Algebra III: Rings and Modules
Solutions for Problem Sheet 2, Autumn Term 2022-23

John Nicholson

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

$$\mathbb{Z}[X], \quad \mathbb{Z}[X]/(X^2+1), \quad \mathbb{F}_2[X]/(X^2+1), \quad \mathbb{F}_2[X]/(X^2+X+1), \quad \mathbb{F}_3[X]/(X^2+X+1).$$

Solution: We have Field $\Rightarrow$ PID $\Rightarrow$ UFD $\Rightarrow$ Integral domain. It therefore suffices to find the rightmost property which each ring does not possess.

$\mathbb{Z}[X]$: A UFD but not a PID. We proved that R a UFD implies $R[X]$ a UFD. $\mathbb{Z}$ is a UFD by the fundamental theorem of arithmetic, therefore $\mathbb{Z}[X]$ is a UFD. It is not a PID since, as shown in lectures, $(2, X)$ is not principal.

$\mathbb{Z}[X]/(X^2+1)$: A PID but not a Field. First note that $\mathbb{Z}[X]/(X^2+1) \cong \mathbb{Z}[i]$. To show this, let $\varphi : \mathbb{Z}[X] \to \mathbb{Z}[i]$ be the unique ring homomorphism which maps X to i. This is clearly surjective. By the first isomorphism theorem, it suffices to prove that $\ker(\varphi) = (X^2+1)$. Firstly, $\varphi(X^2+1) = i^2+1 = 0$ so $X^2+1 \in \ker(f)$ and $(X^2+1) \subseteq \ker(\varphi)$ since $\ker(\varphi)$ is an ideal. Let $f \in \ker(\varphi)$. Since X^2+1 is monic, it can be proven by induction (similar to the Euclidean algorithm for $F[X]$ where F is a field) that we can write $f = q(X^2+1)+(a+bX)$ where $q \in \mathbb{Z}[X]$ and $a, b \in \mathbb{Z}$. (Note that $\mathbb{Z}[X]$ is not a Euclidean domain so we cannot use that!) Then $\varphi(f) = a + bi = 0$ implies $a = b = 0$ and so $f = q(X^2+1) \in (X^2+1)$.

We know that $\mathbb{Z}[i]$ is a Euclidean domain and hence is also an PID. It is not a field since $2 \notin \mathbb{Z}[i]^\times$. To see this, let $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}, a+bi \mapsto a^2+b^2$. Suppose $2 \cdot x = 1$ for some $x \in \mathbb{Z}[i]$. Since N is multiplicative, this implies that $1 = N(1) = N(2 \cdot x) = N(2) \cdot N(x) = 4 \cdot N(x)$ which is a contradiction.

$\mathbb{F}_2[X]/(X^2+1)$: Not an integral domain. Note that $(X+1)^2 = X^2+1 = 0$ but $X+1 \neq 0$ since it can be shown that distinct coset representatives are given by $\{a + bX : a, b \in \mathbb{F}_2\}$.

$\mathbb{F}_2[X]/(X^2+X+1)$: A field. Since X^2+X+1 has no roots in $\mathbb{F}_2$, it can't have any linear factors. Hence $X^2+X+1 \in \mathbb{F}_2[X]$ is irreducible. Since $\mathbb{F}_2[X]$ is a Euclidean domain, hence a PID, this implies that $(X^2+X+1) \subseteq \mathbb{F}_2[X]$ is a maximal ideal by a result in lectures. (Note that, in an exam, you should clearly state any results from lectures you are using. We avoid doing this here due to lack of space!) Finally this implies that $\mathbb{F}_2[X]/(X^2+X+1)$ is a field. [Can you find a proof which does not use the fact that $\mathbb{F}_2[X]$ is a Euclidean domain?]

$\mathbb{F}_3[X]/(X^2+X+1)$: Not an integral domain. Similarly to the above example, just note that $(X-1)^2 = X^2+X+1 = 0$ but $X-1 \neq 0$.

