1. Sheet 0

Exercise 1.1 (1)**.** (1) Find rings R and S and a nonzero map $\varphi\colon R \to S$ such that

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{and} \quad \varphi(ab) = \varphi(a)\varphi(b)$$

for all $a, b \in R$, but for which $\varphi(1_R) \neq 1_S$.

(2) Describe the set $\mathrm{Hom}_{\mathrm{URing}}(\mathbb{Z}/m, \mathbb{Z}/n)$ for all possible choices of $n, m \in \mathbb{Z}_{\geq 0}$.

(3) Let R be a ring. Prove that there is a bijective correspondence

$$\mathrm{Hom}_{\mathrm{URing}}(\mathbb{Z}[x], R) \cong R.$$

(4) Prove that the abelian group $(\mathbb{Q}/\mathbb{Z}, +)$ does not admit a ring structure. Precisely, this means that for any operation $\circ\colon \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, the triplet $(\mathbb{Q}/\mathbb{Z}, +, \circ)$ does not satisfy the ring axioms.

(5) Show that the set $\mathrm{Hom}_{\mathrm{URing}}(\mathbb{Z}/m, \mathbb{Z}/n)$ does in general not admit a ring structure.

Proof. (1) Choose $\varphi\colon \mathbb{Z}/2 \to \mathbb{Z}/4$ by $1 \mapsto 2$.

(2) Any map $\varphi\colon \mathbb{Z}/m \to \mathbb{Z}/n$ in URing must take $1 \mapsto 1$, and is uniquely determined thereby since $\varphi(k) = \varphi(1 + \ldots + 1) = \varphi(1) + \ldots + \varphi(1) = k$. Therefore, $0 = \varphi(m) = m$ in $\mathbb{Z}/n$, so $n \mid m$. And it is clear that if $n \mid m$, then $1 \mapsto 1$ is a well-defined ring homomorphism. Thus

$$\mathrm{Hom}_{\mathrm{URing}}(\mathbb{Z}/m, \mathbb{Z}/n) = \begin{cases} \{1 \mapsto 1\}, & n \mid m \\ \varnothing, & \text{otherwise} \end{cases}.$$

(3) We claim that the correspondence

$$\begin{aligned} \mathrm{Hom}_{\mathrm{URing}}(\mathbb{Z}[x], R) &\to R \\ \varphi &\mapsto \varphi(x) \end{aligned}$$

is bijective. Indeed, $\varphi(1) = 1$ necessarily, so $\varphi(k) = k$ for all $k \in \mathbb{Z}$, so we simply have $\varphi\left(\sum \alpha_i x^i\right) = \sum \varphi(\alpha_i)\varphi(x)^i = \sum \alpha_i \varphi(x)^i$, so φ is uniquely determined by where it sends x. Furthermore, for any $r \in R$, define $\varphi_r\colon \mathbb{Z}[x] \to R$ by $x \mapsto r$. This extends uniquely to a ring homomorphism $\mathbb{Z}[x] \to R$.

(4) Suppose $(\mathbb{Q}/\mathbb{Z}, +)$ admits a ring structure with multiplication $\cdot$. Let $\frac{a}{b} \in \mathbb{Q}/\mathbb{Z}$ be the unit. Then, in particular, $\frac{a}{b} \cdot \frac{1}{x} = \frac{1}{x}$ for all x, so $\left(\frac{a}{b} - 1\right)\frac{1}{x} \in \mathbb{Z}$ for all x, meaning that any x divides $\frac{a}{b} - 1$. Thus is only possible if $\frac{a}{b} = 1$. But $1 \in \mathbb{Z}$, so the unit is the zero element, so for any $\frac{x}{y} \in \mathbb{Q}/\mathbb{Z}$, we have $\frac{x}{y} = \frac{x}{y} \cdot 1 = 0$. Hence $\mathbb{Q}/\mathbb{Z}$ becomes the zero ring, but then 1 does not act by the identity on any rational element in $\mathbb{Q}/\mathbb{Z}$.

(5) By (2), $\mathrm{Hom}_{\mathrm{URing}}(\mathbb{Z}/m, \mathbb{Z}/n)$ is either a single map or empty, and as the empty set is not a ring, this Hom set in general does not admit a ring structure - when it does, it must be the trivial one.

□

Exercise 1.2 (2)**.** (1) Let A be a ring. How many $\mathbb{Z}$-algebra structures does A admit?

(2) Find rings R and A, such that A admits more than one R-algebra structure.

(1) A admits a unique $\mathbb{Z}$-algebra structure since any ring homomorphism $\mathbb{Z} \to A$ is uniquely determined by $1 \mapsto 1$.
(2) Take $A = \mathbb{Z}[x]$ and R to be any ring with more than one element. By exercise 1.(c), $\mathrm{Hom}_{\mathrm{Ring}}(\mathbb{Z}[x], R) \cong R$, so R admits more than one R-algebra structure.

However, these structures could be isomorphic in the sense that there exists maps $\varphi, \psi \colon R \to R$ with $\varphi\psi = \mathrm{id} = \psi\varphi$ and composing one algebra structure $\mathbb{Z}[x] \to R$ with φ gives ψ and vice versa.

So we must find explicit examples which are non-isomorphic. Define $f, g \colon \mathbb{Z}[x] \to \mathbb{Z}/6$ by $f(x) = 2$ and $g(x) = 3$. Now, there is no ring homomorphism $\varphi\mathbb{Z}/6 \to \mathbb{Z}/6$ such that $\varphi \circ f = g$ since $0 = \varphi(0) = \varphi \circ f(3x) = g(3x) = 3$ gives a contradiction.

Exercise 1.3 (3)**.** This is just the 4th isomorphism theorem for ideals of rings.
Define a map $\pi \colon \mathcal{A} \to \mathcal{B}$ by sending $A \to \overline{A} = A + I$.
Suppose $\pi(A) = \pi(B)$. Then for any $a \in A$, there exists $b \in B$ such that $a - b \in I \subset A \cap B$, hence $a, b \in A \cap B$. Thus $A \subset B \subset A$, so $A = B$.
Now, suppose $V \in \mathcal{B}$. Let $A = \pi^{-1}(V)$. This is an ideal containing I. If $a, b \in A$ then $\pi(a), \pi(b) \in V$ so $\pi(ab) = \pi(a)\pi(b) \in V$, hence $ab \in \pi^{-1}(V)$. Similar closure for the rest. And if $r \in R$ then $\pi(ar) = \pi(a)\pi(r) \in V$ as $\pi(a) \in V$ and V is an ideal, so $ar \in A$, hence A is an ideal. This gives surjectivity.

