coefficients of f are rational numbers.

30. (a) Find integers x, y such that $95x + 432y = 1$.
  (b) Express $\frac{77}{505}$ as a fraction $\frac{a}{5} + \frac{b}{101}$.
  (c) Find P, Q, in $\mathbb{Q}[X]$ such that $(X^2 + 2)P + (X^3 - 7)Q = 1$.
  (d) Show that x^2+2 is invertible in the ring $(\mathbb{Z}/7\mathbb{Z})[X]/\langle X^5 + 5\rangle$, where $x = X$ mod $X^5 + 5$, and find its inverse.

31. Show that $\mathbb{Z}$ is not a field and that for any ring A, the polynomial ring $A[X]$ is not a field.

32. Show that $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ is a Euclidean domain for $d = 3, 7, 11$. What can you say about the case $d = 15$?

33. Let R be a ring satisfying $a^2 = a$ for every a in R. Give an examples to show that R may be a PIR, or have an ideal which is not principal.

34. Show that every irreducible in $\mathbb{C}[X]$ is linear and that every irreducible in $\mathbb{R}[X]$ is linear or quadratic.

35. Show that there is an irreducible quadratic in $F_p[X]$.

36. Find the two irreducible cubics in $F_2[X]$, say f_1 and f_2. Establish an explicit isomorphism between the fields $F_2[X]/\langle f_1(X)\rangle$ and $F_2[Y]/\langle f_2(Y)\rangle$. and deduce that $\mathbb{Z}[X]/I$ is finite.

37. Show that the following are Euclidean domains: $\mathbb{Z}[\sqrt{d}]$ for $d = -1, -2, 2, 3$ and $\mathbb{Z}[\omega]$ where ω is a primitive 6th root of 1.

38. For $\alpha = \sqrt{d}$, with $d \equiv 3 \bmod 4$, show that $\mathbb{Z}[\alpha]/\langle 2\rangle$ contains a nilpotent element, and that $\langle 2\rangle = \langle \alpha + 1, 2\rangle^2$.

39. For $\alpha = 2^{1/3}$, show that $\langle 7\rangle$ is a prime ideal in $Z[\alpha]$ and that $\langle 31\rangle$ is not.

40. Let K be a finite field with q elements and put $F(X) = X^q - X$. Show that $F(a) = 0$ for all $a \in K$ and that if G is any polynomial in $K[X]$ with this property then F divides G.

41. Show that $X^3 - X + 1$ is irreducible in $\mathbb{F}_3[X]$ and that the quotient ring $\mathbb{F}_3[X]/\langle X^3 - X + 1\rangle$ is a field with 27 elements.

42. Let ξ be the image of X mod $X^3 - X$ in $\mathbb{F}_3[X]/\langle X^3 - X\rangle$. Show that the map $\phi : \xi \mapsto (f(0), f(1), f(2))$ gives an isomorphism from $\mathbb{F}_3[X]/\langle X^3 - X\rangle$ to the product $\mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_3$.

43. Let $d \geq 3$ and $R = \mathbb{Z}[\sqrt{-d}]$. Show that 2 is irreducible but not prime in R.

44. Factorise the following polynomials in $\mathbb{Q}[X]$:

$$X^2+1,\ X^2-X+1,\ 2X^5-6X^3+9X^2-15,\ 2x^4-2x^3+x^2+6x-7.$$

45. (a) Let K be a finite field of order q. Let $I_q(d)$ be the number of irreducible polynomials of degree n in $K[X]$. Show that

$$q^n = \sum_{d|n} dI_q(d)$$

where the sum runs over the positive divisors d of n. Deduce that

$$I_q(n) = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}$$

where μ is the function defined in question 1.16(b).

(b) By estimating $I_q(n)$ directly, show that there is a finite field of every prime power order.

