1. Let R be a ring. We say that an element $x \in R$ is *nilpotent* if there is some $n \in \mathbb{N}$ such that $x^n = 0$. Let $N = \{x \in R : x \text{ is nilpotent}\}$.

   (a) [8 marks] Show that if R is a commutative ring, then N is an ideal in R. Is N necessarily an ideal if R is not commutative?

   (b) [9 marks] Define what it means for $x \in R$ to be a unit. Show that if R is commutative then the set $1 + N = \{1 + x : x \in N\}$ is a subgroup of $R^\times$ the group of units of R.

   (c) [8 marks] Let $R = \mathbb{Z}/n\mathbb{Z}$. Describe explicitly the elements of the group $R^\times$ and the ideal N of nilpotent elements in terms of the prime factors of n. Calculate the order of N. Show that there are infinitely many n for which $1 + N = R^\times$.

Solution: Part *a*): [S] Clearly if $x \in N$ and $r \in R$ then if $x^n = 0$ it follows $(rx)^n = r^n.x^n = 0$. If $x^n = y^m = 0$, then

$$(x+y)^{n+m} = \sum_{r+s=m+n} \binom{m+n}{r} x^r y^s = 0,$$

since if $r + s = m + n$ we cannot have both $r < n$ and $s < m$ hence one of the factors x^r or y^s is zero, and hence each term in the sum vanishes. If R is not commutative then N is not an ideal: if $R = \mathrm{Mat}_2(\mathbb{C})$ for example, then E_{12} and E_{21} are both nilpotent, but $A = E_{12} + E_{21}$ is a unit since $A^2 = I$.

Part *b*): [S] An element $x \in R$ is a unit if there is a $y \in R$ such that $xy = yx = 1$. The units in R form a group $R^\times$ under multiplication. If $x, y \in N$ and R is commutative, then $(1 + x)(1 + y) = 1 + (x + y + xy)$, and since N is an ideal $x + y + xy \in N$ if $x, y \in N$, so that $1 + N$ is closed under multiplication. Moreover, if $x^n = 0$ we have

$$(1+x)(1+\sum_{i=1}^{n-1}(-x)^i) = 1 + (-1)^{n-1}x^n = 1,$$

so that $1 + x$ is a unit, and since N is an ideal again, $\sum_{i=1}^{n-1}(-x)^i \in N$ so that $(1 + x)^{-1}$ is in $1 + N$. Thus $1 + N$ is a subgroup of $R^\times$ as claimed.

Part *c*): [S] An element $k + n\mathbb{Z}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if there exists $a, b \in \mathbb{Z}$ such that $a.k + bn = 1$, and hence if and only if h.c.f.$(k, n) = 1$. In terms of the prime factors of n, $k + n\mathbb{Z}$ is a unit if and only if every prime p dividing n does not divide k.

[N] Next note that by the Chinese Remainder Theorem, if $n = \prod_{i=1}^r p_i^{a_i}$ is the prime factorization of n (where the $a_i > 0$ and p_i are distinct primes) then $k^m = 0 \mod n$ if and only if $k^m = 0 \mod p_i^{a_i}$ for each i $(1 \leqslant i \leqslant r)$. Clearly such an m exists if and only if p_i divides k for each i $(1 \leqslant i \leqslant r)$. It follows that $N = \{k(p_1 \dots p_r) + n\mathbb{Z} : k \in \mathbb{Z}\}$.

Alternative: Suppose that $k^m = 0 \mod n$. Then if p is a prime dividing n it follows p divides k^m, and hence p divides k (by the defining property of prime elements). Thus if p_i $(1 \leqslant i \leqslant r)$ are the distinct primes dividing n, then we must have $p_i \mid k$ for each every i $(1 \leqslant i \leqslant k)$. Conversely if $p_i \mid k$ for all i, then if $a = \max\{a_i : 1 \leqslant i \leqslant r\}$ (where $n = \prod_{i=1}^r p_i^{a_i}$), clearly n divides k^a, and so $k \mod n$ is nilpotent.