Exercise 1.4 (4)**.** $(2, x) \subset \mathbb{Z}[x]$ is not principle as an ideal generated over $\mathbb{Z}$. If $(2, x) = (p(x))$, then $p(x) \mid 2$ implies that that the degree of p is 0. Now let $q(x)$ be such that $p(x)q(x) = x$ and $h(x)$ such that $p(x)h(x) = 2$. Then the degree of h is 0 and that of q is 1. Furthermore, as $p \in (2, x)$, we must have either $p(x) = 2k(x)$ or $p(x) = xl(x)$. But this implies that either $2k(x)q(x) = x$, so $2 \mid x$ in $\mathbb{Z}[x]$, which is impossible, or $xl(x)h(x) = 2$, so $x \mid 2$ in $\mathbb{Z}[x]$ which is impossible by degree as $\mathbb{Z}$ is an integral domain. Hence we obtain a contradiction.

Exercise 1.5 (5)**.** (1) Let I, J be ideals in a ring R. Show that we always have the inclusion of ideals

$$(I + J)(I \cap J) \subset IJ \subset I \cap J \subset I + J.$$

(2) For each of the inclusions above, find an example where it is a proper inclusion.
(3) Show that if $I + J = R$, then all the inclusions above are in fact equalities (False. Counterexample below)
(4) Prove the following generalization of the Chinese Remainder Theorem. Given a ring R and finitely many ideals $\{I_1, \ldots, I_n\}$ in R, such that for each pair $1 \leq i \neq j \leq n$, one has $I_i + I_j = R$. Let

$$I = \bigcap_i I_i.$$

Construct an isomorphism of rings

$$\prod R/I_i \cong R/I.$$

Proof. (1) Recall that $(I + J) = (I \cup J)$ and that for ideals N, M, $NM = (nm \mid n \in N, m \in M)$. If $x \in (I + J)(I \cap J)$, then $x = \sum \alpha_i\beta_i$ where $\alpha_i \in (I + J)$ and $\beta_i \in (I \cap J)$. So let $\alpha_i = \sum c_{ij}$ where c_{ij} is in I or in J. Writing $\beta_i = \sum e_i$ where $e_i \in I \cap J$, we have $x = \sum c_{ij}e_k$. If c_{ij} is in I, then $c_{ij}e_k \in IJ$ since $e_k \in J$, and similarly if $c_{ij} \in J$.

Next assume $x \in IJ$, so $x = \sum c_i d_i, c_i \in I, d_i \in J$. Since I and J are ideals, each $c_i d_i \in I \cap J$, hence $IJ \subset I \cap J$.

Lastly, $x \in I \cap J$ then $x \in I, J$ so also in $I \cup J$, hence $x \in I + J$.

(2) Let $R = \mathbb{Z}[x]$. Then Let $I = (2x), J = (3x^2)$. Then $I + J = (2x, 3x^2)$ while $I \cap J = \left(6x^2\right)$. Then $(I + J)(I \cap J) = \left(12x^3, 18x^4\right)$ while $IJ = \left(6x^3\right)$, so the containment is clearly proper as $6x^3$ is not in $(I + J)(I \cap J)$.
Next, if $I = (x) = J$, then $IJ = (x^2)$ is properly contained in $(x) = I \cap J$.
Lastly, if $I = (2x)$ and $J = (3x)$, then $I \cap J = (6x)$ while $I + J = (x)$ since $3x - 2x = x \in I + J$.

(3) This cannot be true: consider $I = 2\mathbb{Z}, J = 3\mathbb{Z}$. Then $I + J = \mathbb{Z}$ while $I \cap J = 6\mathbb{Z}$. □

Exercise 1.6 (7)**.** (1) Surjectivity amounts to finding an $f \in K[x_1, \ldots, x_n]$ such that $f(y) = k$ for some arbitrary $k \in K$. Consider the map $f(x_1, \ldots, x_n) = k + (x_1 - y_1) \ldots (x_n - y_n)$. Or the constant polynomial at k works also. Now, $\varphi_y(f + g) = (f + g)(y) = f(y) + g(y) = \varphi_y(f) + \varphi_y(g)$, and $\varphi_y(fg) = \varphi_y(f)\varphi_y(g)$ is seen likewise.

That it is a homomorphism of K-algebras (with the standard K-algebra structure) amounts to showing that $\varphi_y(k) = k$ which is clear.

(2) Let $\varphi\colon K[x_1, \ldots, x_n] \to K$ be a ring homomorphism. Let $y_i = \varphi(x_i)$. Then $\varphi\left(\sum a_I x_I\right) = \sum \varphi(a_I) y_I = \varphi_{y_I}\left(\sum a_I x_I\right)$ (for this we need φ to be a K-algebra homomorphism of with $K[x_1, \ldots, x_n]$ in the standard structure. Is there a different way of arguing?)

2. Sheet 1

Exercise 2.1 (1)**.** *Proof.* (i) We claim that $\left(x^2 + 1\right)$ is a radical, prime and maximal ideal in $\mathbb{R}[x]$. This can be seen by noting that $\mathbb{R}[x] / \left(x^2 + 1\right) \cong \mathbb{C}$ which is a field. Hence $\left(x^2 + 1\right)$ is maximal. Suppose $f^n \in \left(x^2 + 1\right)$. Since $x^2 + 1$ is irreducible and $x^2 + 1 \mid f^n$, we must have $x^2 + 1 \mid f$, hence $f \in \left(x^2 + 1\right)$, so $\sqrt{\left(x^2 + 1\right)} = \left(x^2 + 1\right)$. Over $\mathbb{C}[x]$, we claim that $\left(x^2 + 1\right)$ is neither prime nor maximal, but still radical. It is not prime as $x^2 + 1 = (x + i)(x - i)$ and hence also not maximal since $\left(x^2 + 1\right) \subset (x + i) \neq \mathbb{C}[x]$, where inequality follows from $(x + i)$ only having polynomials of degree ≥ 1.
Now suppose $f^n \in \left(x^2 + 1\right)$. Then $x + i, x - i \mid f^n$, hence both must divide f as they are irreducible, so $x^2 + 1 \mid f$. Thus $f \in \left(x^2 + 1\right)$, so $\sqrt{\left(x^2 + 1\right)} = \left(x^2 + 1\right)$ over $\mathbb{C}[x]$ as well.

(ii) Since $\left(x^2 + 1\right)$ is a prime ideal in $\mathbb{R}[x]$ by the previous exercise, we find by Eisenstein's criterion that $y^2 + x^2 + 1$ is irreducible in $\mathbb{R}[x][y] =: \mathbb{R}[x, y]$.

(iii)
Let $C = \left\{f \in C\left(\mathbb{R}^2, \mathbb{R}\right) \mid \forall x \in \mathbb{R}\colon f(x, 0) = 0\right\} \subset C\left(\mathbb{R}^2, \mathbb{R}\right)$. We claim that C is radical, but neither prime nor maximal.

To see that it is radical, suppose $g^n \in C$, so $g(x,0) \cdot \ldots \cdot g(x,0) = g^n(x,0) = 0$. Since $\mathbb{R}$ is an integral domain, this forces $g(x,0) = 0$, so $g \in C$. Thus $\sqrt{C} = C$.
Now let $h(x) = \mathbb{1}_{\geq 0}(x)x$ and $k(x) = \mathbb{1}_{\leq 0}(x)x$. Then $h, k \notin C$, but $hk \in C$. Therefore, C is not prime. Since $C\left(\mathbb{R}^2, \mathbb{R}\right)$ is a commutative ring and maximal ideals are prime over a commutative ring, we thus also conclude that C is not maximal.