2. Given a set $X \subseteq \mathbb{Z}$ of prime numbers, let $S(X) \subseteq \mathbb{Z}$ be the set consisting of 1 and the $n \geq 2$ all of whose prime factors are in X.

   (i) Prove that $S(X)$ is a submonoid of $(\mathbb{Z}, \cdot)$.

   (ii) Let $R_X = S(X)^{-1}\mathbb{Z}$ denote the localisation of the integers at the set $S(X)$. Prove that if X' is another set of prime numbers, then $R_X \cong R_{X'}$ if and only if $X = X'$.

   (iii) Prove that every subring of $\mathbb{Q}$ is of the form R_X for some set of prime numbers X, realising $(a, b) \in R_X$ as the fraction $\frac{a}{b}$.

   (iv) Show that there exists a countable integral domain R (i.e. the set R is countable) for which there exists uncountably many subrings which are distinct up to ring isomorphism.

   Solution:

   (i) To see this is a submonoid, note that it has one by definition, and the product of any two multiples of primes in X must still be a multiple of a prime in X.

   (ii) If X and X' are two sets of prime numbers, and $X \neq X'$, then without loss of generality there is a prime $p \in X$ with $p \notin X'$. Then there exists a multiplicative inverse ($\frac{1}{p} = (1, p)$) in R_X for p but not in $R_{X'}$. Any isomorphism $R_X \to R_{X'}$ must be the identity on $\mathbb{Z}$, since it must send $\iota(m) = 1 + 1 + \cdots + 1$ to $\iota(m)$ for all $m \in \mathbb{Z}$. So it would send p to p, but could not send $\frac{1}{p}$ to anything. Hence R_X and $R_{X'}$ cannot be isomorphic.

   (iii) Let $R \leq \mathbb{Q}$ be a subring. By definition, R contains 1 and so we must have $\mathbb{Z} \leq R \leq \mathbb{Q}$. Let X be the set of primes p for which $\frac{1}{p} \in R$. Then R_X, viewed as a subring of $\mathbb{Q}$, is generated by the $\frac{1}{p}$ for $p \in X$ and so $R_X \leq R$. Suppose there exists $r \in R$ with $r \notin R_X$. Write $r = \frac{a}{b}$ with $b \neq 0$ and $(a, b) = 1$. Since $r \notin R_X$, there must exist a prime $q \notin X$ such that $q \mid b$. Let $b = b'q$. Then $\frac{a}{q} = b'r \in R$. Since $q \mid b$, we have $(q, a) = 1$. By Bezout's lemma, there exists $x, y \in \mathbb{Z}$ such that $ax + qy = 1$. Then $\frac{1}{q} = x \cdot \frac{a}{q} + y \in R$ since $\frac{a}{q}, y \in R$. This implies that $q \in X$ (by definition of X) which is a contradiction.

   (iv) Take $\mathbb{Q}$ (which is countable). Let S denote the set of prime numbers and let $P(S)$ denote the set of subsets of S. Note that $P(S)$ is uncountable (e.g. by Cantor's diagonal argument). For each $X \in P(S)$, we have a subring $R_X \leq \mathbb{Q}$. By (ii), we have that $R_X \cong R_Y$ if and only if $X = Y$ as sets. Hence $\{R_X : X \in P(S)\}$ is an uncountable collection of subrings of $\mathbb{Q}$ which are all pairwise distinct up to ring isomorphism.

3. Let R be a commutative ring and let $S \subseteq R$ be a multiplicative submonoid.

   (i) Let $\iota : R \to S^{-1}R$ be the map $a \mapsto (a, 1)$. Show that ι is injective if and only if S contains no zero divisors or zero. Show further that ι is an isomorphism if and only if $S \subseteq R^\times$.

   (ii) Let $I \subseteq R$ be an ideal. Show that I is prime if and only if $R \setminus I \subseteq R$ is a multiplicative submonoid. Deduce that $R \setminus \{0\} \subseteq R$ is a multiplicative submonoid if and only if R is an integral domain.

