1 Definition of Ring

Example 1.0.1. For an abelian group G, then the group $\mathrm{End}_{\mathsf{Ab}}(G)$ of endomorphisms of G is a ring, under the operations of addition and composition. ⌟

Example 1.0.2. Ring R is called *Boolean* if $a^2 = a$ for all $a \in R$. Boolean ring is commutative and has characteristic 2. The power set ring $\mathscr{P}(S)$ is an example of Boolean ring (exercise III.3.15). ⌟

1.1 Exercises

1. (1.1) We have $a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$ which implies $a \cdot 0 = 0$ for all $a \in R$. Hence, $0 = a \cdot 0 = a \cdot 1 = a$ so $a = 0$ for all $a \in R$. Thus, if $1 = 0$ in R then R is the zero ring.

2. (1.2) (Example of ring) For set S, let $\mathscr{P}(S)$ be a power set of S. Define operations on $\mathscr{P}(S)$:
$$A + B := (A \cup B)\ (A \cap B), A \cdot B := A \cap B$$
Then $(\mathscr{P}(S), +, \cdot)$ is a commutative ring.

3. (1.3) (Example of ring) Let R be a ring, and let S be any set. The following operations endow R^S, set of set-functions $S \to R$, into a ring:
$$(f+g)(a) = f(a) + g(a), (fg)(a) = f(a)g(a).$$

4. (1.4) Since $\mathrm{tr}(A)\mathrm{tr}(B) \neq \mathrm{tr}(AB)$ so $\mathfrak{sl}_n(\mathbb{R})$ and $\mathfrak{sl}_n(\mathbb{R})$ are not rings.
$\mathfrak{so}_n(\mathbb{R})$ is not a ring since $A = \begin{pmatrix} 0 & -a \\ a & 0 \end{pmatrix} \in \mathfrak{so}_n(\mathbb{R})$ but $A^2 = \begin{pmatrix} -a^2 & 0 \\ 0 & -a^2 \end{pmatrix} \notin \mathfrak{so}_n(\mathbb{R})$.

5. (1.5) Let $a = [2]_6, b = [3]_6$ then $ab = 0$ in $\mathbb{Z}/6\mathbb{Z}$ but $a + b = [5]_6$ s not zero-divisor.

6. (1.6) If $a^n = 0, b^m = 0$ then $(a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}$. If $k \le n$ then $m + n - k \ge m$ so $b^{m+n-k} = 0$ for $k \le n$. If $k > n$ then $a^k = 0$. Thus, $(a+b)^{m+n} = 0$.
Note that we need $ab = ba$ for the identity to hold.

7. (1.7) $[m]$ nilpotent in $\mathbb{Z}/n\mathbb{Z}$ iff m^k divisible by n for some $k \in \mathbb{N}$ iff m is divisible by all prime factors of n.

8. (1.8) We have $x^1 = 1 \implies (x-1)(x+1) = 0$ by distributive property. If integral domain then this implies either $x = 1$ or $x = -1$, exactly 2 solutions. If in nonintegral domain such as $\mathbb{Z}/8\mathbb{Z}$ then $x = [1]_8, [3]_8, [7]_8$.

9. (1.9) Not hard.

10. (1.10) If right-unit a has two left-inverses $b_1 \neq b_2$ then a is not left-zero-divisor since if $ax = 0$ implies $x = (b_1 a)x = b_1(ax) = 0$. a is right-zero-divisor since $(b_1 - b_2)a = 0$ and $b_1 - b_2 \neq 0$.

11. (1.11) $(1,0) \cdot (0,1) = (1,1), (0,1)^2 = (1,0)$ and $(1,0)^2 = (0,1)$.

12. (1.12) A division ring shoe elements of the form $a + bi + cj + dk$.

13. (1.13) Not hard.

14. (1.14) Let the leading coefficient of f, g be a, b with $a, b \neq 0$ then the leading coefficient of fg is $ab \neq 0$ since R is an integral domain.

15. (1.15) Since R is isomorphic to a subring of $R[x]$ so if R is not integral domain then so is $R[x]$. Conversely, if R integral domain, we show that every polynomial of degree at least 1 is not a zero-divisor. Indeed, we proceed by induction on $\deg f = n$. Let $f(x) = h(x) + ax^n$ with $\deg h < n$ then if $fg = 0$ we can obtain $a = 0$ to get back to inductive hypothesis.

16. (1.16) (Ring of power series)

    (i) If $a_0 + a_1 x + \cdots$ is unit in $R[[x]]$ then there exists $b_0 + b_1 x + \cdots$ such that $(a_0 + a_1 x + \cdots)(b_0 + b_1 x + \cdots) = 1$. This follows $a_0 b_0 = 1$ or a_0 is a unit. We also have $\sum_{i+j=k} a_i b_j = 0$ so $b_k = \frac{1}{a_0} \sum_{i=1}^{k} (-a_i b_{k-i})$. This proves the claim. In pariticular, inverse of $1 - x$ is $1 + x + \cdots$

    (ii) As R is a subring of $R[[x]]$ so if R not an integral domain then so is $R[[x]]$. If R is a integral domain, consider $(a_0 + a_1 x + \cdots)(b_0 + b_1 x + \cdots) = 0$ then $a_0 b_0 = 0$. As R is integral domain, either $a_0 = 0$ or $b_0 = 0$. However, WLOG, if $a_0 \neq 0$ then $f(x) = a_0 + a_1 x + \cdots$ is a unit according to 1, which implies $b_0 + b_1 x + \cdots = 0$, as desired. Thus, if $a_0 = b_0 = 0$, similarly, we can proceed to obtain $a_i = b_i = 0$ (or else one of f, g must be 0). This proves that $R[[x]]$ is an integral domain.

17. (1.17) A polynomial $f(x) = \sum a_i x^i$ can be viewed as element $\sum a_i \cdot i$ of monoid ring $R[\mathbb{N}]$.

2 The category Ring

Examples of ring homomorphisms

Example 2.0.1. Let R be a ring. $\text{End}_{\mathsf{Ab}}(R)$ is a ring of endomorphisms of R underlying the group $(R,+)$. For $r \in R$, defined left- and right-multiplication by r by λ_r, μ_r, respectively. That is, $\forall a \in R$

$$\lambda_r(a) = ra, \mu_r(a) = ar$$

Then the function $r \mapsto \lambda_r$ is an injective ring homomorphism $\lambda : R \to \text{End}_{\mathsf{Ab}}(R)$. Similarly, the map $r \mapsto \mu_r$ is also an injective ring homomorphism. ⌟

Example 2.0.2. The inclusion map $\iota : \mathbb{Z} \to \mathbb{Q}$ is a ring homomorphism. [Exercise III.2.12] ⌟

2.1 Exercises

1. (2.1) Since every ring homomorphism sends 0 to 0 so we are done.