(iv) The ideal (5) in $\mathbb{Z}[i]$ is not prime, hence not maximal as $\mathbb{Z}[i]$ is commutative. It is not prime because $5 = (2+i)(2-i)$.
For the radical part, if $a+bi \in \sqrt{(5)}$, then $(2+i)(2-i) \mid (a+bi)^n$, so $2+i \mid a+bi$ and $2-i \mid a+bi$ since each is irreducible, hence $5 \mid a+bi$, so $\sqrt{(5)} = (5)$.

(v) We claim that $(n) \subset \mathbb{Z}$ is prime and maximal whenever n is a prime and not otherwise. If n is not prime, then writing $n = ab$ for $a, b > 1$, we have $(n) = (a)(b)$, so (n) is not prime, hence not maximal as $\mathbb{Z}$ is commutative so all maximal ideals are prime ideals. If instead n is a prime, $n = p$, then (p) is both maximal and prime since $\mathbb{Z}/p$ is a field.
Suppose now $m \in \sqrt{(n)}$. Then $m^k \in (n)$, so $m^k = nq$ for some $q \in \mathbb{Z}$. Suppose n is squarefree. Let $p \mid n$. Then $p \mid m^k$ and thus $p \mid m$, so $n \mid m$, hence $m \in (n)$. Conversely, if n is not squarefree, then letting $n = p^k q$ for some $k > 1$, we have $p^{k-1}q \in \sqrt{(n)}$ while $p^{k-1}q \notin (n)$, so (n) is not radical. □

Exercise 2.2 (2)**.** Let $n \in \mathbb{N}$. We denote the set of orthogonal matrices on $\mathbb{R}^n$ by

$$O\left(\mathbb{R}^n\right) = \left\{A \in \mathbb{R}^{n\times n} \mid A^T A = I_n\right\}$$

Write $R = \mathbb{R}\left[x_{ij} \mid i,j = 1,\ldots,n\right]$ for the polynomial ring in variables $X = (x_{ij})_{i,j=1,\ldots,n}$.

(1) Show that $O\left(\mathbb{R}^n\right)$ is the zero set $\mathbb{V}(I)$ of the ideal $I = (\{f_{ij} \mid i,j = 1,\ldots,n\})$ of R where

$$f_{i,j} = \sum_{k=1}^{n} x_{ki}x_{kj} \quad \text{for } i \neq j \quad \text{and} \quad f_{ii} = \sum_{k=1}^{n} x_{ki}^2 - 1.$$

(2) Show that $O\left(\mathbb{R}^n\right)$ is also the real zero set of the ideal $J = (g,h)$ generated by the polynomials $g = \det(X)^2 - 1$ and $h = \sum_{i,j=1}^{n} x_{ij}^2 - n$.

Proof. (a) We know that $A = (\alpha_{ij}) \in O\left(\mathbb{R}^n\right)$ if and only if $A^T A = I$. Taking entries of either side of this equality, we get that A is orthogonal if and only if both of the following conditions hold:

$$0 = \left(A^T A\right)_{ij} = \sum_{k=1}^{n} \left(A^T\right)_{ik} A_{kj} = \sum_{k=1}^{n} \alpha_{ki}\alpha_{kj}$$

$$1 = \left(A^T A\right)_{ii} = \sum_{k=1}^{n} \alpha_{ki}^2.$$

That is, $A \in O\left(\mathbb{R}^n\right)$ if and only if $A \in \mathbb{V}(I)$ where we identify $R \cong M_n\left(\mathbb{R}\right)$ by $\sum \alpha_{ij}x_{ij} \mapsto (\alpha_{ij})$.

(b) Firstly, suppose $A \in O\left(\mathbb{R}^n\right)$. Then $A^T A = I$. Therefore, $\det(A)^2 - 1 =$

$\det(A^T)\det(A) - 1 = \det(A^T A) - 1 = \det(I) - 1 = 0$, so $g(A) = 0$. And now

$$n = \operatorname{tr}(I) = \operatorname{tr}(A^T A) = \sum_{k=1}^{n} \left(A^T A\right)_{kk} = \sum_{k,r=1}^{n} \alpha_{rk}^2$$

hence also $h(A) = 0$. Therefore $O(\mathbb{R}^n) \subset \mathbb{V}(J)$.
Conversely, suppose $A = (\alpha_{ij}) \in \mathbb{V}(J)$. Firstly, note that since

$$x^T A^T A x = (Ax)^T Ax = \|Ax\|^2 \geq 0,$$

the matrix $A^T A$ is positive semi-definite, hence all its eigenvalues are non-negative real numbers. In particular, $\sqrt[n]{\Pi_{i=1}^n \lambda_i}$ is well-defined where $\lambda_1, \ldots, \lambda_m$ are the eigenvalues of $A^T A$ listed with repetition, and we can apply the AMGM inequality. Recall that the AMGM inequality tells us that

$$\frac{\sum_i \lambda_i}{n} \geq \sqrt[n]{\prod_i \lambda_i}$$

with equality if and only if all the λ_i are equal. But by Jordan normal form, $\operatorname{tr}\left(A^T A\right) = \sum_i \lambda_i$, and $\det\left(A^T A\right) = \prod_i \lambda_i$, so we obtain

$$\operatorname{tr}(A^T A) \geq n \det\left(A^T A\right)$$

with equality if and only if all eigenvalues are equal. But since $A \in \mathbb{V}(J)$, we have $g(A) = 0$, so $\det\left(A^T A\right) = \det(A)^2 = 1$. Likewise,

$$\operatorname{tr}\left(A^T A\right) = \sum_{k=1}^{n} \left(A^T A\right)_{kk} = \sum_{k,r=1}^{n} \alpha_{rk}^2 = h(A) + n = n$$

Thus we get

$$n = \operatorname{tr}\left(A^T A\right) \geq n \det\left(A^T A\right) = n$$

so we conclude that, since we have equality between the two sides, all eigenvalues of $A^T A$ must be equal. Now since $A^T A$ is self-adjoint, it is in particular diagonable, hence it has precisely n eigenvalues counted with multiplicity. Therefore, it has one eigenvalue with multiplicity n. Letting wlog λ denote this eigenvalue, we get

$$n\lambda = \operatorname{tr}\left(A^T A\right) = n$$

so $\lambda = 1$ since $\mathbb{R}$ is an integral domain. To see that this forces $A^T A$ to be I, we note that since $A^T A$ is diagonable, we can find some invertible linear map $P \in \mathrm{GL}_n(\mathbb{R})$ such that $PA^T AP^{-1} = I$, implying $A^T A = I$. Thus A is orthogonal, so $A \in O(\mathbb{R}^n)$. This gives the inclusion $\mathbb{V}(J) \subset O(\mathbb{R}^n)$. □

3. Sheet 3

Exercise 3.1 (2)**.** Let R be a Noetherian ring. Show that every ideal of R is a finite intersection of irreducible ideals.