46. Discuss the factorisation of $X^n - 1$ over the field of $q = p^f$ elements.

The questions on these example sheets are intended to provide a choice for the student and supervisor. Many are easy: most are straight-forward. A possible selection might be 2, 4, 5, 8, 13, 21, 25, 26, 30, 32, 36, 37 with a further selection from 3, 10, 15, 33, 38, 39, 42, 45(a) for those who want something a little harder. Questions 16–18 review material from Quadratic Mathematics in the spirit of this course.

Comments to R.G.E. Pinch at DPMMS or email rgep@dpmms.cam.ac.uk

Example sheet 4.

All rings are commutative with 1

1. Review your notes on Linear Mathematics. Which standard results on vector spaces and linear maps over a field remain true for modules and homomorphisms over a ring? Look for counterexamples for those that fail.

2. (a) Give an example in a $\mathbb{Z}$-module for which the exchange lemma fails.
(b) Give an example of a free $\mathbb{Z}$-module F and a set S which generates F, such that no subset of S generates F, but S is not a basis.
(c) Give an example of a $\mathbb{Z}$-module with a proper submodule of the same rank.

3. Show that R has a natural structure as R-module. What are the submodules?

4. Let A and B be submodules of M. Show that
(i) $A \cap B$ is a submodule of M;
(ii) $A + B = \{a + b : a \in A, b \in B\}$ is a submodule of M;
(iii) $(A + B)/B \cong A/(A \cap B)$.

5. Let θ be a surjective homomorphism from the R-module M onto N. Let V be a submodule of N and U be the complete inverse image of V under θ. Show that M/U is isomorphic to N/V.

6. Let T, U, W be submodules of the R-module M. Prove or give counter-examples to the following statements.
(i) $T + (U \cap W) = (T + U) \cap (T + W)$;
(ii) $(T + U) \cap W = (T \cap W) + (U \cap W)$;
(iii) $(T + U) \cap W = T + (U \cap W)$ if $T \subseteq W$;
(iv) $T \cap (U + (T \cap W)) = (T \cap U) + (T \cap W)$.

7. Let M be an R-module.
(a) Show that the intersection of any collection of submodules of M is again a submodule of M.
(b) Let $S \subseteq M$. Show that

$$\langle S\rangle = \{r_1 s_1 + \cdots + r_n s_n : s_i \in S\} = \bigcap_{S \subseteq U \leq M} U$$

where the intersection runs over all submodules U of M containing S.
(c) Show that $U + W = \langle U \cup W\rangle$.

8. An R-module M is *finitely generated* or *FG* if there are $m_1, \ldots, m_n \in M$ such that $M = Rm_1 + \cdots + Rm_n$. If N is a submodule of M, show that M is FG if N and M/N are. Does the converse hold?

9. Let M be a module over R and X any set. Show that the set of maps M^X becomes a module over R under pointwise operations. When is it finitely generated?

10. Let $f \in M^X$. Define the *support* of f to be $\sigma(f) = \{x \in X : f(x) \neq 0\}$.
(a) Define the functions of *finite support* to be

$$M^{(X)} = \{f \in M^X : \sigma(f) \text{ is finite }\}.$$

Show that $M^{(X)}$ is a submodule of M^X.
(b) Identify $R^{(\mathbb{N})}$ with the additive group of a well-known ring.
(c) Prove a similar result to (a) for the functions of countable support.

11. An R-module M is *cyclic* if there is $m \in M$ such that $M = Rm$.
(a) Show that any FG $\mathbb{Z}$-submodule of the additive group of rationals is cyclic.
(b) Show that R/J is a cyclic R-module for any ideal J of R.
(c) Show that if M is cyclic then there is an ideal I of R such that M is isomorphic to R/I as R-module.
(d) Give an example to show that a submodule of a cyclic module need not be cyclic.

12. An R-module M is *irreducible* if the only submodules of M are O and M.
(a) Show that irreducible implies cyclic, but not conversely.
(b) Let M, N be irreducible. Describe the R-module homomorphisms from M to N.

13. Let M be an irreducible R-module. Let $m \in M$, $m \neq 0$ and let $\operatorname{ann} m = \{r \in R : rm = 0\}$. Show that $\operatorname{ann} m$ is a maximal ideal of R and that M is isomorphic to $R/\operatorname{ann} m$.