   Solution:

   (i) For the first part it suffices to show that the kernel of $\iota : R \to S^{-1}R$ is the set of zero divisors, i.e. elements $r \in R$ such that $rt = 0$ for some $t \in S$. To see this, note that $(a, 1) \sim (b, 1)$ if and only if $t(a - b) = 0$ for some $t \in S$.

   If $S \subseteq R^\times$, then ι is injective by the first part. It is surjective since every $(a, b) \in S^{-1}R$ has $(a, b) \sim (ab^{-1}, 1)$ since $b \in S \subseteq R^\times$. Conversely, if ι is an isomorphism, then S contains no

zero divisors. Let $b \in S$. Since ι is surjective, we must have $(1, b) \sim (r, 1)$ for some $r \in R$. Hence $t \cdot (1 - br)$ for some $t \in S$ which implies that $1 - br = 0$ since S contains no zero divisors. Hence $br = 1$ and $b \in R^\times$.

(ii) Let I be an ideal. Then $R \setminus I$ is a multiplicative submonoid if and only if $1 \in R \setminus I$ and every $a, b \in R \setminus I$ has $ab \in R \setminus I$, i.e. $1 \notin I$ and $ab \in I$ implies $a \in I$ or $b \in I$. This is the definition of prime ideal.

For the last part, just note that $\{0\} \subseteq R$ is a prime ideal if and only if R is an integral domain.

4. A ring R is *simple* if it is non-trivial and its only two-sided ideals are $\{0\}$ and R. The *centre* of a ring R is the subset $Z(R) \subseteq R$ of elements $x \in R$ such that $xy = yx$ for all $y \in R$.

   (i) Let R be any non-trivial ring. Find two nilpotent elements $x, y \in M_2(R)$ such that $x + y$ and xy are both not nilpotent. [Compare with Problem 2 on Problem Sheet 1.]

   (ii) Let $R = F$ be a field. Prove that $M_n(F)$ is simple.

   (iii) Let R be a ring. Prove that the centre of $M_n(R)$ is $Z(R) \cdot I_n$ where I_n denotes the $n \times n$ identity matrix, i.e. the diagonal matrices whose diagonal entries are all equal to some $x \in Z(R)$.

   Solution:

   (i) We can take: $x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Note that this example works for any nonzero ring R.

   (ii) We have to show that if $A \in M_n(F)$ is any matrix, then the two-sided ideal (A) is all of $M_n(F)$. Suppose that $A = (a_{ij})$ for $a_{ij} \in R$. Let i, j be two indices such that $a_{ij} \neq 0$. Then (A) contains the matrix $a_{ij}^{-1} e_{ii} A e_{jj} = e_{ij}$. Therefore it also contains $c e_{ki} e_{ij} e_{j\ell} = e_{k\ell}$ for all k, ℓ and all $c \in F$. Every matrix is a sum of such elements so $(A) = M_n(F)$ as desired.

   (iii) If $A = (a_{\ell,k}) \in M_n(R)$ commutes with e_{ij}, i.e. $e_{ij}A = Ae_{ij}$, then we deduce that $a_{jj} = a_{ii}$ and $a_{jk} = a_{\ell i} = 0$ for $k \neq j$ and $\ell \neq i$. Requiring this for all i, j implies that A is diagonal with all diagonal entries equal, i.e., a scalar matrix. Finally, in order for the scalar matrix to commute with R we require that the scalar be central, i.e., in $Z(R)$. Conversely, it is easy to see that every element in $Z(R) \cdot \mathrm{Id}$ commutes with everything in $M_n(R)$.

5. Let d be an integer which is not a square.

   (i) Show that, in $\mathbb{Z}[\sqrt{d}]$, if I is any nonzero ideal, then $\mathbb{Z}[\sqrt{d}]/I$ is finite. [Hint: If $a + b\sqrt{d} \in I$, show that $a^2 - b^2 d \in I$ as well. Then show that $|\mathbb{Z}[\sqrt{d}]/(m)| = m^2$ if $m \geq 1$.]

   (ii) Show that every nonzero prime ideal in $\mathbb{Z}[\sqrt{d}]$ is maximal.