Proof. Let $\mathcal{A}$ be the set of ideals of R which are not a finite intersection of irreducible ideals. Suppose $\{X_i\} = \mathcal{X} \subset \mathcal{A}$ is a chain with respect to inclusion. Then since R is Noetherian, this chain stabilizes, hence it has an upper bound. Thus $\mathcal{A}$ has a maximal element, call it M. Now, M is not a finite intersection of irreducible ideals, so in particular, M is not irreducible, so write $M = I \cap J$ where I and J contain M properly. But then $I, J \notin \mathcal{A}$, so they are finite intersections of irreducible ideals. However, then their intersection is also a finite intersection of irreducible ideals. □

Exercise 3.2 (3)**.** Let R be a ring. Show that an ideal $\mathfrak{B}$ of R is a prime ideal if and only if for all ideals I and J of R, $IJ \subset \mathfrak{B}$ implies $I \subset \mathfrak{B}$ or $J \subset \mathfrak{B}$.

Proof. If $\mathcal{B}$ is a prime ideal, then suppose $IJ \subset \mathcal{B}$, and suppose $I \not\subset \mathcal{B}$. Then there exists some $i \in I$ such that $i \notin \mathcal{B}$ but $iJ \subset \mathcal{B}$. Since $\mathcal{B}$ is prime, we must have that $J \subset \mathcal{B}$.
Conversely, suppose that for all I, J, $IJ \subset \mathcal{B}$ implies $I \subset \mathcal{B}$ or $J \subset \mathcal{B}$. Let $a, b \in R$ such that $ab \in \mathcal{B}$. Then
$(a)(b) \subset \mathcal{B}$, so either $(a) \subset \mathcal{B}$ or $(b) \subset \mathcal{B}$, so either $a \in \mathcal{B}$ or $b \in \mathcal{B}$. So $\mathcal{B}$ is prime. □

Exercise 3.3 (4)**.** Let R_S be the localization of the integral domain R by a multiplicative subset S which does not contain 0. Let $\mathfrak{U}$ be a primary ideal of R. Show that the extension $\mathfrak{U}R_S$ is a primary ideal of R_S and that $R \cap \mathfrak{U}R_S = \mathfrak{U}$.

Proof. Let $\tau\colon R \to R_S = (R-S)^{-1}R$. Recall that $\mathfrak{U}R_S = (\tau(\mathfrak{U}))$. Suppose $ab \in \mathfrak{U}R_S$. Then there exists $\sum \alpha_i u_i \in \mathfrak{U}$ such that $ab = \sum \alpha_i \tau(u_i) = \sum \alpha_i \frac{u_i}{1}$. We can write $a = \frac{x}{y}$ and $b = \frac{v}{w}$. Then $xv \in \mathfrak{U}$, so either $x \in \mathfrak{U}$, in which case $\frac{x}{y} \in \mathfrak{U}R_S$, or $v^n \in \mathfrak{U}$, in which case $\left(\frac{v}{w}\right)^n \in \mathfrak{U}R_S$ since S is multiplicative, so $w^n \in S$. Thus $a \in \mathfrak{U}R_S$ or $b^n \in \mathfrak{U}R_S$. Hence $\mathfrak{U}R_S$ is primary in R_S.
Now recall that $R \cap \mathfrak{U}R_S$ denote the contraction of $\mathfrak{U}R_S$ along τ, i.e., $R \cap \mathfrak{U}R_S = \tau^{-1}(\mathfrak{U}R_S)$. Clearly, $\mathfrak{U} \subset R \cap \mathfrak{U}R_S$. Conversely, suppose $a \in \tau^{-1}(\mathfrak{U}R_S)$. Then $\frac{a}{1} \in \mathfrak{U}R_S$, so $\frac{a}{1} = \sum \alpha_i \frac{u_i}{1}$. So there exists some $r \in R - S$ such that $ra = r\sum \alpha_i u_i$. So since $r \neq 0$ as $0 \notin S$, we have $a = \sum \alpha_i u_i$ since R is an integral domain. Thus $a \in \mathfrak{U}$. □

Exercise 3.4 (5)**.** Let R be a ring and $\mathfrak{U}$ a $\mathfrak{B}$-primary ideal. Show the following.

(1) For all $x \in \mathfrak{U}$, we have $(\mathfrak{U}\colon x) = R$.
(2) For all $x \in R - \mathfrak{U}$, we have that $(\mathfrak{U}\colon x)$ is $\mathfrak{B}$-primary.
(3) For all $x \in R - \mathfrak{B}$, we have that $(\mathfrak{U}\colon x) = \mathfrak{U}$.
(4) If R is Noetherian, then there is some $x \in R - \mathfrak{U}$ such that $(\mathfrak{U}\colon x) = \mathfrak{B}$.

Proof. So $\sqrt{\mathfrak{U}} = \mathfrak{B}$ by assumption.

(1) Since $\mathfrak{U}$ is an ideal, $x\mathfrak{U} \subset \mathfrak{U}$ for all $x \in R$, so for all $x \in \mathfrak{U}$, $(\mathfrak{U}\colon x) = R$.
(2) Suppose $a \in \sqrt{(\mathfrak{U}\colon x)}$, so $a^n x \in \mathfrak{U}$. Since $\mathfrak{U}$ is primary, either $x \in \mathfrak{U}$, which we have assumed it is not, or $a^{nm} \in \mathfrak{U}$ for some m. Hence the latter must be true. So $a \in \sqrt{\mathfrak{U}} = \mathfrak{B}$.
Hence $\sqrt{(\mathfrak{U} : x)} \subset \mathfrak{B}$. Conversely, suppose $a \in \mathfrak{B}$, so $a^n \in \mathfrak{U}$. So for any $x \in R - \mathfrak{U}$, we have $a^n x \in \mathfrak{U}$, so $a \in \sqrt{(\mathfrak{U} : x)}$.
(3) Suppose $x \in R - \mathfrak{B}$. Now if $y \in \mathfrak{U}$ then $xy \in \mathfrak{U}$, so $y \in (\mathfrak{U} : x)$. Conversely, suppose $y \in (\mathfrak{U} : x)$. So $xy \in \mathfrak{U}$, so since $x \notin \mathfrak{B} = \sqrt{\mathfrak{U}}$, we must have that $y \in \mathfrak{U}$.
(4) Let n be minimal such that $\mathfrak{B}^n \subset \mathfrak{U}$. Let $x \in \mathfrak{B}^{n-1} - \mathfrak{U}$. We claim $(\mathfrak{U} : x) = \mathfrak{B}$. For $b \in \mathfrak{B}$, we have $bx \in \mathfrak{B}^n \subset \mathfrak{U}$, so $b \in (\mathfrak{U} : x)$. Conversely, if $bx \in \mathfrak{U}$, then since $x \notin U$, we have $b^m \in \mathfrak{U}$, so $b \in \sqrt{U} = \mathfrak{B}$. □

4. Assignment 2

Exercise 4.1. Given two local rings $(R, \mathfrak{m})$ and $(S, \mathfrak{n})$ be local rings. A ring homomorphism $f\colon R \to S$ is called a local homomorphism if the image of $\mathfrak{m}$ under f is contained in $\mathfrak{n}$.

