1 Homework 1.

1. Suppose A is a unital commutative ring. Prove that

$$A[x]^\times = \{a_0 + a_1x + \cdots + a_nx^n \mid a_0 \in A^\times, a_1, \ldots, a_n \in \mathrm{Nil}(A), n \in \mathbb{Z}^+\}.$$

2. For every ring A, prove that

$$A[x]/\langle x^2 - 2\rangle \simeq \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a, b \in A \right\}.$$

(**Hint**. Send $f(x) \in A[x]$ to $f(\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$ and show that the kernel is $\langle x^2 - 2\rangle$. Here is an alternative approach: for every $f(x) \in A[x]$, by long division, there exists unique $a, b \in A$ and $q(x) \in A[x]$ such that $f(x) = (x^2-2)q(x)+ a+bx$. Deduce that $f(x) + \langle x^2 - 2\rangle = (a + bx) + \langle x^2 - 2\rangle$ for a unique pair of elements $a, b \in A$. Send $a + bx + \langle x^2 - 2\rangle$ to $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$.)

3. Let $\omega := \frac{-1+i\sqrt{3}}{2}$ and

$$\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\}.$$

Convince yourself that $\mathbb{Z}[\omega]$ is a subring of $\mathbb{C}$.

   (a) Let $N(z) := |z|^2$ and check that

   $$N(a + bw) = a^2 - ab + b^2$$

   for every $a, b \in \mathbb{R}$.

   (b) Prove that for every $z_1 \in \mathbb{Z}[\omega]$ and $z_2 \in \mathbb{Z}[\omega] \setminus \{0\}$ there are $q, r \in \mathbb{Z}[\omega]$ such that

   $$z_1 = z_2q + r \quad \text{and} \quad N(r) < N(z_2).$$

   (c) Prove that $\mathbb{Z}[\omega]$ is a Euclidean domain and so it is a PID.

   (d) Prove that $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$.

4. Let n be a square-free integer more than 3. Let

$$\mathbb{Z}[\sqrt{-n}] := \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}\}.$$

(a) Prove that $2, \sqrt{-n}, 1 \pm \sqrt{-n}$ are all irreducible in $\mathbb{Z}[\sqrt{-n}]$.

(b) Find an element of $\mathbb{Z}[\sqrt{-n}]$ which is irreducible but not prime.

(c) Show that $\mathbb{Z}[\sqrt{-n}]$ is not a UFD.

(**Hint**. Use $N(z) := |z|^2$. Notice that 2 is either a divisor of n or $n+1$. Deduce that 2 is not prime.)

5. Suppose A is a unital commutative ring and $\mathfrak{a}$ is an ideal of A. Let

$$\sqrt{\mathfrak{a}} := \{a \in A \mid \exists n \in \mathbb{Z}^+, a^n \in \mathfrak{a}\}.$$

(a) Prove that $\sqrt{\mathfrak{a}}$ is an ideal of A and $\mathrm{Nil}(A/\mathfrak{a}) = \sqrt{\mathfrak{a}}/\mathfrak{a}$.

(b) Let $V(\mathfrak{a})$ be the set of *prime divisors* of $\mathfrak{a}$; that means

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{a} \subseteq \mathfrak{p}\}.$$

Prove that $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}$.

6. 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 $b \in \mathfrak{a}$, $\langle a, b \rangle = \langle a \rangle$.)