14. Let R be an ID, F a free R-module and M a submodule of F. Must M be free? Must M be finitely generated?

15. For any R-module V, let $\gamma(V)$ denote the smallest number of elements in a generating set for V. If B is a submodule of the R-module A and $C = A/B$, show that

$$\gamma(C) \leq \gamma(A) \leq \gamma(B) + \gamma(C).$$

Give examples to show that equality need not hold. Is it true that $\gamma(B) \leq \gamma(A)$?

16. Let R be an ID and F a free R-module of rank n. Suppose F is generated by $S = \{m_1, \ldots, m_n\}$. Show that S is a basis of F. Deduce that $R^m \cong R^n$ iff $m = n$.

17. Let $\mathcal{X} = \{x_\alpha : \alpha \in \mathrm{A}\}$ be a subset of a module M. Show that $\mathcal{X}$ is a basis for M iff whenever N is a module and $\mathcal{Y} = \{y_\alpha : \alpha \in \mathrm{A}\}$ is a subset of N, there is a unique module morphism $\phi : M \to N$ such that $\phi(x_\alpha) = y_\alpha$ for all $\alpha \in \mathrm{A}$.
If such a morphism always exists (without assuming uniqueness), must $\mathcal{X}$ be linearly independent? If there is always at most one such morphism (without assuming existence), must $\mathcal{X}$ be a generating set for M?

18. (a) Let W be a subset of the R-module M. Define the *annhilator* of W to be the set

$$W^b = \{a \in R : aw = 0 \text{ for all } w \in W\}.$$

Show that $W^\flat$ is a ideal of R and that $W^\flat = \langle W\rangle^\flat$.

(b) Let I be an ideal of R. Define

$$I^\sharp = \{m \in M : im = 0 \text{ for all } i \in I\}.$$

Show that $I^\sharp$ is a submodule of M.

(c) Show that $(W^\flat)^\sharp \supseteq W$ and $(I^\sharp)^\flat \supseteq I$. Give examples to show that equality need not hold in either case.

(d) Show that $W^{\flat\sharp\flat} = W^\flat$ and $I^{\sharp\flat\sharp} = I^\sharp$.

[The annihilator $W^\flat$ is often denoted $\operatorname{ann} W$.]

19. Let R be a commutative ring with 1. Define an R-module structure on $\operatorname{Hom}_R(M,N)$, the set of all R-module homomorphisms from the R-module M to the R-module N.

20. Let R and S be rings, A a R-module, B a S-module (with the action written on the right) and C a R-module which is also an S-module (again, with the action written on the right) and satisfies $r(cs) = (rc)s$ for $c \in C$, $r \in R$ and $s \in S$. Show how to define the structure of a R-module on $\operatorname{Hom}_S(B,C)$ and the structure of an S-module on $\operatorname{Hom}_R(A,C)$. Prove that the Abelian groups $\operatorname{Hom}_R(A, \operatorname{Hom}_S(B,C))$ and $\operatorname{Hom}_S(B, \operatorname{Hom}_R(A,C))$ are isomorphic.

21. Prove the equivalence of the following three properties of a module P:

(i) Given a morphism $\phi : P \to M/N$ there is a morphism $\psi : P \to M$ such that $\phi = \psi\pi$ where π is the quotient morphism $\pi : M \to M/N$;

(ii) If $P \cong M/N$ then $M = N \oplus P'$ for some $P' \cong P$;

(iii) There is a module Q such that $P \oplus Q$ is free.

[A module with these properties is *projective*.]

22. A sequence of maps between R-modules

$$\ldots M_{i-1} \xrightarrow{\phi_{i-1}} M_i \xrightarrow{\phi_i} M_{i+1} \ldots$$

is *exact* if $\ker\phi_i = \operatorname{im}\phi_{i-1}$ whenever this condition makes sense.

What can you say if $0 \to A \to B$ is exact? What if $B \to C \to 0$ is exact? Hence interpret the statement that $0 \to A \to B \to C \to 0$ is exact.