2. (2.2) If φ surjective then exists $a \in R$ such that $\varphi(a) = 1_S$. This follows $\varphi(1_R) = \varphi(1_R)\varphi(a) = \varphi(a)$ so $\varphi(1_R) = 1_S$.

   If $\varphi \neq 0$ and S an integral domain, there exists $b \in R, c \in S, c \neq 0$ such that $\varphi(b) = c$. This follows $c = \varphi(b) = \varphi(1_R)\varphi(b) = \varphi(1_R)c$ which implies $(1_S - \varphi(1_R))c = 0$. Since S integral domain and $c \neq 0$ so this follows $\varphi(1_R) = 1_S$.

3. (2.3) The ring $\mathscr{P}(S)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^S$ by the map $\varphi : \mathscr{P}(S) \to (\mathbb{Z}/2\mathbb{Z})^S$ defined as $A \mapsto f_A$ where $A \subseteq S$ and $f_A(x) = 1$ if $x \in A$ and $f_A(x) = 0$ otherwise.

4. (2.4) There are injective ring homomorphism $\mathbb{H} \to \mathfrak{gl}_4(\mathbb{R})$ and $\mathbb{H} \to \mathfrak{gl}_2(\mathbb{C})$:

$$a + bi + cj + dk \mapsto \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}, a + bi + cj + dk \mapsto \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}.$$

5. (2.5) The function from the multiplicative group $\mathbb{H}^*$ of nonzero quartenions to the multiplicative group $\mathbb{R}^+$ of positive real numbers, defined by assinging to each nonzero quartenion its norm, is a group homomorphism. The kernel of this homomorphism is isomorphic to $\text{SU}_2(\mathbb{C})$.' Kernel of φ consists of $a + bi + cj + dk \in \mathbb{H}^*$ such that $a^2 + b^2 + c^2 + d^2 = 1$. From exercise II.6.3, $\text{SU}_2(\mathbb{C})$ are $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$ such that $a^2 + b^2 + c^2 + d^2 = 1$. This suggests obvious isomorphism from $\ker\varphi$ to $\text{SU}_2(\mathbb{C})$.

6. (2.6) A map $\overline{\varphi} : R[x] \to S$ extending $\varphi : R \to S$ and sending $x \in R[x]$ to s while preserving mutiplication and addition is unique since

$$\overline{\varphi}\left(\sum_{i=1}^{n} a_i x^i\right) = \sum_{i=1}^{n} \varphi(a_i) s^i.$$

   The map is a ring homomorphism since φ is a ring homomorphism and s commutes with $\varphi(r)$ for all $r \in R$, which explains

$$\overline{\varphi}\left(\sum a_i x^i\right)\left(\sum b_j x^j\right) = \overline{\varphi}\left(\sum a_i x^i\right)\overline{\varphi}\left(\sum b_j x^j\right).$$

7. (2.7) Distinguish between concepts of 'polynomial' and 'polynomial function' well distinct.

8. (2.8) Obvious.

9. (2.9) The *center* of a ring R is a subring of R. Center of a division ring is a field.

10. (2.10) The *centralizer* of $a \in R$ consists of elements $r \in R$ such that $ar = ra$.

    Centralizer of a is a subring of R, for every $a \in R$. Indeed, denote such set as Z_a. We have $1_R \in Z_a$. If $a, b \in Z_a$ then $(a-b)r = ar - br = ra - rb = r(a-b)$ so Z_a is a subgroup of Z. Furthermore, $(ab)r = a(rb) = (ra)b = r(ab)$ so Z_a subring of R.

    Center of R is the intersection of all its centrelizers. This is not hard.

    Every centralizer in a division ring is a division ring. Indeed, for $r \in Z_a$ then $ar = ra \implies rar^{-1} = a \implies ar^{-1} = r^{-1}a$ so $r^{-1} \in Z_a$. Thus, Z_a is a division ring.

11. (2.11) Division ring R of p^2 elements, where p prime, is commutative. Indeed, if R is not commutative, then its center C (exercise 2.9) is a *proper* subring of R, which means C is a proper subgroup of R so $|C| = p$.

    Let $r \in R, r \notin C$ then centerlizer Z_r of r (exercise 2.10) contains both r and C. This follows $|Z_r| > p$. However, Z_r is also a subgroup of R so $|Z_r|$ divides p^2. Hence, $|Z_r| = p^2$ or $Z_r = R$. As this is true for all $r \notin C$, we can easily show that every $r \notin C$ commutes in R, which means $r \in C$, a contradiction. Thus, R must be commute.

12. (2.12) Given homomorphism $\varphi : R \to S$ then cokerφ is an initial object in the category of homomorphism $\alpha : S \to T$ such that $\alpha \circ \varphi = 0$.

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[rr, bend left, "0"] & S \arrow[r, "\alpha"] \arrow[d, two heads] & T \\
 & \operatorname{coker}\varphi \arrow[ur, "\exists!\overline{\alpha}"'] &
\end{tikzcd}$$

    In category Ab there R, S, T are abelian group then coker$\varphi \cong S/\mathrm{im}\varphi$. In category Ring, as every ring is also abelian group under $+$ and ring homomorphism also group homomorphism, cokerφ is also $S/\mathrm{im}\varphi$ with multiplication defined $(s_1 + \mathrm{im}\varphi)(s_2 + \mathrm{im}\varphi) = s_1 s_2 + \mathrm{im}\varphi$.

    For $\varphi = \iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ then coker$\iota = \mathbb{Q}/\mathbb{Z}$.

13. (2.13) Not hard. The componentwise product $R_1 \times R_2$ of two rings satisfies the universal property for products in category Ring.