(1) Let $g\colon A \to B$ be a ring homomorphism between two arbitrary rings and let $\mathfrak{p} \subset B$ and $\mathfrak{q} = g^{-1}(\mathfrak{p}) \subset A$ be prime ideals. Show that g localizes to a ring homomorphism $A_{\mathfrak{q}} \to B_{\mathfrak{p}}$ to be more precise, let $\pi_A\colon A \to A_{\mathfrak{q}}$ and $\pi_B\colon B \to B_{\mathfrak{p}}$ be the natural ring homomorphisms from the rings to their localizations. You need to construct a ring homomorphism $g'\colon A_{\mathfrak{q}} \to B_{\mathfrak{p}}$ such that $\pi_B \circ g = g' \circ \pi_A$. Show that the map g' you construct is a local homomorphism.
(2) Find a ring homomorphims between local rings which is not a local homomorphism.

Proof. (1) Consider the diagram

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ {\scriptstyle \pi_A}\downarrow & & \downarrow{\scriptstyle \pi_B} \\ A_{\mathfrak{q}} & \xrightarrow[g']{} & B_{\mathfrak{p}} \end{array}$$

Note that by the universal property of localizations, the map g' exists if and only if $\pi_B \circ g\left((A-\mathfrak{q})\right) \subset B_{\mathfrak{p}}^{\times} = (R-\mathfrak{p})_{\mathfrak{p}}$. Let $a \in A - \mathfrak{q}$. By assumption, $g(a) \notin \mathfrak{p}$, so $\pi_B\left(g(a)\right) = \frac{g(a)}{1} \in (R-\mathfrak{p})_{\mathfrak{p}}$. This gives the existence of g'.
Next we show that g' is a local homomorphism. Note that $A_{\mathfrak{q}}$ and $B_{\mathfrak{p}}$ are local rings with unique maximal ideals $\mathfrak{q}_{\mathfrak{q}}$ and $\mathfrak{p}_{\mathfrak{p}}$, respectively. Thus, to show that g' is a local homomorphism, we must show that $g'\left(\mathfrak{q}_{\mathfrak{q}}\right) \subset \mathfrak{p}_{\mathfrak{p}}$. Explicitly,

$$\mathfrak{q}_{\mathfrak{q}} = \left\{ \frac{a}{b} \in A_{\mathfrak{q}} \colon a \in \mathfrak{q} \right\}$$
$$\mathfrak{p}_{\mathfrak{p}} = \left\{ \frac{a}{b} \in B_{\mathfrak{p}} \colon a \in \mathfrak{q} \right\}.$$

Let $x \in \mathfrak{q}_{\mathfrak{q}}$, so there exist $a \in \mathfrak{q}$ and $b \in A - \mathfrak{q}$ such that $x = \frac{a}{b}$. Then $\frac{a}{b} = \pi_A(a)\pi_A(b)^{-1}$, so $g'\left(\frac{a}{b}\right) = g' \circ \pi_A(a)\left(g' \circ \pi_A(b)\right)^{-1} = \pi_B \circ g(a)\left(\pi_B \circ g(b)\right)^{-1} = \frac{g(a)}{g(b)}$ where we can invert by $g(b)$ since $g(b) \in B - \mathfrak{p}$ as $b \in A - \mathfrak{q}$ and $\mathfrak{q} = g^{-1}\left(\mathfrak{p}\right)$. Since $g(b) \in B - \mathfrak{p}$ and $g\left(\mathfrak{q}\right) \subset \mathfrak{p}$, so $g(a) \in \mathfrak{p}$, we have $\frac{g(a)}{g(b)} \in \mathfrak{p}_{\mathfrak{p}}$, so $g'(x) \in \mathfrak{p}_{\mathfrak{p}}$, hence $g\left(\mathfrak{q}_{\mathfrak{q}}\right) \subset \mathfrak{p}_{\mathfrak{p}}$.

(2) The ring $\mathbb{Z}_{(p)}$ is local and $\mathbb{Q}$ being a field is also local. However, the inclusion $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Q}$ is not a local homomorphism since $\frac{p}{1}$ is not mapped to 0, for example. □

5. Assignment 3

Exercise 5.1. Let R be a Noetherian ring. Show the following

(1) For every ideal $I \subset R$, there exists $n \in \mathbb{N}$ such that $\left(\sqrt{I}\right)^n \subset I$.
(2) Every radical ideal of R is a finite intersection of prime ideals.
(3) If a radical ideal of R is irreducible, then it is a prime ideal.

Proof. (1) Since $I \subset \sqrt{I}$ are sub-R-modules of R considered as a module over itself, we find that $\sqrt{I}$ must be finitely generated, so let $\sqrt{I} = \langle x_1, \ldots, x_n \rangle$, and by assumption, there exist $\alpha_1, \ldots, \alpha_n$ such that $x_i^{\alpha_i} \in I$. Let $\alpha = \alpha_1 + \ldots + \alpha_n$. Now let $x \in \sqrt{I}$ and write $x = \sum_i c_i x_i$. Then any term in x^α will contain some x_i to the power of at least α_i by the pigeonhole principle. Since I is an ideal, the whole term is in I, so again, ideals are closed under sums, so $x^\alpha \in I$. Since x was arbitrary, we

find that $\left(\sqrt{I}\right)^{\alpha} \subset I$.

(2) Let I be a radical ideal of R, so $\sqrt{I} = I$. By theorem 7.19 (Primary decomposition), I is the finite intersection of primary ideals, so

$$I = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_\mathfrak{n}$$

where each $\mathfrak{p}_i$ is primary.

Lemma 5.2. *For an ideal $J = J_1 \cap \ldots \cap J_n$, we have*

$$\sqrt{J} = \sqrt{J_1} \cap \ldots \cap \sqrt{J_n}$$

Proof. Suppose $x \in \sqrt{J}$ so $x^i \in J = J_1 \cap \ldots \cap J_n$, then $x^i \in J_j$ for all j so $x \in \sqrt{J_j}$ for all J, so $x \in \sqrt{J_1} \cap \ldots \cap \sqrt{J_n}$. Conversely, if $x \in \sqrt{J_1} \cap \ldots \cap \sqrt{J_n}$ then there exist $\alpha_1, \ldots, \alpha_n$ such that $x^{\alpha_i} \in J_i$. Let $\alpha = \max_i \{\alpha_i\}$. Then $x^\alpha \in J_1 \cap \ldots \cap J_n = J$, so $x \in \sqrt{J}$. □

Hence we obtain

$$I = \sqrt{I} = \sqrt{\mathfrak{p}_1} \cap \ldots \cap \sqrt{\mathfrak{p}_n}.$$

To finish it off, we note that by Lemma 7.11, each $\sqrt{\mathfrak{p}_i}$ is prime.

