1 Homework 1.

1. A *Bezout* domain is an integral domain D in which for all $a, b \in D$, there exists $c \in D$ such that
$$\langle a, b \rangle = \langle c \rangle.$$
   (a) Prove that an integral domain D is a Bezout domain if and only if for all $a, b \in D \setminus \{0\}$ there exists $d \in D$ such that
      i. $d|a$ and $d|b$, and
      ii. $d \in \langle a, b \rangle$.

      (Notice that if d satisfies the above properties and d' is another common divisor of a and b, then $d'|d$. So we refer to such a d as a *greatest common divisor* of a and b.)

   (b) Prove that every finitely generated ideal of a Bezout domain is principal.

   (c) Prove that D is a PID if and only if it is both a UFD and a Bezout domain. (**Hint**. In class, we show that every PID is UFD. For the converse, suppose $\mathfrak{a}$ is a non-zero proper ideal. Let $a \in \mathfrak{a}$ be an element with smallest number of irreducible factors. Show that for every $b \in \mathfrak{a}$, $\langle a, b \rangle = \langle a \rangle$.)

2. Let A be a subring of $\mathbb{Q}[x, y]$ which is generated by $x, xy, xy^2, \ldots$; that means
$$A := \mathbb{Q}[x, xy, xy^2, \ldots].$$
   Prove that A is not Noetherian.

   (**Hint.** Consider the chain of ideals
$$\langle x \rangle \subseteq \langle x, xy \rangle \subseteq \langle x, xy, xy^2 \rangle \subseteq \cdots .)$$

3. Let D be a UFD.

   (a) (Rational root criterion) Suppose $a_i \in D$ and $\frac{r}{s}$ is a zero of
$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

where $r, s \in D$ and r and s do not have a common irreducible factor. Prove that $s|a_n$ and $r|a_0$.

(b) (Integrally closed) Prove that a fraction $\frac{r}{s}$ is a zero of a monic polynomial in $D[x]$ if and only if it belongs to D.

(c) Prove that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD.

(**Hint.** Show that $a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0$. Deduce that

$$r|a_0 s^n \quad \text{and} \quad s|a_n r^n.$$

Use factorization into irreducibles and the assumption that r and s do not have a common irreducible factor, and obtain that $r|a_0$ and $s|a_n$. For the last part, notice that $\sqrt{2} = \frac{2\sqrt{2}}{2}$ is a zero of the monic polynomial $x^2 - 2$, but it is not in $\mathbb{Z}[2\sqrt{2}]$.)

4. Let $A := \mathbb{Z} + x\mathbb{Q}[x]$; this means

$$A = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_0 \in \mathbb{Z}, a_1, \ldots, a_n \in \mathbb{Q}, n \in \mathbb{Z}^+\}.$$

(a) Prove that $f(x) \in A$ is irreducible if and only if either $f(x) = \pm p$ where p is a prime integer or $f(x) \in \mathbb{Q}[x]$ is irreducible and $f(0) = \pm 1$.

(b) Prove that x cannot be written as a product of irreducibles in A.

(c) Prove that A is not either a UFD or Noetherian.

5. Suppose A is a unital commutative ring.

(a) Let $\Sigma := \{\mathfrak{a} \trianglelefteq A \mid \mathfrak{a} \text{ is not finitely generated}\}$. Suppose Σ is not empty. Prove that Σ has a maximal element.

(b) Suppose $\mathfrak{p}$ is a maximal element of Σ. Prove that $\mathfrak{p}$ is a prime ideal.

(c) (Cohen) Suppose all the prime ideals of A are finitely generated. Prove that A is Noetherian.

(**Hint.** For the first part use Zorn's lemma. Suppose $\mathfrak{p}$ is a maximal element of Σ and it is not a prime ideal. Argue why $\mathfrak{p}$ is a proper ideal, and deduce that there exist $a, b \in A$ such that $a, b \notin \mathfrak{p}$ and $ab \in \mathfrak{p}$. Deduce that $\mathfrak{p} + \langle a \rangle$ is a finitely generated ideal; say

$$\mathfrak{p} + \langle a \rangle = \langle p_1 + r_1 a, \ldots, p_n + r_n a \rangle$$

for some $p_i \in \mathfrak{p}$ and $r_i \in A$. Let

$$(\langle a \rangle : \mathfrak{p}) := \{x \in A \mid xa \in \mathfrak{p}\}.$$

Notice that this is an ideal and it properly contains $\mathfrak{p}$. Deduce that

$$(\langle a \rangle : \mathfrak{p})$$

is a finitely generated ideal; say

$$(\langle a \rangle : \mathfrak{p}) = \langle s_1, \ldots, s_m \rangle$$

for some $s_i \in A$. Prove that

$$\mathfrak{p} = \langle p_1, \ldots, p_n, s_1 a, \ldots, s_m a \rangle.$$

To this end, first show that the RHS is a subset of the LHS. Next take $x \in \mathfrak{p}$. Argue that there exist $a_1, \ldots, a_n$ such that

$$x = a_1(p_1 + r_1 a) + \cdots + a_n(p_n + r_n a).$$

Deduce that $\sum_{i=1}^n a_i r_i \in (\langle a \rangle : \mathfrak{p})$. Complete the proof.)

6. Suppose $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ is a monic polynomial of degree d. Prove that

$$|(\mathbb{Z}/n\mathbb{Z})[x]/\langle f(x) \rangle| = n^d.$$

(**Hint.** Use long division to show that for every $g(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ there exists a unique polynomial $r(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ of degree at most $d-1$ such that

$$g(x) + \langle f(x) \rangle = r(x) + \langle f(x) \rangle.)$$

7. Suppose $p \in \mathbb{Z}$ is prime. Prove that the following statements are equivalent.

   (a) p is not irreducible in $\mathbb{Z}[i]$.

   (b) There exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.

   (c) $x^2 \equiv -1 \pmod{p}$ has a solution.

(**Hint.** Suppose $p = z_1 z_2$ and z_i's are not unit. Deduce that $|z_i|^2 = p$. Suppose $p = a^2 + b^2$, look at both sides modulo p, argue why b is invertible in $\mathbb{Z}/p\mathbb{Z}$, and deduce that $x^2 + 1$ has a zero in $\mathbb{Z}/p\mathbb{Z}$. Suppose $p | x_0^2 + 1$. Deduce that $p | (x_0 + i)(x_0 - i)$, and obtain that p is not prime. Use the fact that $\mathbb{Z}[i]$ is a PID.)

8. Suppose $p \in \mathbb{Z}$ is prime. Prove that the following statements are equivalent.

   (a) p is not irreducible in $\mathbb{Z}[\omega]$ where $\omega := \frac{-1+i\sqrt{3}}{2}$.

   (b) There exist $a, b \in \mathbb{Z}$ such that $p = a^2 - ab + b^2$.

   (c) $x^2 - x + 1 \equiv 0 \pmod{p}$ has a solution.

   (**Hint.** The same line of argument as in the previous problem.)