14. (2.14) Let's first draw out the diagram for coproduct:

$$\begin{tikzcd}
\mathbb{Z}[x] \arrow[dr, "\pi_1"] \arrow[drr, bend left, "f_1"] & & \\
 & \mathbb{Z}[x_1, x_2] \arrow[r, "\varphi"] & S \\
\mathbb{Z}[x] \arrow[ur, "\pi_2"'] \arrow[urr, bend right, "f_2"'] & &
\end{tikzcd}$$

Observe that ring homomorphism $f_1 : \mathbb{Z}[x] \to S$ is completely determined by $f_1(x)$. Similarly, $f_2 : \mathbb{Z}[x] \to S$ is determined by $f_2(x)$ and $\varphi : \mathbb{Z}[x_1, x_2] \to S$ determined by $\varphi(x_1)$ and $\varphi(x_2)$. Hence, this suggests $\varphi(x_1) = f_1(x)$ and $\varphi(x_2) = f_2(x)$. Since we are in the the category of commutative ring so this definition makes φ into a ring homomorphism (as one can commute $\varphi(x_1)$ and $\varphi(x_2)$ to satisfy the product property of ring).

The diagram also suggests that $\pi_1 : \mathbb{Z}[x] \to \mathbb{Z}[x_1, x_2]$ by $x \mapsto x_1$ and π_2 defined similarly. With π_1, π_2 defined as this, the uniqueness of φ is obtained from the commutativity of the diagram.

15. (2.15) There exists many different ways to give a structure of ring without identity to the group $(\mathbb{Z}, +)$:

    One views $(m\mathbb{Z}, +, \cdot)$ as "ring without identity" then $\cdot$ means multiplication in $\mathbb{Z}$, i.e. $(mn_1)(mn_2) = m(mn_1n_2)$.

    Note $\varphi : \mathbb{Z} \to m\mathbb{Z}$ as $n \mapsto mn$ is a group isomorphism. One can use this to transfer the structure of 'ring without identity' $(m\mathbb{Z}, +, \cdot)$ back onto $\mathbb{Z}$: $\varphi^{-1}(mn_1 \cdot mn_2) = \varphi^{-1}(mn_1) \bullet \varphi^{-1}(mn_2)$ so $mn_1n_2 = n_1 \bullet n_2$. This induces multiplication $\bullet$ in $\mathbb{Z}$ as $a \bullet b = mab$. With this, $(\mathbb{Z}, +, \bullet)$ is a ring without identity.

    For different m, the structures of $\mathbb{Z}$ are nonisomorphic as 'rings without 1'. Indeed, if we have a ring homomorphism $\varphi : (\mathbb{Z}, +, \bullet_m) \to (\mathbb{Z}, +\bullet_n)$ then by addition property of ring, we have $\varphi(x) = x\varphi(1)$. On the other, by using multiplication, we have $\varphi(1 \bullet_m 1) = \varphi(1) \bullet_n \varphi(1)$ so $m\varphi(1) = n\varphi(1)^2$. If φ is bijective then $\varphi(1) \neq 0$ so $m = n\varphi(1)$. Since $m, n > 1$ so if $\varphi(1) \neq 1$ then φ is not surjective, i.e. for any $x \in \mathbb{Z}, \gcd(x, \varphi(1)) = 1$ then there does not exist $\varphi(y) = x$. Thus, $(\mathbb{Z}, +, \bullet_m)$ not isomorphic to $(\mathbb{Z}, +, \bullet_n)$ for different m, n.

16. (2.16) There exists (up to isomorphism) only one structure of ring with identity on the group $(\mathbb{Z}, +)$:

    Let R be a ring whose underlying group is $\mathbb{Z}$. By proposition 2.7, there is injective ring homomorphism $\lambda : R \to \mathrm{End}_{\mathsf{Ab}}(R)$ mapping $r \in R$ to left-multiplication $\lambda_r : R \to R$ by r.

    Proposition 2.6, we know that $\mathrm{End}_{\mathsf{Ab}}(R) \cong \mathbb{Z}$ as rings. Hence, it suffices to show λ is surjective: For any $\varphi \in \mathrm{End}_{\mathsf{Ab}}(R)$, if $\varphi(1) = r$ then $\varphi(n) = \varphi(1)n = rn$ so $\varphi = \lambda_r = \lambda(r)$. Thus, λ is indeed surjective and therefore, $R \cong \mathbb{Z}$ as rings.

17. (2.17) Let R be a ring, and $E = \mathrm{End}_{Ab}(R)$ be ring of Endomorphisms of underlying abelian group $(R, +)$. Prove center of E isomorphic to a subring of center of R.

    Denote Z_R, Z_E centers of R, E, respectively. From proposition 2.7, there exists injective ring homomorphism $\lambda : R \to E$ defined as $r \mapsto \lambda_r$ where $\lambda_r : R \to R$ is left-multiplication by r. Since λ is injective so λ^{-1} (restricting to image of λ) is a well-defined ring homomorphism. Hence, it suffices to show $\lambda^{-1}(Z_E) \subseteq Z_R$.

    For $\alpha \in Z_E$ then α commutes with right-multiplication $\mu_r \in E$ by r. We have $(\alpha \circ \mu_r)(x) = (\mu_r \circ \alpha)(x)$ for every $r, x \in R$. This follows $\alpha(xr) = \alpha(x)r$ and by letting $x = 1$ then $\alpha(r) = \alpha(1)r$ so α is essentially left-multiplication by $\alpha(1)$. Hence, $\lambda^{-1}(\alpha) = \alpha(1)$. Thus, $\lambda^{-1}(Z_E) \subseteq Z_R$.

18. (2.18) Not hard.

19. (2.19) For positive integer n then $\mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ as rings. Us exrcise 2.7, it suffices to show $\lambda : \mathbb{Z}/n\mathbb{Z} \to \mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n\mathbb{Z})$ is surjective. For $\varphi \in \mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n\mathbb{Z})$ then $\varphi(\overline{a}) = \varphi(1)\overline{a}$ so $\varphi = \lambda_{\varphi(1)}$. Thus, λ is indeed surjective.

3 Ideals and quotient rings

Example 3.0.1. If J is two sided ideal of $\mathcal{M}_n(R)$, a ring of $n \times n$ matrices over ring R. Then

1. (Exercise III.3.5) A matrix $A \in \mathcal{M}_n(R)$ belongs to J if and only if the matrices obtained by placing any entry of A in any position, and 0 elsewhere, belong to J.
2. If I set of $(1,1)$-entries of matrices in J. Then I is two-sided ideal of R and J consists of those matrices whose entries all in I.

One can use these two properties to show that $\mathcal{M}_n(\mathbb{F})$ is simple (exercise III.3.9). ⌟

Example 3.0.2. Let S be a set and $T \subseteq S$. Subsets of S contained in T form an ideal $\mathscr{P}(T)$ of the power set ring $\mathscr{P}(S)$.