[N] The order of N is thus $|N| = \prod_{i=1}^s p_i^{a_i - 1}$. If $n = 2^k$, then there are 2^{k-1} odd residues modulo n, and hence $1 + N = R^\times$ for any such n. (In fact these are the only integers for which $1 + N = R^\times$).

Turn Over

2. Let $n \in \mathbb{Z}$ be any integer.

   (a) [5 marks] Show that $R_n = \{a + b\sqrt{n} : a, b \in \mathbb{Z}\}$ is a subring of the complex numbers $\mathbb{C}$.

   (b) [8 marks] Let $F_n = \{r/s : r, s \in R_n, s \neq 0\} \subseteq \mathbb{C}$. Then F_n is a field containing $\mathbb{Q}$. Calculate the degree d_n of the field extension $F_n/\mathbb{Q}$.

   (c) [7 marks] Assume now that R_n is a Euclidean domain. Prove that if $x \in F_n$ satisfies $x^m + c_1 x^{m-1} + \ldots + c_{m-1}x + c_m = 0$, where $c_i \in R_n$, $(1 \leqslant i \leqslant m-1)$ then $x \in R_n$.

   (d) [5 marks] Is $\mathbb{Z}[\sqrt{-3}]$ a Euclidean domain? Justify your answer carefully.

   [*You may use any standard properties of a Euclidean domain provided you state them clearly.*]

Solution: Part *a*):[B] Firstly R_n clearly contains 1 and if we have $a_1 + b_1\sqrt{n}, a_2 + b_2\sqrt{n} \in R_n$, then

$$(a_1 + b_1\sqrt{n})(a_2 + b_2\sqrt{n}) = (a_1a_2 + nb_1b_2) + (a_1b_2 + a_2b_1)\sqrt{n} \in R_n,$$

Similarly:

$$(a_1 + b_1\sqrt{n}) - (a_2 + b_2\sqrt{n}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{n} \in R_n,$$

so that by the subring test, R_n is a subring of $\mathbb{C}$.

Part *b*):[S] There are two cases: If n is a square, say $n = m^2$, then clearly $R_n = \mathbb{Z}$ and so $F_n = \mathbb{Q}$ and $d_n = 1$. Now suppose that n is not a square. We claim that 1 and $\sqrt{n}$ are linearly independent over $\mathbb{Q}$. Indeed if $a + b\sqrt{n} = 0$ where $a, b \in \mathbb{Q}$, then multiplying by a suitable common denominator we would obtain $c + d\sqrt{n} = 0$, where $c, d \in \mathbb{Z}$, and by cancelling common factors we can assume g.c.d.$\{c, d\} = 1$. But then we find $c^2 = nd^2$, and so since $\mathbb{Z}$ is a unique factorisation domain, every prime occuring in n occurs to an even power, so that n is a square, contradicting our assumption. Thus $\{1, \sqrt{n}\}$ are $\mathbb{Q}$-linearly independent. Let $Q_n = \mathbb{Q}$-span$\{1, \sqrt{n}\}$. We claim that $F_n = Q_n$ and hence $d_n = 2$ for n a non-square. Indeed since the formulae in part *a*) show that Q_n is clearly closed under addition and multiplication, it is enough to check that if $r = a + b\sqrt{n} \in R_n \backslash \{0\}$ then $1/r \in Q_n$. But if we set $s = a - b\sqrt{n}$, then $rs = a^2 - nb^2 \neq 0$ (since $r, s \neq 0$ as $\{1, \sqrt{n}\}$ are $\mathbb{Q}$-linearly independent and $r \neq 0$) and so $r.(s/(a^2 - nb^2)) = 1$ and $s/(a^2 - nb^2) \in Q_n$ as required.