   (iii) Now suppose $\mathbb{Z}[\sqrt{d}]$ is a UFD. Then show that, for every irreducible $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, then $\mathbb{Z}[\sqrt{d}]/(a + b\sqrt{d})$ is a field.

   (iv) Is $\mathbb{Z}[\sqrt{5}]$ a Euclidean domain? [Hint: Show that $\mathbb{Z}[\sqrt{5}]/(2) \cong (\mathbb{Z}/2)[X]/(X^2)$.]

   Solution:

   (i) We can write all the elements of $\mathbb{Z}[\sqrt{d}]/(m)$ uniquely as $\overline{a} + \overline{b}\sqrt{d}$ for $\overline{a}, \overline{b} \in \mathbb{Z}/m$ (although for the finiteness we don't actually need the uniqueness). Therefore this quotient is finite for

all integers $m \neq 0$. On the other hand if $a + b\sqrt{d} \in I$ for I an ideal (and not both of a and b are zero), then $(a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d \in I$, and since d is not a square, $a^2 - b^2 d$ can only be zero if $a = b = 0$, which we assumed was not the case. Therefore every nonzero ideal I contains a nonzero integer. We conclude that R/I is finite for I a nonzero ideal (its size is at most m^2 for some integer m).

(ii) If I is a nonzero prime ideal, then R/I is a finite integral domain (with finiteness from (i)). Therefore it is a field, and hence I is maximal.

(iii) For every irreducible element $a + b\sqrt{d}$, the UFD property ensures it is a prime element, hence it generates a prime ideal. By (ii) this ideal is maximal. Therefore the quotient $\mathbb{Z}[\sqrt{d}]/(a + b\sqrt{d})$ is a field.

(iv) We will show that it is not a UFD (and hence not a Euclidean Domain). We first claim that $2 \in \mathbb{Z}[\sqrt{5}]$ is irreducible. If not, then we have $2 = xy$ for x, y non-units. Let $N : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}, a + b\sqrt{5} \mapsto (a + b\sqrt{5})(a - b\sqrt{5}) = a^2 - 5b^2$ which is a multiplicative function. We then have that $4 = N(2) = N(x)N(y)$. If $N(x) = \pm 1$, then x would be a unit. Hence we can assume that $N(x) \neq \pm 1$ and similarly $N(y) \neq \pm 1$. Hence $N(x) = N(y) = \pm 2$. If $x = a + b\sqrt{5}$, this implies that $a^2 - 5b^2 = \pm 2$ and so $a^2 = \pm 2 \bmod 5$. However, only ± 1 are squares mod 5 so this is a contradiction.

Since 2 is irreducible it suffices, by (iii), to show that $\mathbb{Z}[\sqrt{5}]/(2)$ is not a field. To see this, note that $(1 + \sqrt{5})^2 = 0$ but $1 + \sqrt{5} \neq 0$ since a set of distinct coset representatives is given by $\{a + b\sqrt{5} : a, b \in \{0, 1\}\}$ (i.e. the ring has order 4). [Note: This can certainly also be proven by showing that $\mathbb{Z}[\sqrt{5}]/(2) \cong (\mathbb{Z}/2)[X]/(X^2)$. But the 'hint' is really to look at the element $2 \in \mathbb{Z}[\sqrt{5}]$.]

6. Let R be a UFD and let $f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$ be primitive (i.e. $\gcd(a_0, \cdots, a_n) = 1$) with $a_n \neq 0$. Let $p \in R$ be irreducible (hence prime) and such that $p \nmid a_n$, $p \mid a_i$ for all $0 \leq i < n$ and $p^2 \nmid a_0$.

   (i) Prove that f is irreducible in $R[X]$. This is *Eisenstein's criterion.* [Hint: If f factorises in $R[X]$, what would an induced factorisation in $R[X]/(p) \cong (R/(p))[X]$ look like?]

   (ii) Use Eisenstein's criterion to show that $3X^5 + 12X^3 + 18$ is irreducible over $\mathbb{Q}$.