If S finite, then every ideal of $\mathscr{P}(S)$ is of this form. This is not true for the case S is infinite (exercise III.3.16). ⌟

Example 3.0.3. Let R be a commutative ring. Then set of nilpotent elements of R is ideal of R. The ideal N is called *nilradical* of R. This is not true if R is noncommutative (exercise III.3.12).

Then R/N contains no nozero nilpotent elements (such ring is said to be *reduced*). ⌟

3.1 Exercises

1. (3.1) im φ is a subring of S since $1_S \in \text{im } \varphi$ and for $\varphi(a), \varphi(b) \in \text{im } \varphi$ then $\varphi(a) - \varphi(b) = \varphi(a-b) \in \text{im } \varphi$ and $\varphi(a)\varphi(b) = \varphi(ab) \in \text{im } \varphi$.

   If im φ is ideal of S but $1_S \in \text{im } \varphi$ so $S = \text{im } \varphi$ so φ is surjective.

   If $\ker \varphi$ is subring of R then $1_R \in \ker \varphi$ and since $\ker \varphi$ is ideal of R so $R = \ker \varphi$ or $\varphi = 0$.

2. (3.2) For ring homomorphism $\varphi : R \to S$ and ideal J of S then $I = \varphi^{-1}(J)$ is an ideal of R. Indeed, for $r \in R$ then $\varphi(rI) = \varphi(r)\varphi(I) = \varphi(r)J \subseteq J$ since J ideal of S. This follows $rI \subseteq \varphi^{-1}(J) = I$. Similarly, $Ir \subseteq I$. Thus, I ideal of R.

3. (3.3) For ring homomorphism $\varphi : R \to S$ and ideal J of R.

   $\varphi(J)$ need not be ideal of S. Indeed, consider the inclusion $\iota : \mathbb{Z} \to \mathbb{Q}$ then $\iota(n\mathbb{Z}) = n\mathbb{Z}$ is not ideal in $\mathbb{Q}$.

   However, if φ is surjective then $\varphi(J)$ is ideal of S. Indeed, for any $s \in S$, there exists $r \in R$ such that $\varphi(r) = s$. This follows $s\varphi(J) = \varphi(rJ) \subseteq \varphi(J)$ as $rJ \subseteq J$. Similarly, $\varphi(J)s \subseteq \varphi(J)$.

   For surjective φ, $I = \ker \varphi$ then we can identify S with R/I through the isomorphism $r + I \mapsto \varphi(r)$. Let $\varphi(J)$ can be identified as an ideal $\overline{J}$ of R/I by previous argument. In fact, $\overline{J} = (I+J)/I$. Therefore,
   $$\frac{R/I}{\overline{J}} \cong \frac{R/I}{(J+I)/J} \cong \frac{R}{I+J}$$
   by Third Isomorphism theorem.

4. (3.4) Consider unique ring homomorphism $\varphi : \mathbb{Z} \to R$ defined as $a \mapsto a \cdot 1_R$ then im φ is a subgroup of R so it is an ideal of R. From exercise III.3.1, φ is surjective and therefore $R = \text{im } \varphi \cong \mathbb{Z}/\ker \varphi = \mathbb{Z}/n\mathbb{Z}$ where n charactieristic of R.

5. (3.5) Let $E_{a,b}$ be $n \times n$ matrix that has 1 at (a,b)-entry and 0 everywhere else. Then $n \times n$ matrix A then (m,n)-th entry of $E_{m,a}AE_{b,n}$ is (a,b)-th entry of A and 0 everywhere else.

   Hence, if A in a two-sided ideal J of $\mathcal{M}_n(R)$ then $E_{m,a}AE_{b,n} \in J$, as desired.

6. (3.6) J two-sided ideal of ring $\mathcal{M}_n(R)$ and $I \in R$ set of all $(1,1)$-entries of matrices in J then I is two-sided ideal of R. From previous exericse III.3.5, if x is $(1,1)$-entry of some matrix in J then $\begin{pmatrix} y & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \in J$. For any $y \in R$ then $\begin{pmatrix} x & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} y & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} xy & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \in J$ so therefore, $xy \in I$ for any $x \in I, y \in R$. Similarly, $yx \in I$ for any $x \in I, y \in R$. Furthermore, I is obviously a subgroup of R so therefore, I is a two-sided ideal of R.

   Next, we show J consists precisely of matrices whose entries all belong to I. For matrix $A = (a_{i,j}) \in J$ then from previous exercise III.3.5, $\begin{pmatrix} a_{i,j} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \in J$ and therefore, $a_{i,j} \in I$. This follows every entry of A is in I for every $A \in J$.

   Conversely, consider a matrix $A = (a_{i,j})$ whose entries are in I, we want to show that $A \in J$. Indeed, from previous exercise III.3.5, A can be written as $A = \sum_{i,j} E_{i,1}(a_{i,j}E_{1,1})E_{1,j}$ where $a_{i,j}E_{1,1} \in J$ by exercise III.3.5. Therefore, as J is two-sided ideal of $\mathcal{M}_n(R)$ so indeed, $A \in J$.

7. (3.7) Ra left-ideal of R and aR is right-ideal of R. Also, a is left-, resp. right-, unit if and only if $R = aR$.

8. (3.8) A ring R is a division ring if and only if its only left-ideals and right-ideals are $\{0\}$ and R. Indeed, if R is division ring and has left-ideal I. Then either $I = \{0\}$ or there exists $a \neq 0, a \in I$ which then implies $1 = a^{-1}a \in I$ and hence, $I = R$. The argument is similar with right-ideal of R.

   Conversely, if the only left- and right- ideals of R are $\{0\}$ and R, then from exercise III.3.7, as Ra left-ideal of R then either $Ra = \{0\}$, which means $a = 0$, or $Ra = R$, which means a has left-unit. Similarly, either $a = 0$ or a has right-unit. This follows R is a division ring.

9. (3.9) A nonzero ring such that its only two-sided ideals are $\{0\}$ and R is called *simple*. And $\mathcal{M}_n(R)$ is simple.

   Indeed, if J two-sided ideal of $\mathcal{M}_n(\mathbb{R})$ then let $I \subseteq \mathbb{R}$ set of $(1,1)$-entries of matrices in T. From exercise III.3.6, if $I = \{0\}$ then $J = \{O_{n\times n}\}$. On the other hand, if $a \in I, a \neq 0$ then since I is a two-sided ideal of a field $\mathbb{R}$, we find $I = \mathbb{R}$. This implies $J = \mathcal{M}_n(\mathbb{R})$.