Alternative: There is a unique ring homomorphism $\phi\colon \mathbb{Q}[t] \to \mathbb{C}$ such that $\phi(t) = \sqrt{n}$. Its image, im(ϕ) is a subring of $\mathbb{C}$ which, since it consists of linear combinations of powers of $\sqrt{n}$ is clearly the subring generated of $\mathbb{Q}$ generated by $\sqrt{n}$. Since $\mathbb{C}$ is an integral domain (it is a field) im(ϕ) is an integral domain, and so $\ker(\phi)$ is a prime ideal of $\mathbb{Q}[t]$. Moreover, since $t^2 - n \in \ker(\phi)$, the kernel is nonzero, and so since $\mathbb{Q}[t]$ is a PID it follows that $\ker(\phi)$ is maximal, and hence im$(\phi) \cong \mathbb{Q}[t]/\ker(\phi)$ is a field, and is therefore clearly the subfield F_n of $\mathbb{C}$ generated by $\sqrt{n}$. Now since $\mathbb{Q}[t]$ is a PID, $\ker(\phi)$ is a principal ideal $\langle f \rangle$ for a unique monic irreducible polynomial f (since irreducibles are prime in a PID) and hence $f \mid t^2 - n$. Now by Gauss's Lemma, $t^2 - n$ is reducible over $\mathbb{Q}[t]$ if and only if it is reducible in $\mathbb{Z}[t]$, which since it is monic, is possible if and only if it has an integer root, that is, if and only if n is a square. If n is a square, clearly $R_n = \mathbb{Z}$ and $F_n = \mathbb{Q}$. Otherwise we see that $t^2 - n$ is irreducible and so is equal to f and $\ker(\phi) = \langle t^2 - n \rangle$. It follows $F_n \cong \mathbb{Q}[t]/\langle t^2 - n \rangle$ is of degree two over $\mathbb{Q}$.

Part *c*): [S] If R_n is an ED, then we may write $x = a/b$ where $a, b \in R_n$ are coprime (indeed this can done in any integral domain provided highest common factors exist, which they do in any ED) then we find that

$$b^m + c_1 a^{m-1} b + \ldots + a^m = 0.$$

But then it follows b divides a^m, and so in particular a and b cannot be coprime unless b is a unit, in which case $x \in R_n$ as required.

Part d): [N] Note that $x = \frac{1-\sqrt{-3}}{2}$ satisfies $x^2 - x + 1 = 0$, but $x \notin R_{-3}$, whence by part c) it cannot be a Euclidean domain.

Alternative: Note that the restriction of the map $z \mapsto z\bar{z}$ is a multiplicative map $N\colon R_{-3} \to \mathbb{Z}_{\geqslant 0}$ sending $a + b\sqrt{-3}$ to $a^2 + 3b^2$. Moreover, if $z \in R_{-3}$ is a unit with inverse w, it follows $1 = N(1) = N(zw) = N(z).N(w)$, so that $N(z) = 1$. Since $a^2 + 3b^2 = 1$ if and only if $a = \pm 1$ and $b = 0$ we see that $R_{-3}^{\times} = \{\pm 1\}$. Next note that N takes the value 4 on each of $2, 1 \pm \sqrt{-3}$, and since the equation $N(z) = 2$ has no solutions it follows that these elements are irreducible, and moreover since $R^{\times} = \{\pm 1\}$ they are not associates. But then the equation $2.2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ shows that irreducibles in R_{-3} are not prime, and so R_{-3} is not a PID and hence not an ED. (*This second solution is close to a problem sheet question, and for that reason I would expect full justification along the lines given, so it is longer to write out than the first solution.)*

3. Let R be a commutative ring.

   (a) [6 marks] (i) Let M be an R-module and let $X \subseteq M$ be any subset. Define what it means for X to be linearly independent, what it means for X to span M, and what it means for M to be a free module.

   (ii) Show how any abelian group is naturally a $\mathbb{Z}$-module.