(3) Suppose $I \subset R$ is a radical ideal which is irreducible. By Lemma 7.16, I is primary, and now by Lemma 7.11, $I = \sqrt{I}$ is prime. □

Exercise 5.3. Let $V \subset K^n$ be an affine algebraic set. Show the following.

(1) V is irreducible if and only if $\mathbb{I}(V)$ is a prime ideal.
(2) V can be written as a finite union of irreducible affine algebraic sets.
(3) There is a minimal decomposition $V = V_1 \cup \ldots \cup V_m$ of V into irreducible affine algebraic sets V_i, where $m \in \mathbb{N}_0$. This is meant in the sense that no V_i is contained in $\bigcup_{j \neq i} V_j$.
(4) The minimal decomposition $V = V_1 \cup \ldots \cup V_m$ is unique, up to reordering of $V_1, \ldots, V_m$. We call $V_1, \ldots, V_m$ the irreducible components of V.

Proof. (1) Since $V \subset K^n$ is an affine algebraic set, there exists some ideal $I \subset k[x_1, \ldots, x_n]$ such that $V = \mathbb{V}(I)$. Suppose $V = V_1 \cap V_2$ with both V_1 and V_2 being affine algebraic sets properly containing V. Then $\mathbb{I}(V) \subset \mathbb{I}(V_1) \cap \mathbb{I}(V_2)$ since any polynomial vanishing on V must vanish on both V_1 and on V_2. But now any prime ideal is irreducible, so $\mathbb{I}(V_1) = \mathbb{I}(V)$ or $\mathbb{I}(V_2) = \mathbb{I}(V)$. Suppose without loss of generality that $\mathbb{I}(V_2) = \mathbb{I}(V)$. Then $V_2 = \mathbb{V}(\mathbb{I}(V_2)) = \mathbb{V}(\mathbb{I}(V)) = V$. For this, we need to show that $\mathbb{V}(\mathbb{I}(W)) = W$ when W is an affine algebraic set. But $\mathbb{I}(\mathbb{V}(U)) \subset U$ always, so since $\mathbb{V}$ is containment-reversing, we get $W = \mathbb{V}(U) \subset \mathbb{V}(\mathbb{I}(W))$. For the opposite direction, we simply have that if $x \in \mathbb{V}(\mathbb{I}(W))$, then any $f \in \mathbb{I}(W) = \mathbb{I}(\mathbb{V}(U)) \subset U$ vanishes on x. Suppose $x \notin W = \mathbb{V}(U)$. Then there exists some $g \in U$ such that $g(x) \neq 0$. But $g \in \mathbb{I}(\mathbb{V}(U)) = \mathbb{I}(W)$ by definition which gives a contradiction. Hence $\mathbb{V}(\mathbb{I}(W)) \subset W$. Having concluded that $V = V_1$ or $V = V_2$, this shows that V is irreducible.

A faster way to see this, I suppose would be the following: If $V = V_1 \cup V_2$, then $\mathbb{I}(V_1) \cap \mathbb{I}(V_2) \subset \mathbb{I}(V)$, showing that $\mathbb{I}(V)$ is not irreducible, contradicting lemma 7.3.

Conversely, if $\mathbb{I}(V)$ is not prime, let $fg \in \mathbb{I}(V)$ such that $f, g \notin \mathbb{I}(V)$. Then $V = \mathbb{V}(\mathbb{I}(V)) \subset \mathbb{V}((f)(g)) \subset \mathbb{V}(f) \cap \mathbb{V}(g)$ using that $\mathbb{V}$ is inclusion-reversing. Now by assumption, if $V = \mathbb{V}(f)$, then f would vanish on all of V, contradicting $f \notin \mathbb{I}(V)$. Similarly for g. Hence V is shown to not be irreducible.
(2) Since V is an affine algebraic set, there exists an ideal I such that $V = \mathbb{V}(I)$. Now, $I \subset k[x_1, \ldots, x_n]$ which is Noetherian by applying Hilbert's basis theorem iteratively since a field is Noetherian (having only (0) and itself as ideals) considered as k-modules. This in particular gives us a decomposition

$$I = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$$

where each $\mathfrak{p}_i$ is primary. Hence

$$\mathbb{V}(I) = \mathbb{V}(\mathfrak{p}_1) \cup \ldots \cup \mathbb{V}(\mathfrak{p}_n).$$

To show that $\mathbb{V}(\mathfrak{p}_i)$ is irreducible, we can show that $\mathbb{I}(\mathbb{V}(\mathfrak{p}_i))$ is a prime ideal. This can be easily achieved if we may use Nullstellensatz since then $\mathbb{I}(\mathbb{V}(\mathfrak{p}_i)) = \sqrt{\mathfrak{p}_i}$ which is prime by Lemma 7.11.

(3) By part (2), V can be decomposed as $V = V_1 \cup \ldots \cup V_n$ where each V_i is an irreducible affine algebraic set. Suppose now that $V_1 \subset \bigcup_{i=2}^n V_i$. But then

$$V_1 = \bigcup_{i=2}^{n} (V_1 \cap V_i).$$

Now, the intersection of affine algebraic sets is still an affine algebraic set since $\mathbb{V}(I_1) \cap \mathbb{V}(I_2) = \mathbb{V}(I_1 \cup I_2)$. Similarly, a union of finitely many affine algebraic sets is also an affine algebraic set since $\mathbb{V}(I_1 \cdots I_n) = \mathbb{V}(I_1) \cap \ldots \cap \mathbb{V}(I_n)$. So by irreducibility of V_1, either $V_1 = V_1 \cap V_2$ or $V_1 = \bigcup_{i=3}^n V_1 \cap V_i$. Inductively, we obtain that for some $i \geq 2$, $V_1 = V_1 \cap V_2$, i.e., $V_1 \subset V_2$. Hence we may discard V_1 from the collection, so $V = V_2 \cup \ldots \cup V_n$. Thus if we have a collection $V = V_1 \cup \ldots \cup V_n$ such that $V_i \subset \bigcup_{j \neq i} V_j$, then we can simply discard V_i. We can continue to do so and after at most $n - 1$ steps, we will obtain a minimal decomposition.