   Thus, the only two-sided ideals of $\mathcal{M}_n(\mathbb{R})$ can be only $\{0_{n\times n}\}$ or $\mathcal{M}_n(\mathbb{R})$. This is also true for ring of $n \times n$ matrices over any field k.

10. (3.10) Let $\varphi : k \to R$ is a ring homomorphism where k is a field and R is a nonzero ring. Then φ is injective.

    Indeed, if $u \in \ker\varphi, u \neq 0$ then as $\ker\varphi$ is ideal of k, we obtain $1 \in \ker\varphi$ and hence, $\ker\varphi = R$, which is not ring homomorphism since $\varphi(1_k) \neq 1_R$. Hence, $\ker\varphi = \{0_k\}$ and so φ is injective.

11. (3.11) Let R be a ring containing $\mathbb{C}$ as subring. Then there are no ring homomorphism $R \to \mathbb{R}$. Indeed, it suffices to show there is no ring homomorphism from $\mathbb{C}$ to $\mathbb{R}$. Indeed, if there is such ring homomorphism $\varphi : \mathbb{C} \to \mathbb{R}$. then $\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -\varphi(1) = -1$ so $\varphi(i)^2 = -1$, a contradiction since $\varphi(i) \in \mathbb{R}$.

12. (3.12) Let R be a commutative ring. Then set of nilpotent elements of R is ideal of R. The ideal is called *nilradical* of R. Let such set be $I(R)$. If $a, b \in I(R)$. then $a^n = 0, b^m = 0$ for some positive integer m, n. Hence, due to commutativity of R, we have

$$(a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k} = 0$$

Hence, $I(R)$ is an abelian group. Furthermore, for $r \in R, a \in I(R)$ such that $a^n = 0$ then $(ra)^n = r^n a^n = 0$ so $ra \in I(R)$. Thus, $I(R)$ is an ideal of R.

The case is not true when R is noncommutative, i.e. there exists noncommutative ring with set of nilpotent elements not forming an ideal: $\mathcal{M}_3(\mathbb{R})$ has two nilpotents

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 1 & -1 \end{pmatrix}$$

while $(A+B)^3 = -(A+B)$ so $A+B$ is not nilpotent.

13. (3.13) Let R commutative ring, N be its nilradical then R/N contains nonzero nilpotent elements (called *reduced*). Indeed, if R/N has nilpotent element $r+N$ then $(r+N)^n = 0$ or $r^n + N = 0$ or r^n nilpotent or r nilpotent or $r + N = N$. Hence, every nonzero element in R/N is not nilpotent.

14. (3.14) Let R be an integral domain with characteristic n then either $n = 0$ or n is a prime. If R has nonzero characteristic n and n is composite number, there exist $a, b \geq 2$ such that $n = ab$. This follows $0 = n \cdot 1_R = (a \cdot 1_R)(b \cdot 1_R)$. As R is integral domain so either $a \cdot 1_R = 0$ or $b \cdot 1_R = 0$. This leads to a contradiction due to definition of characteristic of R.

15. (3.15) Ring R is called *Boolean* if $a^2 = a$ for all $a \in R$. Then $\mathscr{P}(S)$ is Boolean, for every set S. Indeed, $A^2 = A \cap A = A$ for every $A \in \mathscr{P}(S)$.

    Boolean ring R is commutative and has characteric 2. Indeed, we have $(a+a)^2 = a + a$ implies $4a = 2a$ as $a^2 = a$ so $2a = 0$. Thus, R is characteristic 2. On the other hand, we have $(a+b)^2 = a + b$ implies $ab + ba = 0$ as $a^2 = a, b^2 = a$. However, as $2ab = 0$ so $ab = ba$, so R is commutative.

    If an integral domain R is Boolean then $R \cong \mathbb{Z}/2\mathbb{Z}$. Indeed, $a^2 = a$ implies $a(a-1) = 0$ so $a = 1$ or $a = 0$ as R is integral domain. Therefore, $R = \{0, 1\} \cong \mathbb{Z}/2\mathbb{Z}$.

16. (3.16) (i) Let S be a set and $T \subseteq S$. Prove that subsets of S contained in T form an ideal of the power set ring $\mathscr{P}(S)$. Indeed, denote such set to be $\mathscr{P}(T)$ then for $A, B \subseteq T$ then $A + B = (A \cup B) \setminus (A \cap B) \subseteq T$ and $A + A = \emptyset \subseteq T$. Hence, $\mathscr{P}(T)$ is a subgroup of $(\mathscr{P}(S), +)$.

    For $C \subseteq S$ and $A \in \mathscr{P}(T)$ then $CA = C \cap A \subseteq A \subseteq T$ so $CA \in S(T)$. Similarly, $AC \in \mathscr{P}(T)$. Thus, $\mathscr{P}(T)$ is an ideal of $\mathscr{P}(S)$.

    (ii) If S finite, then every ideal of $\mathscr{P}(S)$ is of the form in (i). Let $\mathcal{J}$ be an ideal of $\mathscr{P}(S)$ then there exists $T \in \mathcal{J}$ with maximal number of elements comparing to other sets in $\mathcal{J}$.

    We show that $\mathscr{P}(T) = \mathcal{J}$. Indeed, for any $K \subseteq T$, since $T \in \mathcal{J}$ so $KT \in \mathcal{J}$ or $K = K \cap T = KT \in \mathcal{J}$. Hence, any subset of T is in $\mathcal{J}$. This follows $\mathscr{P}(T) \subseteq \mathcal{J}$.

    Next, we show $\mathcal{J} \subseteq \mathscr{P}(T)$. Indeed, if there exists $T' \in \mathcal{J}$ such that $T' \notin \mathscr{P}(T)$. Then note that $(T' + T) \cap (TT') = \emptyset$ so $(T' + T) + TT' = T \cup T'$. As $T, T' \in \mathcal{J}$ so $T \cup T' = T' + T + TT' \in \mathcal{J}$. But $|T \cup T'| > |T|$, a contradiction to maximality of $|T|$ in $\mathcal{J}$. Thus, every set in $\mathcal{J}$ must be subset of T, as desired.

    (iii) For infinite S, there exists ideal of $\mathscr{S}$ that is not of the form in (i). Let T be an infinite subset of S then an ideal $\mathcal{I}$ of $\mathscr{P}(S)$ is the set of all finite subsets of T.

    Indeed, if $\mathcal{I}$ is obviously a subgroup of $\mathscr{P}(S)$. For $S' \subseteq S, I' \in \mathcal{I}$ then $S'I' = I' \cap S' \subseteq I'$ so $S'I' \in \mathcal{I}$. Thus, $\mathcal{I}$ is indeed an ideal of $\mathscr{P}(S)$ and $\mathcal{I}$ is not of the form in (i).