   [*You need only describe the $\mathbb{Z}$-module structure, not prove that it satisfies the axioms.*]

   (b) [6 marks] Let M be a free module over a commutative ring R. Give a proof or a counter-example to the following:

   (i) If X is a spanning set for M then X necessarily contains a basis of M.

   (ii) If Y is a linearly independent set, then there is a basis X of M containing Y.

   (c) [9 marks] Now let $R = \mathbb{Z}$, $M = \mathbb{Z}^3$ and $X = \{(2,4,6),(2,6,4),(4,6,2)\}$. Let N be the submodule spanned by X. Find a basis of M adapted to N, that is, find a basis $\{e_1,\dots,e_n\}$ for M and elements $r_1,\dots,r_m \in R$ such that $\{r_1e_1,\dots,r_me_m\}$ is a basis of N where $m \in \mathbb{N}$ and $m \leqslant n$.

   (d) [4 marks] State the theorem on the canonical form for a finitely generated module over a Euclidean domain R. Applying the theorem in the case $R = \mathbb{Z}$ or otherwise, find with proof how many isomorphism classes of abelian groups there are of order 675.

Solution: Part *a)i)*:[B] A subset X is *linearly independent* if for any $n \in \mathbb{N}$ and $x_1,\dots,x_n \in X$, $r_1,\dots,r_n \in R$ whenever $\sum_{i=1}^n r_ix_i = 0$ then $r_i = 0$ for all i $(1 \leqslant i \leqslant n)$. A subset X *spans* M if M is the only submodule of M which contains X is the entire module M itself. A module is *free* if it has a basis, that is, a set B which is linearly independent and which spans M.

Part *a)ii)*:[B] If M is an abelian group, then for $m \in M$ define $0.m = m$, and inductively $(n+1).m = n.m + m$ for $n \in \mathbb{Z}_{\geqslant 0}$. If $n < 0$ then set $n.m = -((-n).m)$ the additive inverse (in M) of $(-n).m$.

Part *b)i)*:[S] If we let $R = \mathbb{Z}$ and $M = \mathbb{Z}$, then $X = \{2,3\}$ spans M (because $1 = 3-2$) but no subset of X spans M, so a spanning set need not contain a basis.

Part *b)ii)*: [S] If we take $R = M = \mathbb{Z}$ again, then $\{2\}$ is a linearly independent set, but it cannot be extended to a basis of M (as the only bases of $\mathbb{Z}$ are $\{1\}$ and $\{-1\}$).

Part *c)*: [S] Using row operations on the matrix with rows given by the three vectors in X, we reduce to an upper triangular matrix with rows $\{(2,4,6),(0,2,-2)(0,0,6)\}$ (and thus these rows are linearly independent). Thus if we let $F = \{(1,2,3),(0,1,-1),(0,0,1)\}$ then F is a basis for M since

$$(a,b,c) = a.(1,2,3) + (b-2a).(0,1,-1) + (c-a+b)(0,0,1)$$

and thus $\{2.(1,2,3),2.(0,1,-1),12.(0,0,1)\}$ is a basis for N (or note that the change of basis matrix between this basis and the standard basis is invertible since it has determinant $1 \in \mathbb{Z}^\times$).

Alternative: Let $\{f_1,f_2,f_3\}$ be the standard basis of $\mathbb{Z}^3$ and let $M_1 = \mathrm{Span}\{e_1\}$, $M_2 = \mathrm{Span}\{f_1,f_2\}$ and $M_3 = \mathbb{Z}^3$. We build a basis of M adapted to N by considering $N_i = M_i \cap N$. We have

