Commutative algebra and algebraic geometry
Exercises 1

1. A ring is a **principal ideal domain** if it is a domain in which every ideal is principal.

   (a) Show that $\mathbb{Z}$ and $K[X]$ for a field K are both principal ideal domains.
   [Hint: use Euclid's Algorithm for $\mathbb{Z}$ and the Division Algorithm for $K[X]$.]

   (b) Compute all prime ideals for $\mathbb{Z}$ and for $K[X]$.

   (c) Let R be a principal ideal domain, and $I, J, K \lhd R$. Show that

$$(I+J)\cap K = I\cap K + J\cap K \quad \text{and} \quad (I+J)(I\cap J) = IJ.$$

2. Let m be a positive integer, with prime decomposition $m = p_1^{a_1}\cdots p_n^{a_n}$.

   (a) Use the Chinese Remainder Theorem to show that

$$\mathbb{Z}/(m) \cong \prod_i \mathbb{Z}/(p_i^{a_i}).$$

   (b) Recall that an element x in a ring R is called a **unit** provided there exists $y \in R$ with $xy = 1$. The set of units $R^\times$ forms a group under multiplication.
   Show that the group of units of $\mathbb{Z}/(m)$ decomposes as

$$(\mathbb{Z}/(m))^\times \cong \prod_i \big(\mathbb{Z}/(p_i^{a_i})\big)^\times.$$

   (c) Show that the canonical ring homomorphism $\mathbb{Z}/(p^r) \to \mathbb{Z}/(p^{r-1})$ yields a surjective group homomorphism between the groups of units. Compute the kernel.
   Hence prove that if $\phi(m) := |(\mathbb{Z}/(m)^\times|$, then

$$\varphi(p^r) = p^r\big(1-\tfrac{1}{p}\big) \quad \text{and} \quad \varphi(m) = \prod_i \varphi(p_i^{a_i}) = m\prod_i \big(1-\tfrac{1}{p_i}\big).$$

3. A ring homomorphism $f\colon R \to S$ is an **isomorphism** provided there exists a ring homomorphism $g\colon S \to R$ with $gf = \mathrm{id}_R$ and $fg = \mathrm{id}_S$.

   Show that a ring homomorphism f is an isomorphism if and only if it is bijective.

4. (Second Isomorphism Theorem). Let R be a ring, S a subring, and $I \lhd R$ an ideal.

   (a) Show that $S + I$ is a subring of R, and $S \cap I$ is an ideal of S.

   (b) Show that there is an isomorphism $(S+I)/I \cong S/(S\cap I)$.

5. (Third Isomorphism Theorem). Let R be a ring, $I \lhd R$ an ideal, and $\pi\colon R \to R/I$ the canonical ring homomorphism.

   (a) Show that the map $\bar{J} \mapsto \pi^{-1}(\bar{J})$ determines a bijection between ideals of R/I and ideals of R containing I, with inverse $J \mapsto J/I$.

   (b) If $J \lhd R$ contains I, show that there is a ring isomorphism $R/J \cong (R/I)/(J/I)$.

6. Prove Lemma 2.1 from the lectures.

Extra questions

7. A ring R is a **Euclidean domain** if it is a domain and there exists a (Euclidean) function $N\colon R \to \mathbb{N} \cup \{-\infty\}$ such that $N(r) \in \mathbb{N}$ for $r \neq 0$, $N(0) = -\infty$, and for all $x, y \in R$ there exist $q, r \in R$ with $x = qy + r$ and $N(r) < N(y)$.

   (a) Show that every Euclidean domain is a principal ideal domain.
   Conversely, see Bergman's Notes, where it is shown that $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]$ is a principal ideal domain, but not a Euclidean domain.

   (b) Let $w \in \mathbb{Q}[i]$ be a complex number and consider the subring $\mathbb{Z}[w]$. Show that there exists $r > 0$ such that $N(z) := r|z|^2$ takes integer values for all $z \in \mathbb{Z}[w]$.

   (c) Show that $\mathbb{Z}[w]$ is a Euclidean domain (with respect to N) provided that, for each $z \in \mathbb{Q}[i]$, we can find $x, y \in \mathbb{Z}[w]$ with $y \neq 0$ and $N(z - \frac{x}{y}) < 1$.

   (d) Show that this holds for $c = i$, and also for $c = \frac{1}{2}(-1+\sqrt{-3})$.

   (e) What goes wrong for $c = \sqrt{-3}$?

8. Now read the appendix on unique factorisation domains.

   We want to describe all prime ideals of $K[X,Y]$. In fact, we will show that every chain of prime ideals of maximal length has length two and is of the form

   $$(0) \subset (f) \subset M \quad \text{with } f \text{ irreducible and } M \text{ maximal.}$$

   In particular, $K[X,Y]$ has **Krull dimension** 2 (and is **catenary**).

   (a) A prime $P \lhd K[X,Y]$ has **height one** provided it is a minimal non-zero prime; that is, $P \neq 0$ and if $0 \neq Q \subset P$ is prime, then $Q = P$. Show that every height one prime ideal is of the form (f) for some irreducible polynomial $f \in K[X,Y]$.

   (b) Let f be irreducible. Show that (f) is not maximal.
   Hint. Take $g \in K[X]$ irreducible. Show that $K[X,Y]/(g) \cong (K[X]/(g))[Y]$ and that $K[X]/(g)$ is a field. The map $K[X,Y] \to K[X,Y]/(g)$ sends a polynomial $h = h_0 + h_1Y + \cdots + h_nY^n$ with $h_i \in K[X]$ to the polynomial $\bar{h} = \bar{h}_0 + \bar{h}_1Y + \cdots + \bar{h}_nY^n$, where $\bar{h}_i \in K[X]/(g)$. Hence show that $\bar{h}$ is a unit if and only if g divides h_i for all $i \geq 1$, but not h_0.
   Now assume that $f \notin K[X]$ and that (f) is maximal. Consider $\bar{f} \in K[X,Y]/(g)$ as g runs through all irreducible elements of $K[X]$.

   (c) Find some maximal ideals of $\mathbb{R}[X,Y]$ containing $f = X^2 + Y^2 - 1$, or $g = X^2 + Y^2 + 1$, or $h = Y^2 - X^3$.

   (d) Now suppose that $P \neq 0$ is not height one. Show that we can find non-associate irreducible polynomials $f, g \in P$.
   Suppose next that $f, g \notin K[Y]$. By Gauss's Lemma, f, g remain irreducible in $K(Y)[X]$. Show that they are coprime. Deduce that there exist polynomials $a, b \in K[X,Y]$ such that $0 \neq af + bg \in K[Y]$.
   Thus show that there exist irreducible $\alpha, \beta \in P$ with $\alpha \in K[X]$ and $\beta \in K[Y]$.

   (e) Again let $P \neq 0$ be not height one. Taking $\alpha, \beta \in P$ as in the previous part, show that $K[X,Y]/(\alpha, \beta)$ is finite dimensional, and hence that $K[X,Y]/P$ is finite dimensional. Deduce that P is maximal.
   [Hint: for $0 \neq a \in K[X,Y]/P$ show that multiplication by a gives an automorphism of $K[X,Y]/P$, using that $K[X,Y]/P$ is both a domain and finite dimensional over K.]