17. (3.17) $J/(I \cap J) \cong (I + J)/I$ by mapping $J \to R/I$ where $j \mapsto j + I$.

4 Ideals and quotients: Remarks and examples, Primes and maximal ideals

Definition 4.0.1. A commutative ring R is *Noetherian* if every ideal of R is finitely generated.

Definition 4.0.2. An integral domain R is a *Principal Ideal Domain* (PID) if every ideal of R is principal.

4.1 Exercises

1. (4.1) For family of ideals $\{I_\alpha\}_{\alpha\in A}$ of ring R then

   $$\sum_{\alpha\in A} I_\alpha = \left\{ \sum_{\alpha\in A} : r_\alpha \in I_\alpha \text{and } r_\alpha = 0 \text{ for all fbut finitely many } \alpha \right\}$$

   is the smallest ideal containing all of ideals I_α. Indeed, we have

   $$r\left(\sum_{\alpha\in A} r_\alpha\right) = \sum_{\alpha\in A} r r_\alpha \in \sum_{\alpha\in A} I_\alpha.$$

   and hence, $\sum_{\alpha\in A} I_\alpha$ is indeed an ideal of R. It is obviously the smallest ideal satisfying the condition.

2. (4.2) Homomorphic image of a Noetherian ring is Noetherian. Indeed, if $\varphi : R \to S$ is surjective ring homomorphism and R is Noetherian, we show that S is Noetherian.

   Indeed, for ideal of I of S then $\varphi^{-1}(I)$ ideal of R (exercise III.3.2). Since R Noetherian so the ideal $\varphi^{-1}(I)$ of R is finitely generated, i.e. $\varphi^{-1}(I) = (a_1, \dots, a_n)$ for $a_i \in R$. This follows $\varphi(a_i) \in I$ for all $1 \le i \le n$ and hence $(\varphi(a_1), \dots, \varphi(a_n)) \subseteq I$.

   For every $i \in I$ then there exists $r \in \varphi^{-1}(I)$ such that $i = \varphi(r) = \varphi(r_1a_1 + \ldots + r_na_n) = \sum_{j=1}^n \varphi(r_j)\varphi(a_j) \in (\varphi(a_1), \dots, \varphi(a_n))$.

   Thus, I is finitely generated and therfore, S is indeed Noetherian.

3. (4.3) Ideal of $(2, x)$ of $\mathbb{Z}[x]$ is not principal. Indeed, suppose if $(2, x)$ is generated by $h(x) \in \mathbb{Z}[x]$. Then $h(x)$ divides 2 and x, which implies $h(x)$ does not exist.

4. (4.4) If k is field then $k[x]$ is a PID.

   Let $I \subseteq k[x]$ be an ideal of $k[x]$. If I is nonzero then there exists a nonzero monic polynomial $f(x)$ (possible since k is a field) with minimal degree in I. For any $g(x) \in I$, there exists $q(x), r(x) \in k[x]$ such that $g(x) = f(x)q(x) + r(x)$ with $0 \le \deg r < \deg f$. Since $g, f \in I$ so $r(x) \in I$ but as $0 \le \deg r < \deg f$ so $r(x) = 0$ or $g(x) = f(x)q(x)$. This implies $I = (f(x))$ or I is finitely generated, as desired.

5. (4.5) For ideals I, J in commutative ring R such that $I + J = (1)$ then $IJ = I \cap J$.

   For any ideals I, J of R then $IJ \subseteq I \cap J$ since any $i \in I, j \in J$ then $ij \in I \cap J$, which means the ideal IJ generated by ij is also in $I \cap J$.

   We use the condition $I + J = (1)$ to show $I \cap J \subseteq IJ$. There exists, $i \in I, j \in J$ such that $i + j = 1$. Hence, for any $\ell \in I \cap J$ then $\ell = \ell \cdot 1 = i\ell + \ell j \in IJ$. Therefore, $I \cap J \subseteq IJ$, as desired.

6. (4.6) For ideals I, J in commutative ring, if $R/(IJ)$ is reduced then $IJ = I \cap J$. We know that $IJ \subseteq I \cap J$ so it suffices to show $I \cap J \subseteq IJ$. Indeed, for $\ell \in I \cap J$ then $\ell^2 \in IJ$ so $(\ell + IJ)^2 = IJ$. However, since $R/(IJ)$ is reduced so $\ell \in IJ$. Thus, $I \cap I \subseteq IJ$, desired.

7. (4.7) For a field k then every nonzero ideal in $k[x]$ is generated by a unique monic polynomial. Indeed, from exercise III.4.4, for any nonzero ideal I of $k[x]$, there exists at least one monic polynomial (with minimal degree in I) that generates I. Hence, it suffices to prove uniqueness. If f_1, f_2 be two monic polynomials of minimal degree in I that generates I then $f_1 - f_2 \in I$ but $\deg(f_1 - f_2) < \deg f_1$ so this happens only when $f_1 = f_2$, as desired.

8. (4.8) For ring R and $f(x) \in R[x]$ a monic polynomial then $f(x)$ is not a (left- or right-) zero-divisor. Indeed, if $f(x)g(x) = 0$ then the leading coefficient of fg is the leading coefficient of g (as f is monic) and hence, $g = 0$. Thus, f is not a left-zero-divisor.

9. (4.9) (Generalise exercise III.4.8) For commutative ring R and f zero-divisor in $R[x]$ then there exists $b \in R, b \neq 0$ such that $f(x)b = 0$.

   Let $f(x) = \sum_{i=0}^n a_i x^i$ be zero-divisor of $R[x]$ then there exists $g(x) = \sum_{i=0}^m b_i x^i \in R[x]$ such that $f(x)g(x) = 0$. Suppose g is of minimal degree, i.e. if $h \in R[x]$ and $fh = 0$ then $\deg g \leq \deg h$.

   We will show that $f(x)b_m = 0$ by inductively showing that $a_k b_m = 0$ on $k \leq n$.

   Note that $[x^{m+n}](fg) = a_n b_m = 0$ so $\deg(a_n \cdot g(x)) < \deg g(x)$. Furthermore, $f(x)(a_n \cdot g(x)) = 0$ so due to minimality of $\deg g$, we obtain $a_n g(x) = 0$.