(4) Suppose

$$V = V_1 \cup \ldots \cup V_m = W_1 \cup \ldots \cup W_n$$

are two minimal decompositions. Then $W_i \subset V_1 \cup \ldots \cup V_m$, so

$$W_i = \bigcup_{j=1}^{m} V_j \cap W_i$$

By part (3), this is a union of affine algebraic sets, so we completely equivalently obtain that $W_i = V_j \cap W_i$ for some j. Hence $W_i \subset V_j$. For each i, let j_i be such that $W_i \subset V_{j_i}$. Repeating this the other way around, we obtain i_k such that $V_k \subset W_{i_k}$. Now $V_k \subset W_{i_k} \subset V_{j_{i_k}}$. So since the decomposition is minimal, we must have $k = j_{i_k}$, so $V_k = W_{i_k}$ for all k. This in particular gives an injective map $\{1, \ldots, m\} \to \{1, \ldots, n\}$, so $m \leq n$. And similarly, $W_i = V_{j_i}$ for all i, so we similarly get $n \leq n$. This implies that $m = n$ and that indeed the decompositions are the same up to reordering, namely by the reordering $\sigma \colon k \mapsto i_k$ giving $V_k = W_{\sigma(k)}$. $\square$

6. Assignment 4

Exercise 6.1 (2)**.** Which of the following modules are flat over the corresponding rings? Justify your answer

(1) $R = \mathbb{C}[x, y]$ and the module is $I = (x, y) \subset R$.
(2) $R = \mathbb{C}[x]/(x^2)$ and the module is $I = (x) \subset R$.
(3) $R = \mathbb{C}[x]$ and the module is the ring $\mathbb{C}[y]$ considered as an R-module by ring homomorphism $\mathbb{C}[x] \to \mathbb{C}[y] : x \mapsto y^2$.
(4) $R = \mathbb{C}[x]$ and the module is the ring $\mathbb{C}[x, y]/(xy)$ considered as an R-module by ring homomorphism $\mathbb{C}[x] \to \mathbb{C}[x, y]/(xy) \colon x \mapsto x$.

Solution. (1) We claim that $I = (x, y)$ is not a flat $R = \mathbb{C}[x, y]$ module. Firstly, $\mathbb{C}[x, y]$ is Noetherian by Hilbert's basis theorem since $\mathbb{C}$ is, and it is also local: we claim that $(x, y) = I$ is precisely the maximal ideal. Firstly, it is maximal because $\mathbb{C}[x, y]/(x, y) \cong \mathbb{C}$ is a field. Now if $M \subset \mathbb{C}[x, y]$ is a maximal ideal, then $1 \notin M$, so for any $f \in M$, we have that $f(x, y) = \sum_{i+j\geq 1} \alpha_{ij} x^i y^j \in (x, y)$. Thus $M \subset (x, y)$, so M is not maximal unless $M = (x, y)$. Therefore (x, y) is the only maximal ideal. Now, I is finitely generated as a $\mathbb{C}[x, y]$-module with generators x and y, hence proposition 9.15 applies. Since (x, y) is not free since it in particular is a proper submodule of R, we have that it is not flat.

(2) We claim that $I = (x) \subset \mathbb{C}[x]/(x^2)$ is indeed flat. This can be seen since $\mathbb{C}[x]/(x^2) = \mathbb{C} \oplus (x) \cong \mathbb{C} \oplus \mathbb{C}$, so since (x) is a direct summand of $R = \mathbb{C}[x]/(x^2)$, it is flat by proposition 9.13 and the fact that R is itself flat by example 9.2.

(3) **I will give two solutions since I'm not sure whether I may use that over a PID, a module is flat iff it is torsion-free** Suppose there is a relation $\sum a_i y^i = 0$ in $\mathbb{C}[y]$ where $a_i \in \mathbb{C}[x]$. However, then taking the maximal degree of x^j in a_j for y^j the maximal degree of y in the relation, we find that $a_j = 0$. But this contradicts y^j being the maximal degree. Hence $a_i = 0$ for all i. But this shows that the relation is trivial. Now remark 9.21 tells us that $\mathbb{C}[y]$ is flat cosidered as a $\mathbb{C}[x]$ module by the homomorphism $\mathbb{C}[x] \to \mathbb{C}[y]$ by $x \mapsto y^2$.

The other solution is the following: Since $R = \mathbb{C}[x]$ is a PID, we immediately find that $\mathbb{C}[y]$ is flat if and only if it is torsion-free considered as a $\mathbb{C}[x]$-module by restriction of scalars along $x \mapsto y^2$. Suppose $f(y) \in \mathbb{C}[y]$ is such that for $g(x) \in R$, $g(x)f(y) = 0$, i.e., $g(y^2)f(y) = 0$ in $\mathbb{C}[y]$. However, this forces f or g to be 0, so we find that $\mathbb{C}[y]$ is torsion-free as a $\mathbb{C}[x]$ module under the ring-homomorphism $x \mapsto y^2$. Thus $\mathbb{C}[y]$ is a flat $\mathbb{C}[x]$-module by the ring homomorphism $\mathbb{C}[x] \to \mathbb{C}[y]$ sending $x \mapsto y^2$.

(4) We note that if a module has torsion, this gives an non-trivial relation since $am = 0$ with $a \neq 0$ and $m \neq 0$ admitting a genuinely trivial reparametrization implies $a = 0$, contradiction. Hence proposition 9.20 gives that if a module has torsion, then it cannot be flat. $\mathbb{C}[x, y]/(xy)$ is clearly not a flat $\mathbb{C}[x]$-module under the homomorphism $\mathbb{C}[x] \to \mathbb{C}[x, y]/(xy)$ sending $x \mapsto x$ since y is nonzero in $\mathbb{C}[x, y]/(xy)$ however, $x \cdot y := xy = 0$, hence $\mathbb{C}[x, y]/(xy)$ is not torsion-free over $\mathbb{C}[x]$.

7. Assignment 5

Exercise 7.1 (1)**.** (2)
We claim that $\mathbb{Z}[x_1, x_2, x_3]$ is a finite extension. Now, clearly, we can express $1, x_1, x_1^2, x_1^3$ as linear combinations over $1, x_1, x_1^2, x_1^3$. Suppose we can express x_1^n as a linear combination of $1, x_1, x_1^2, x_1^3$ for $n = 1, \ldots, N-1$ for some $N \geq 4$. Since

$$\begin{aligned} x^n &= x_1^{n-1}(x_1 + x_2 + x_3) - x_1^{n-1}x_2 - x_1^{n-1}x_3 \\ &= x_1^{n-1}\sigma_1 - x_1^{n-2}\sigma_2 + x_1^{n-2}x_2x_3 \\ &= x_1^{n-1}\sigma_1 - x_1^{n-2}\sigma_2 + x_1^{n-3}\sigma_3 \end{aligned}$$

we find that for $N \geq 4$, x_1^N can be written as a linear combination over x_1^{N-1}, x_1^{N-2} and x_1^{N-3} which by the inductive assumption can be written as linear combinations of $1, x_1, x_1^2, x_1^3$. Hence $\mathbb{Z}[x_1, x_2, x_3]$ is a finite extension over $\mathbb{Z}[\sigma_1, \sigma_2, \sigma_3]$ with

$$\left\{1, x_1, x_1^2, x_1^3, x_2, x_2^2, x_2^3, x_3, x_3^2, x_3^3\right\}$$

as a finite generating set. By proposition 10.11, this also implies that the extension is integral.