   (iii) Show that the UFD hypothesis is not needed if we replace p by a prime ideal P and the conditions $p \mid a_i$ by $a_i \in P$ and $p^2 \nmid a_0$ by $a_0 \notin P^2$.

   Solution: The proof of Eisenstein's criterion is important so I will write the proof below in two different ways: one by considering $R[X]/(p)$ (as in the hint) and another more direct proof working inside of $R[X]$.

   (i) [Proof 1] Observe that, since f is primitive and p divides all coefficients except possibly the leading coefficient, and p is not a unit, it follows that p cannot divide the leading coefficient.

   Now suppose $f = gh$. Since p is prime, $R/(p)$ is an integral domain. Modulo p, we have $f = a_n x^n$ with $a_n \in R/(p)$ nonzero. Thus, modulo p, we have $g = cX^m, h = dX^{n-m}$ for some $c, d \in R/(p)$. Now, if m and $n - m$ are both positive, this implies that p divides the constant terms of both g and h, and hence p^2 divides the constant term of $f = gh$, a contradiction. Hence either m or $n - m$ is zero. Suppose without loss of generality that $m = 0$. Then we claim g has degree zero (this is only obvious modulo p). If not, the leading term of g had coefficient a multiple of p, but then the same would be true for $f = gh$, a contradiction. So g is a scalar. Since we assumed f was primitive, this scalar must be invertible, so f is irreducible in $R[X]$.

(i) [Proof 2] Suppose we have a factorisation $f = gh$ with

$$g = r_0 + r_1 X + \cdots + r_k X^k$$
$$h = s_0 + s_1 X + \cdots + s_\ell X^\ell,$$

for $r_k, s_\ell \neq 0$.

We know $r_k s_\ell = a_n$. Since $p \nmid a_n$, so $p \nmid r_k$ and $p \nmid s_\ell$. We can also look at bottom coefficients. We know $r_0 s_0 = a_0$. We know $p \mid a_0$ and $p^2 \nmid a_0$. So p divides exactly one of r_0 and s_0. wlog, $p \mid r_0$ and $p \nmid s_0$.

Now let j be such that

$$p \mid r_0, \quad p \mid r_1, \cdots, \quad p \mid r_{j-1}, \quad p \nmid r_j.$$

We now look at a_j. This is, by definition,

$$a_j = r_0 s_j + r_1 s_{j-1} + \cdots + r_{j-1} s_1 + r_j s_0.$$

We know $r_0, \cdots, r_{j-1}$ are all divisible by p. So

$$p \mid r_0 s_j + r_1 s_{j-1} + \cdots + r_{j-1} s_1.$$

Also, since $p \nmid r_j$ and $p \nmid s_0$, we know $p \nmid r_j s_0$, using the fact that p is prime. So $p \nmid a_j$. So we must have $j = n$.

We also know that $j \leq k \leq n$. So we must have $j = k = n$. So $\deg g = n$. Hence $\ell = n - h = 0$. So h is a constant. But we also know f is primitive. So h must be a unit. So this is not a proper factorisation.

(ii) First, this is not primitive. To form a primitive polynomial, divide by 3. Then we get $X^5 + 4X^3 + 6$. This polynomial is primitive and hence it is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$, and we can apply Eisenstein's criterion: $2 \mid 6$ and $2 \mid 4$ but $4 \nmid 6$ shows, using $p = 2$, that the polynomial is irreducible.

(ii) The proof is the same as before, using R/P instead of $R/(p)$. Since R/P is an integral domain, everything goes through.

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

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

Solution: By Gauss' lemma, a primitive polynomial is irreducible in $\mathbb{Q}[X]$ if and only if it is irreducible in $\mathbb{Z}[X]$. All polynomials are monic and so primitive. Hence it suffices to determine irreducibility in $\mathbb{Z}[X]$.

$X^4 + 2X + 2$: Irreducible. Apply Eisenstein's criterion for $p = 2$.

$X^4 + 18X^2 + 24$: Irreducible. Apply Eisenstein's criterion for $p = 3$.