   Note that if we know $a_{n-i}g(x) = 0$ for all $0 \leq i \leq k-1$ then

   $$0 = [x^{n-k+m}](fg) = \sum_{n \geq i \geq n-k} a_i b_{n-k+m-i} = a_{n-k} b_m$$

   With the same argument as the case $k = 0$, we obtain that $a_{n-k}g(x) = 0$. Indcutively, we obtain $a_i b_m = 0$ for all $0 \leq i \leq n$ so $f(x)b_m = 0$ and $b_m \neq 0, b_m \in R$, as desired.

10. (4.10) $\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{C}$. Furthermore, $\mathbb{Q}(\sqrt{d})$ is a field an in fact the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{d}$.

    Consider the function $\varphi : \mathbb{Q}[t] \to \mathbb{Q}(\sqrt{d})$ defined as $f(t) \mapsto f(\sqrt{d})$ then φ is a ring homomorphism with $\ker \varphi = (x^2 - d)$ so $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[t]/(x^2 - d)$.

11. (4.11) For commutative ring R, $a \in R$ and $f_1(x), \dots, f_r(x) \in R[x]$. Then as $f_i(x) = (x-a)h_i(x) + f_i(a)$ for all $1 \leq i \leq r$ so

    $$(f_1(x), \dots, f_r(x), x - a) = (f_1(a), \dots, f_r(a), x - a).$$

    Define $\varphi : R[x] \to \frac{R}{(f_1(a), \dots, f_r(a))}$ as $f(x) \mapsto f(a) + (f_1(a), \dots, f_r(a))$ then φ is a surjective ring homomorphism. We will calculate $\ker \varphi$. Indeed, if $f(x) \in \ker \varphi$ then $f(a) \in (f_1(a), \dots, f_r(a))$ or $f(a) = \sum_{i=1}^r h_1 f_1(a)$ for $h_i \in R$. This follows $f(x) = (x-a)h(x) + f(a) = (x-a)h(x) + \sum_{i=1}^r h_1 f_1(a)$ so $f(x) \in (x - a, f_1(a), \dots, f_1(a)) = (f_1(x), \dots, f_r(x), x - a)$. Therefore, $\ker \varphi = (f_1(x), \dots, f_r(x), x - a)$. As a result, we obtain

    $$\frac{R[x]}{(f_1(x), f_2(x), \dots, f_r(x), x - a)} \cong \frac{R}{f_1(a), \dots, f_r(a)}.$$

12. (4.12) For commutative ring R and $a_1, \dots, a_n \in R$, define the map $\varphi : R[x_1, \dots, x_n] \to R$ defined as $f(x_1, \dots, x_n) \mapsto f(a_1, \dots, a_n)$. φ is obviously a surjective ring homomorphism. We will go and find $\ker \varphi$. If $f(x_1, \dots, x_n) \in \ker \varphi$ then $f(a_1, \dots, a_n) = 0$. View f as a polynomial over one variable x_1 then there exists $q_1(x_1, \dots, x_n), r_1(0, x_2, \dots, x_n) \in R[x_1, \dots, x_n]$ such that

    $$f_1(x_1, \dots, x_n) = (x_1 - a_1)q_1(x_1, \dots, x_n) + r_1(0, x_2, \dots, x_n).$$

Then $r_1(0, x_2, \ldots, x_n) \in R[x_2, \ldots, x_n]$ and we can repeat the same process to conclude that $f \in (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$. Hence, $\ker \varphi = (x_1 - a_1, \ldots, x_n - a_n)$ and we obtain

$$\frac{R[x_1, \ldots, x_n]}{(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)} \cong R.$$

13. (4.13) If R is an integral domain then from exercise III.4.12, we have $\frac{R[x_1,\ldots,x_n]}{(x_1,\ldots,x_n)}$ is an integral domain so $(x_1, \ldots, x_n)$ is prime ideal of $R[x_1, \ldots, x_n]$.

14. (4.14) Show maximal ideal is prime without using quotient rings. Indeed, if I is maximal ideal of ring R. For any $ab \in I$, suppose $a \notin I$, then $I \subset I + (a)$ but as I is maximal, we must have $I + (a) = R$. Hence, there exists $x \in I, y \in R$ such that $x + ay = 1 \implies b = bx + bay \in I$ (as R is commutative so $ab = ba \in I$ and also $x \in I$). Thus, for any $a, b \in R$ so $ab \in I$ then either $a \in I$ or $b \in I$, which makes I a prime ideal of R.

15. (4.15) For ring homorphism $\varphi : R \to S$ of commutative rings, $I \subseteq S$ an ideal. If I is prime in S then $\varphi^{-1}(I)$ is a prime ideal in R. We know $\varphi^{-1}(I)$ is an ideal of R (exercise III.3.2) so it suffices to show $\varphi^{-1}(I)$ is prime. Indeed, if $a, b \in R$ such that $ab \in \varphi^{-1}(I)$ then $\varphi(ab) \in I$ so as I is primes, either $\varphi(a) \in I$ or $\varphi(b) \in I$. Thus, either $a \in \varphi^{-1}(I)$ or $b \in \varphi^{-1}(I)$, as desired.

5 Modules over a ring

5.1 Submodules and quotients

Definition 5.1.1 (Submodules)**.** A *submodule* N of an R-module M is subgroup preserved by the action of R. That is, for all $r \in R, n \in N$ then rn (defined by the R-module structure of M) is in N. Put otherwise, N is itself an R-module, and the inclusion $N \subseteq M$ is an R-module homomorphism. [1]

Example 5.1.2. We can view R it self as a (left-)R-module. The submodule of R are precisely the (left-)ideas of R.

Indeed, recall [1, Exp III.5.6] that the left-action on N is $\rho(r,s) = rs$ for all $r, s \in R$. Hence, with $n \in N$, submodule N of R must satisfies $\rho(r,n) = rn \in N$ for any $r \in R$, i.e. $rN \subseteq N$. Thus, N is a left-ideal on R. ⌟

Example 5.1.3. Both the kernel and the image of a homomorphism $\varphi : M \to M'$ of R-modules are submodules (of M, M', respectively).

Indeed, if $s \in \ker\varphi$ then $\varphi(rs) = r\varphi(s) = r0_M = 0_M$ so $rs \in \ker\varphi$. If $s = \varphi(t) \in \mathrm{im}\varphi$ then $rs = r\varphi(t) = \varphi(rt) \in \mathrm{im}\varphi$. ⌟

Example 5.1.4. If r is in center of R and M an R-module then $rM = \{rm : m \in M\}$ is a submodule of M. If I is any ideal of R then $IM = \{\sum_i r_i m_i : r_i \in I, m_i \in M\}$ is a submodule of M.