23. Show that if A is projective then every short exact sequence

$$0 \to A' \to A \to A'' \to 0$$

is *split*: that is, $A \cong A' \oplus A''$.

24. Prove that the short exact sequence

$$0 \to A' \xrightarrow{\alpha} A \xrightarrow{\beta} A'' \to 0$$

is split if and only if there exist homomorphisms $\phi : A'' \to A$ and $\psi : A \to A'$ such that $\alpha\psi + \phi\beta = 1_A$.

25. Let V_k, for $k \in K$, be a family of R-modules, and $V = \bigoplus_{k\in K} V_k$ the external direct sum. If W is any R-module, show that the Abelian group $\operatorname{Hom}_R(V,W)$ is isomorphic to the external direct product of the family $\operatorname{Hom}_R(V_k,W)$, for $k \in K$.

26. Prove that that the external direct sum of a family of projective modules is projective.

27. If R is Noetherian and M is a FG R-module, show that every submodule of M is FG. Is the result true if R is not Noetherian?

28. Suppose that in the following diagram of modules and linear maps the rows are exact and that the diagram *commutes*: that is, any maps with the same domain and codomain (such as ϕg and $f\phi'$) are equal.

$$\begin{array}{ccccccccc} 0 & \to & A & \xrightarrow{\phi} & B & \xrightarrow{\psi} & C & \to & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \to & A' & \xrightarrow{\phi'} & B' & \xrightarrow{\psi'} & C' & \to & 0 \end{array}$$

(a) Show that if f and h are injective, then g is injective.

(b) Show that if f and h are surjective, then g is surjective.

29. Let R be a principal ideal domain. Prove that a finitely generated R-module is free iff it is *torsion-free*: that is, $rm = 0$ implies $r = 0$ or $m = 0$.

30. Let R be a principal ideal domain. Let M be a free R-module on n generators and let N be a submodule of M with $N \neq M$. Prove that N is also a finitely generated free module of rank at most n. Show by an example that N can have rank n. Deduce that a submodule of a finitely generated R-module is again finitely generated.

31. Let E, F be modules over a principal ideal domain. Suppose F is free and $\phi : E \to F$ is a surjective morphism. Show that E has a free submodule F' such that E is the direct sum of $\ker\phi$ and F', and that ϕ restricted to F' is an isomorphism.

32. Let U be a subspace of a (not necessarily FD) vector space V over a field F. The *coset* of $x \in V$ is

$$U + x = \{v \in V : v - x \in U\}$$

and the *quotient* of V by U is the set of cosets $V/U = \{U + x : x \in V\}$.

(a) Verify that $U + x = U + y$ if and only if $x - y \in U$ and that $U + x$ and $U + y$ are either disjoint or equal.

Define operations of addition and scalar multiplication on V/U by $(U + x) + (U + y) = U + (x + y)$ and $\lambda(U + x) = U + \lambda x$.

(b) Show that these operations are well-defined: that is, if $U + x = U + x'$ and $U + y = U + y'$ then $(U + x) + (U + y) = (U + x') + (U + y')$ and $\lambda(U + x) = \lambda(U + x')$. Show that they make V/U into a vector space: the *quotient space*.

(c) Show that the *quotient map* $q : V \to V/U$ defined by $x \mapsto U + x$ is linear, surjective, and has kernel U. Note that any subspace of any vector space is the kernel of some linear map.

(d) If V is finite-dimensional, show that $\dim(V/U) = \dim V - \dim U$.

(e) If $\alpha : V \to W$ is linear with kernel U, show that $\operatorname{im}\alpha$ is naturally isomorphic to V/U. If V is FD, what result on dimensions does this imply?

(f) If $\alpha : V \to W$ is linear and $U \subseteq \ker\alpha$, show that there is a linear map $\alpha_1 : V/U \to W$ such that $\alpha(x) = \alpha_1(q(x))$.