$X^3 - 9$: Irreducible. If it is reducible then, since it has degree 3, it must have a linear factor hence a rational root. It is straightforward to show that $\sqrt[3]{9} \notin \mathbb{Q}$ and so $X^3 - 9$ has no rational roots.

$X^3 + X^2 + X + 1$: Not irreducible since equal to $(X + 1)(X^2 + 1)$ which are non-units.

$X^4 + 1$: Irreducible. Substituting $Y = X - 1$ gives $(Y + 1)^4 + 1 = Y^4 + 4Y^3 + 6Y^2 + 4Y + 2$ which is irreducible by Eisenstein's critertion for $p = 2$.

X^4+4: Not irreducible since equal to $(X^2+2)^2-4X^2=(X^2-2X+2)(X^2+2X+2)$.

8. Find the factorisations of $X^{13}+X$, $X^{16}+1$, and X^8+X^4+1 into irreducibles in $\mathbb{F}_2[X]$.

   Solution: We have $X^{13}+X=X(X^{12}+1)=X(X^6+1)^2=X(X^3+1)^4$. Now X^3+1 has 1 as a root, and $X^3+1=(X+1)(X^2+X+1)$. Finally X^2+X+1 has no roots so it is irreducible. We obtain $X^{13}+X=X(X+1)^4(X^2+X+1)^4$.

   Next $X^{16}+1=(X^8+1)^2=(X^4+1)^4=(X^2+1)^8=(X+1)^{16}$.

   Finally $X^8+X^4+1=(X^4+X^2+1)^2=(X^2+X+1)^4$.

9. An element e of a ring R is said to be *idempotent* if $e^2=e$ and $er=re$ for all $r\in R$ (this is often called a *central idempotent*). A nonzero idempotent e is called *primitive* if for any other idempotent e', one has either $e'e=0$ or $e'e=e$. We will call a ring R with no idempotents other than zero or one *indecomposable*.

   (i) Show that if R and S are rings, then $R\times S$ is not indecomposable unless either R or S is the zero ring.

   (ii) Let e be an idempotent element of R other than zero or one. Show that one has an isomorphism:
   $$R\cong R/(e)\times R/(1-e).$$

   (iii) Show that if e is a primitive idempotent then $R/(1-e)$ is indecomposable.

   (iv) Show that a nonzero idempotent e is primitive if and only if e cannot be expressed as e_1+e_2, with e_1,e_2 nonzero idempotents such that $e_1e_2=0$.

   (v) Let R be a ring with finitely many idempotent elements. Show that the number of idempotents is 2^d for some positive integer d, and that R is isomorphic to a product:
   $$R\cong R_1\times R_2\times\cdots\times R_d,$$
   with each R_i indecomposable. Conclude that R has exactly d primitive idempotents.

   Solution:

   (i) If R and S are both not the zero ring, then $(1_R,0_S)$ is an idempotent of $R\times S$ that is neither zero nor one.

   (ii) The ideals generated by (e) and $(1-e)$ are both two-sided ideals since e and $1-e$ commute with all elements of R. Hence it makes sense to write $R/(e)$ and $R/(1-e)$.

   Let $f:R\to R/(e)\times R/(1-e)$ be the natural quotient maps, i.e. $r\mapsto(r+(e),r+(1-e))$. This is surjective since, for all $a,b\in R$, we have $f(a(1-e)+be)=(a,b)$.

   Note that $\ker(f)=(e)\cap(1-e)=\emptyset$ since, if $r\in(e)\cap(1-e)$, then $r=ae=b(1-e)$ implies $r=ae=ae^2=b(1-e)e=0$. Hence f is injective and so an isomorphism.

   This is a special case of the Chinese remainder theorem for rings.

   (iii) By part (ii) we have $R\cong R/(e)\times R/(1-e)$. If $R/(1-e)$ decomposes as $S\times S'$, then we have $R\cong R/(e)\times S\times S'$. Under this isomorphism e maps to $(0,1,1)$. Let e' be the element of R mapping to $(0,1,0)$. Then $ee'=e'$ so e is not primitive.