Indeed, the first part is obvious since for any $r' \in R$ we have $r'(rm) = (r'r)m = (rr')m = r(r'm) \in rM$. For the second part, we have $r\left(\sum_i r_i m_i\right) = \sum_i r(r_i m_i) = \sum_i (rr_i m_i) \in IM$ since $rr_i \in I$. ⌟

Remark 5.1.5 (Turn M/N into an R-module)**.** As mentioned in [1, §III.5.3], one can define an action of R on M/N by $r(m+N) := rm + N$ to turn M/N into a R-module. Note that we need N to be submodule of M (instead of just an abelian group) in order for the above action to make sense, i.e. $r(N) = N$.

[1]

Why these two definitions are equivalent. Let ρ_n, ρ_m be left-action on N, M, respectively. Let $\sigma : N \to M$ be the inclusion map and also R-module homomorphism. Then for $r \in R, n \in N$ we have $\rho_n(r,n) = \sigma(\rho_n(r,n)) = \rho_m(r, \sigma(n)) = \rho_m(r,n)$. This concludes action on M is preserved in N. □

6 Products, coproducts, etc., in R-Mod

6.1 Products and coproducts

6.2 Kernals and cokernels

6.3 Free modules and free algebras

Proposition 6.3.1. $R[A]$ is a free commutative R-algebra on the set A.

Proof. Elaborate. □

Remark 6.3.2. The proof for free modules and free commutative algebras are different because, unlike $R^{\oplus A}$ whose elements can be written uniquely as finite sum $\sum_{a\in A} r_a j(a)$, not every element of $R[A]$ can be written as $\sum_{a\in A} r_a x_a$.

6.4 Submodule generated by a subset; Noetherian modules

The module M is *finitely generated* if $M = \langle A\rangle$ for a *finite* set A.

6.5 Finitely generated vs. finite type

In this subsection, R, S are commutative rings.

Proof of 'finite' $\implies$ 'finite type'. We want to show that if commutative ring S is finite as an R-module over finite set $A = \{\mathbf{1}, \mathbf{2}, \dots, \mathbf{n}\}$ then S is a finite-type R-algebra over A. From previous sections, S is finite generated as an R-module if

$$S = \langle A\rangle = \left\{ \sum_{1\le i\le n} r_i\mathbf{i} | r_i \neq 0 \text{ for only finitely many elements } \mathbf{i} \in A \right\},$$

where $\langle A\rangle$ is the submodule generated by A in S, or the image of onto homomorphism of R-modules $R^{\oplus A} \twoheadrightarrow S$.

Now, going back to our unique homomorphism of R-algebras $\varphi : R[A] \to S$ which sends $j_i := x_i$ to $\mathbf{i}$ for $1 \le i \le n$. As an homomorphism of R-module, φ sends $\sum_{1\le i\le n} r_i j_i$ [2] to $\sum_{1\le i\le n} r_i\mathbf{i}$ where $r_i \in R$. Therefore, φ is surjective homomorphism of R-algebras, which means S is a finite-type R-algebras over A. □

Remark 6.5.1. Perhaps the motivation (or maybe a cleaner proof) for the above proof is to notice that there is an injection (homomorphism of R-modules) $R^{\oplus A} \hookrightarrow R[A]$ sending $k_i \in R^{\oplus A}$ ($k_i(\mathbf{i}) = 1$ and $k_i(\mathbf{l}) = 0$ for $l \neq i$) to $j_i := x_i \in R[A]$, which can be seen in following diagram

$$\begin{tikzcd}
R^{\oplus A} \arrow[d, hook] \arrow[dr, two heads] & \\
R[A] \arrow[r, two heads] & S
\end{tikzcd}$$

And perhaps why the converse is not true because there reverse map $R[A] \to R^{\oplus A}$ cannot be injective(?) since "size of $R[A]$ is much bigger than of $R^{\oplus A}$"(?). Don't have words to describe this yet.

[2]Note that $r_i j_i$ does not mean $r_i x_i \in R[A]$ but rather $r_i j_i$ is the result when we see $R[A]$ as an R-module, i.e. $r_i j_i = (\sigma(r_i))(j_i)$ where σ is a left-action of R on $R[A]$. With this then $\varphi(r_i j_i) = r_i\varphi(j_i) = r_i\mathbf{i}$ as φ is an homomorphism of R-modules.

Example 6.5.2. The polynomial ring $R[x]$ is a finite-type R-algebra, but it is not finite as an R-module. ⌟

7 Complexes and homology

Example 7.0.1. A complex

$$\cdots \longrightarrow 0 \longrightarrow L \xrightarrow{\alpha} M \longrightarrow \cdots$$

is exact at L iff α monomorphism. ⌟

7.1 Exercises

1. (7.1) Complex

$$\cdots \longrightarrow 0 \xrightarrow{\alpha} M \xrightarrow{\beta} 0 \longrightarrow \cdots$$

is exact. Since α a R-module homomorphism so it is also group homomorphism so $\text{im}\alpha = \{0\}$. Since the complex is exact at M so $\text{im}\alpha = \ker\beta$ but $\ker\beta = M$ so $M = 0$.

2. (7.2) Complex

$$\cdots \longrightarrow 0 \longrightarrow M \xrightarrow{\alpha} M' \longrightarrow 0 \longrightarrow \cdots$$

is exact then $M \cong M$. Indeed, exactness at M implies α is injective and at M' implie α is surjective. Thus, α is a R-module isomorphism so $M \cong M'$.

3. (7.3) The complex

$$\cdots \longrightarrow 0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\varphi} M' \xrightarrow{\beta} N \longrightarrow 0 \longrightarrow \cdots$$

is exact then up to natural identifications, $L = \ker\varphi$ and $N = \text{coker}\varphi$. Indeed, exactness at L implies α is injective so one can view L as submodule of M, or $L \cong \text{im}\alpha$. Exactness at M implies $\ker\varphi = \text{im}\alpha \cong L$, as desired.

Exactness at N implies β is surjective so by cannonical decompositions of β, we have $N = \text{im}\beta \cong M'/\ker\beta$. On the other hand, due to exactness at M' so $\ker\beta = \text{im}\varphi$ so $N \cong M'/\text{im}\varphi = \text{coker}\varphi$.

4. (7.4) Construct short exact sequence of $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow \mathbb{Z} \longrightarrow 0$$

and

References

algchap0 [1] Paolo Aluffi. Algebra: Chapter 0