(g) If W is a direct complement of U in V, show that q restricted to W is an isomorphism of W with V/U. If V is FD, what result on dimensions does this imply?

(h) If X is a subspace of V, show that $(U+X)/U$ is naturally isomorphic to $X/(U \cap X)$. If V is FD, what result on dimensions does this imply?

(i) If Y is a subspace of V with $U \subseteq Y$, show that Y/U can be regarded as a subspace of V/U and that $(V/U)/(Y/U)$ is naturally isomorphic to V/Y.

33. Let ϕ be an endomorphism of a free Abelian group A of finite rank. Show that ϕ is injective if and only if $A/\phi(A)$ is finite.

34. Find the invariant factors over $\mathbb{C}[X]$ of

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

and

$$\begin{pmatrix} X^2+2X & 0 & 0 & 0 \\ 0 & (X+2)(X+1) & 0 & 0 \\ 0 & 0 & X^3+2X^2 & 0 \\ 0 & 0 & 0 & X^4+X^3 \end{pmatrix}$$

35. (a) How many Abelian groups are there of order 15? 32? 120? 900?

(b) Let $p(n)$ be the number of partitions of n: so $p(3) = 2$ $(3 = 1+1+1 = 1+2)$. Use this function to express the number of Abelian groups of order N.

36. A is a 4×4 matrix over $\mathbb{Q}$ which satisfies $(A^2 - 4A + I)(A^2 + I) = 0$. What are the possible rational canonical forms for A?

37. Let A and B be $n \times n$ matrices over a field K. Prove that A and B are similar over K if and only if $X1_n - A$ and $X1_n - B$ are equivalent over $K[X]$.

38. Show that the matrices

$$\begin{pmatrix} 3 & 2 & -5 \\ 2 & 6 & -10 \\ 1 & 2 & -3 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 6 & 20 & -34 \\ 6 & 32 & -51 \\ 4 & 20 & -32 \end{pmatrix}$$

are similar.

39. Find the Jordan normal forms of

$$\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}; \quad \begin{pmatrix} 0 & -1 & -1 & -1 \\ 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix}; \quad \begin{pmatrix} 0 & 1 & -2 & 1 \\ -2 & 1 & -6 & 3 \\ 2 & -3 & 0 & 1 \\ 2 & -3 & -2 & 3 \end{pmatrix};$$

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & n \\ & & & & n & n-1 \\ & & & & \vdots & \vdots \\ & & n & \dots & 4 & 3 \\ & n & n-1 & \dots & 3 & 2 \\ n & n-1 & n-2 & \dots & 2 & 1 \end{pmatrix}.$$

40. Show that the minimal and characteristic polynomial determine an $n \times n$ complex matrix up to similarity for $n \leq 3$ but not for $n \geq 4$.

41. Let α be an endomorphism of the FD vector space V with minimal polynomial $\mu(X)$. Suppose that $\mu = fg$ where f and g are coprime. Show that $V = U \oplus W$ where the restriction of α to U has minimal polynomial f and the restriction of α to W has minimal polynomial g.

Show that the result does not hold if f, g are not assumed coprime.

42. Let $R = \mathbb{Z}[\sqrt{d}]$ for some square-free integer d. Show that every ideal of R can be generated by at most two elements.

Let p be a prime number which is not irreducible in R. Show that there is an element $\pi \in R$ such that $\langle p, \pi \rangle$ is a prime ideal of R. Find such an ideal when $d = -5$ and $p = 7$.

43. Let α be an endomorphism of the FD complex vector space V such that $\alpha^m = 1_V$ for some m, and make V a $\mathbb{C}[X]$-module via α. Show that the irreducible submodules of V have dimension 1, and that V is a direct sum of such submodules.

The questions on these example sheets are intended to provide a choice for the student and supervisor. Many are easy: most are straight-forward. A possible selection might be 1, 3, 4, 29, 34–40 with a further selection from 8, 11. 12. 31, 42, 43 for those who want something a little harder.

Comments to R.G.E. Pinch at DPMMS or email rgep@dpmms.cam.ac.uk