   (iv) If $e=e_1+e_2$ with $e_1e_2=0$, then $ee_1=(e_1+e_2)e_1=e_1$, so e is not primitive. Conversely, if e is not primitive, let e' be such that ee' is not equal to zero or e. Then ee' is idempotent, as is $e-ee'$, and $ee'(e-ee')=0$.

(v) Since there are only finitely many idempotents, there exists a primitive idempotent e; then by (ii) and (iii), $R = R_1 \times S$ with R_1 indecomposible. Since for every idempotent e of S, $(0, e)$ and $(1, e)$ correspond to idempotents of R, the number of idempotents of S is half the number of idempotents or R. Proceeding inductively, we find that $R \cong R_1 \times R_2 \times \cdots \times R_d$ with each R_i indecomposable, and R has 2^d idempotents. Under this isomorphism the primitive idempotents of R are e_i, where e_i maps to 1 in R_i and 0 in R_j for $i \neq j$.

10. For each integer $n \geq 1$, show that there exists an ideal in $\mathbb{Z}[X]$ which is generated by $n+1$ elements but not by n elements.

Solution: For $n = 1$, we can take $I_1 = (2, X)$. This consists of polynomials with constant term divisible by 2 and the rest arbitrary. Such an ideal is too complicated to be generated by a single element. We want to generalise this idea somehow. After some thought, we might come up with $I_2 = (4, 2X, X^2)$ for the next case. More generally, let $I_n = (2^n, 2^{n-1}X, 2^{n-2}X^2, \cdots, 2X^{n-1}, X^n)$. This is generated by $n+1$ elements and we claim that it is not generated by n elements. Note that $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$.

Note that, for $I_{n+1} \subseteq I_n$, the quotient I_n/I_{n+1} is an ideal in $\mathbb{Z}[X]/I_{n+1}$ and in particular an abelian group. If I_n is generated by n elements, then the abelian group I_n/I_{n+1} must also be generated by n elements. In the case $n = 1$, we have

$$I_1/I_2 = (2, X)/(4, 2X, X^2) = \{a \cdot 2 + b \cdot X + (4, 2X, X^2) : a, b \in \{0, 1\}\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

The abelian group $(\mathbb{Z}/2\mathbb{Z})^2$ requires two generators and hence so does $(2, X)$ (though we knew this already). More generally, we have that

$$I_n/I_{n+1} = (2^n, 2^{n-1}X, \cdots, X^n)/(2^{n+1}, 2^nX, \cdots, X^{n+1}).$$

The coset representatives are $\{a_0 \cdot 2^n + a_1 \cdot 2^{n-1}X + \cdots + a_n \cdot X^n : a_i \in \{0, 1\}\}$. It is straightforward to see they represent every class. To show they represent distinct classes note that $\sum a_i \cdot 2^{n-i}X^i = \sum b_i \cdot 2^{n-i}X^i$ if and only if $\sum (a_i - b_i) \cdot 2^{n-i}X^i \in I_{n+1}$. By definition, the coefficient in X^i for $i \leq n$ of any polynomial in I_{n+1} is divisible by 2^{n+1-i}. Hence $a_i \equiv b_i \bmod 2$ which implies $a_i = b_i$ since $a_i, b_i \in \{0, 1\}$. Given these coset operations, it follows immediately that $I_n/I_{n+1} \cong (\mathbb{Z}/2\mathbb{Z})^{n+1}$ which is not generated by n elements as an abelian group. Hence I_n is not generated by n elements as an ideal.

$^+$11. Let p be a prime. Is it true that every ideal in $\mathbb{Z}[C_p]$ is a principal if and only if $\mathbb{Z}[\zeta_p]$ is a principal ideal domain? [Here C_p denotes the cyclic group of order p and $\zeta_p = e^{2\pi i/p} \in \mathbb{C}$ denotes the pth roots of unity.]

Solution not provided. You may continue to work on this throughout the term and contact me to discuss ideas and/or hand in a solution. Remember that this problem is optional and may be significantly more challenging than the other problems.