$$N = \{n(a,b,c) = (2a+2b+4c, 4a+6b+6c, 6a+4b+2c) : a,b,c \in \mathbb{Z}\}$$

so that $n(a,b,c)$ lies in N_1 if $4a+6b+6c = 6a+4b+2c = 0$. The general solution to these two equations is $(a,b,c) = (3k,-7k,5k)$ $(k \in \mathbb{Z})$, and so $N_1 = \{(12k,0,0) : k \in \mathbb{Z}\}$. It follows that if we set $e_1 = (1,0,0)$ then $\{e_1\}$ is a basis of M_1 and $\{12e_1\}$ is a basis of N_1. Next $N_2 = \{n(a,b,c) : 6a+4b+2c = 0\}$, and so $c = -3a-2b$, that is $N_2 = \{(10a+6b, 14a+6b, 0) :$

$a, b \in \mathbb{Z}\}$. Then $N_2/N_1 \cong \{(14a+6b : a, b \in \mathbb{Z}\}$, and since h.c.f.$\{14, 6\}$ is 2, where $14 - 2.6 = 2$, it follows that if $e_2 = (-1, 1, 0)$ then $2e_2 \in N_2$ and $2e_2 + N_1$ is a basis of N_2/N_1. Thus $\{e_1, e_2\}$ is a basis of M_2 and $\{12e_1, 2e_2\}$ is a basis of N_2. Finally, $N/N_2 \cong \{6a+4b+2c : a, b, c \in \mathbb{Z}\} = 2\mathbb{Z}$, and $2 = 2c$ lifts to $(4, 6, 2) \in N$, thus $\{(12, 0, 0), (-2, 2, 0), (4, 6, 2)\}$ is a basis of N. It follows that if we set $e_3 = (2, 3, 1)$ and $r_1 = 12, r_2 = 2, r_3 = 2$ then $\{e_1, e_2, e_3\}$ is a basis of M and $\{r_1e_1, r_2e_2, r_3e_3\}$ is a basis of N as required.

Part *d*): [B for statement of theorem, application is N] The canonical form theorem states that if M is a finitely generated module over a Euclidean domain then there are non-zero non-unit elements $d_1, d_2, \ldots, d_k \in R$ (where $k \in \mathbb{Z}_{\geqslant 0}$) unique up to units, and a unique integer $s \in \mathbb{Z}_{\geqslant 0}$ such that $d_1 \mid d_2 \mid \ldots \mid d_k$ and

$$M \cong R^s \oplus \bigoplus_{i=1}^{k} R/d_iR,$$

An abelian group of order 675 must be of the form $\mathbb{Z}/c_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/c_k\mathbb{Z}$, where $1 < c_1|c_2| \ldots |c_k$ and $\prod_{i=1}^{k} c_i = 675$. Since $675 = 5^2.3^3$ we see $k \leqslant \max\{2, 3\}$. If $k = 1$ then the only possibility is (675). If $k = 2$ the possibilities are $(5, 135)$,$(3, 225)$,$(15, 75)$, since c_1 can only be 5^i3^j where $i \leqslant 1$ and $j \leqslant 1$, with $(i, j) \neq (0, 0)$, while if $k = 3$, each c_i is divisible by 3, and the only possibilities are $(3, 3, 75)$,$(3, 15, 15)$, thus there are 6 isomorphism classes.

Alternative: The primary decomposition for modules over R a PID says that any finitely generated R-module is isomorphic to a module of the form

$$R^s \oplus \bigoplus_{i \in I} R/p_i^{n_i}R,$$

where I is a finite set, $n_i \in \mathbb{Z}_{>0}$ and the p_i a prime in R, and moreover the pairs (p_iR, n_i) are unique. Applying this theorem, if M is an abelian group of order $675 = 5^2.3^3$, we see that $s = 0$, the primes p_i must be 3 or 5. Moreover the integers n_i attached to 3 must sum to 3 while those attached to 5 must sum to 2. It follows the integers must be $(3), (2, 1), (1, 1, 1)$ for 5 and $(2), (1, 1)$ for 3, thus there are $3.2 = 6$ possibilities for the primary decomposition of M.