(3) We claim that $\mathbb{Z}[x, y]$ is not a finite extension of $\mathbb{Z}[x, xy]$. Suppose $\{g_1, \ldots, g_n\} \in \mathbb{Z}[x, y]$ is a generating set as a module. Let N be the maximal degree of y over $g_1, \ldots, g_n$. Then $y^{N+1} \in \operatorname{span}(g_1, \ldots, g_n)$, so let $y^{N+1} = f_1(x, xy)g_1(x, y) + \ldots + f_n(x, xy)g_n(x, y)$.
Writing each $f_i(x, xy) = \sum \alpha_{i,k,l}x^k(xy)^l$, we see that

$$\begin{aligned} y^{N+1} &= \sum \alpha_{1,k,l}x^k(xy)^l g_1(x, y) + \ldots + \sum \alpha_{n,k,l}x^k(xy)^l g_n(x, y) \\ &= \sum \left(\alpha_{1,k,l}g_1(x, y) + \ldots + \alpha_{n,k,l}g_n(x, y)\right)x^k(xy)^l. \end{aligned}$$

So in particular, we must have that for $(k, l) \neq (0, 0)$,

$$\alpha_{1,k,l}g_1(x, y) + \ldots + \alpha_{n,k,l}g_n(x, y) = 0.$$

But then we get

$$y^{N+1} = \alpha_{1,0,0}g_1(x, y) + \ldots + \alpha_{n,0,0}g_n(x, y)$$

which has maximal y degree N, giving a contradiction. Thus the extension is not finite. However, clearly, it is a finite-type extension, since y together with $\mathbb{Z}[x, xy]$ precisely generate all of $\mathbb{Z}[x, y]$. By proposition 10.11, we then find that $\mathbb{Z}[x, y]$ is not an integral extension.

(7) If the map $\mathbb{C}[x] \hookrightarrow \mathbb{C}[x, y, z] / \left(z^2 - xy\right)$ were integral, proposition 10.6 gives that $\mathbb{C}[x, y] \subset \mathbb{C}[x, y, z] / \left(z^2 - xy\right)$ would be finitely generated as a $\mathbb{C}[x]$-module. Suppose $f_1, \ldots, f_n$ generated $\mathbb{C}[x, y]$ as a $\mathbb{C}[x]$ module in $\mathbb{C}[x, y, z] / \left(z^2 - xy\right)$. If y^N is the maximal degree of y among $f_1, \ldots, f_n$, then $y^{N+1} = \sum g_i f_i$ for $g_i \in \mathbb{C}[x]$. However, there is clearly no way to obtain y^{N+1} in such a way. So the extension is not integral. Since it is clearly finite type, it is also not finite by proposition 10.11.

(9) If $\mathbb{C}[x] \hookrightarrow \mathbb{C}[x, y, z] / \left(z^2 - xy, x^3 - yz\right)$ were integral, z would be integral over $\mathbb{C}[x]$, so there would be some linear combination

$$f_n(x)z^n + \ldots + f_0(x) = 0$$

However, there is not relation converting xz to something different, so if x^{k_n} is the highest term of x in $f_n(x)$, then $x^{k_n}z^n$ is a term that cannot cancel in the above linear combination. So the extension cannot be integral. Hence it can also not be finite.

(10) The extension $\mathbb{C} \hookrightarrow \mathbb{C}[x_1, x_2, x_3, \ldots] / \left(x_1^2, x_2^2, x_3^2, \ldots\right)$ is not finite: suppose it were generated by $f_1, \ldots, f_n \in \mathbb{C}[x_1, x_2, \ldots] / \left(x_1^2, x_2^2, \ldots\right)$, and let m be maximal such that one of the f_i has a term with x_m. Then $x_{m+1} = c_1 f_1 + \ldots + c_n f_n$ with $c_i \in \mathbb{C}$. However, then multiplying both sides by x_{m+1}, we see that each non-zero term in $c_1 f_1 + \ldots + c_n f_n$ must have a x_{m+1}, contradicting maximality of m.

The extension is integral, however, since for any $b \in \mathbb{C}[x_1, x_2, \ldots] / \left(x_1^2, x_2^2, \ldots\right)$, let $x_{i_1}, \ldots, x_{i_k}$ be the x_i which appear in b. Then $b(x_{i_1} \cdots x_{i_k}) = 0 \subset (x_{i_1} \cdots x_{i_k})$, and $(x_{i_1} \cdots x_{i_k})$ is clearly finitely generated, so by proposition 10.6, b is integral over $\mathbb{C}$.

8. Assignment 6

Exercise 8.1 (1)**.** Let R be a Noetherian ring and A be a finitely generated R-algebra. Show that if $B \subset A$ is a subalgebra such that A is a finitely generated B-module, then B is also a finitely generated R-algebra.

Proof. We want to show that B is finitely generated as an R-algebra.

Suppose $\{y_1, \ldots, y_n\} \subset A$ generate A as an R-algebra, so $A = R[y_1, \ldots y_n]$. Since A is also finitely generated as a R-module, there exist $a_1, \ldots, a_m \in A$ such that $A = Ba_1 + \ldots + Ba_m$. Now using the module expression for A, write

$$y_i = \sum_j b_{ij} a_j$$

and similarly, since $a_i a_j \in A$,

$$a_i a_j = \sum_k b_{ijk} a_k.$$

Then given arbitrary $u, v \in A$, we can write

$$u = \sum_{i,j} \alpha_i b_{ij} a_j$$

and

$$v = \sum_{i,j} \beta_i b_{ij} a_j$$

We have then seen that

$$uv = \sum_{i,j,k,l} \alpha_i b_{ij} a_j \beta_k b_{kl} a_l = \sum_{i,j,k,l} (\alpha_i \beta_k)(b_{ij} b_{kl}) \sum_r b_{jlr} a_r = \sum_{i,,k,l,r} (\alpha_i b_k)(b_{ij} b_{kl} b_{jlr}) a_r.$$

This shows that A is generated by $a_1, \ldots, a_n$ as an $D = R[b_{ij}, b_{jlr} \mid j, l = 1, \ldots, n \quad i, r = 1, \ldots, m]$ algebra. In particular, D is Noetherian by corollary 6.15, so A is a Noetherian D-module by applying by theorem 6.11. Hence since B is a natural D-submodule of A it is finitely generated as a D-module, so $B = Db_1 + \ldots + Db_n$. However, this in particular expresses B as the R-algebra $R[b_{ij}, b_{ijk}, b_1, \ldots, b_n \mid i, j, k = 1, \ldots, n]$.

□

Exercise 8.2 (2)**.** Let K be a field and let A be a finitely generated K-algebra. Show that if A is a field, then A is finite-dimensional as a K-vector space. In particular, note that for every maximal ideal $\mathfrak{R} \subset A$, $A/\mathfrak{R}$ is a finite dimensional K-vector space.

Proof. If A is a field extension of K such that A is finite type over K, then by Zariski's lemma, we directly find that A is finite over K - i.e. that it is finitely generated as a K-module, and since K is a field, this is saying that A is finitely generated as a K-vector space. The latter part is corollary 11.7.

□