1. R is a ring. $x \in R$ is **nilpotent** if there exists $n \in \mathbb{N} \setminus \{0\}$ such that $x^n = 0$. Prove that if $x \in R$ is nilpotent, then $1 - x \in R^\times$.

   Solution: If x is nilpotent, then

   $$(1-x)(1+x+x^2+...+x^{n-1}) = 1-x+x-x^2+...-x^n = 1-x^n = 1$$

   So $1-x$ is a unit.

2. The ring of **Gaussian integers** is the set $\mathbb{Z}[i] = \{a+bi \in \mathbb{C} | a, b \in \mathbb{Z}\}$, with addition and multiplication the same as those in $\mathbb{C}$.

   (i). What are the units in this ring?

   (ii). What are the elements associated to $2+3i$?

   Solution:

   (i). Each element $a+bi \in \mathbb{Z}[i]$ has norm $\sqrt{a^2+b^2}$ as a complex number, and if $a+bi \neq 0$, $|a+bi| = 1$ when $a+bi \in \{\pm 1, \pm i\}$ and $|a+bi| > 1$ otherwise. If $a+bi$ has inverse $c+di$, $(a+bi)(c+di) = 1$, so

   $$|a+bi||c+di| = 1$$

   This happens if and only if $|a+bi| = 1$, i.e. $a+bi \in \{\pm 1, \pm i\}$. We see The units are $\pm 1, \pm i$

   (ii). $2+3i, -2-3i, -3+2i, 3-2i$

3. R is a ring. $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ is a chain of ideals in R. Prove $I = \cup_{i \in \mathbb{N}} I_i$ is an ideal in R.

   Solution: For any $a, b \in \cup_{i \in \mathbb{N}} I_i$, there exists $m, n \in \mathbb{N}$ such that $a \in I_m$ and $b \in I_n$. Without loss of generality, we may assume $m \leq n$, then $I_m \subseteq I_n$, so $a, b \in I_n$, it follows $a+b \in I_n \subseteq \cup_{i \in \mathbb{N}} I_i$.

   For any $r \in R$, $s \in \cup_{i \in \mathbb{N}} I_i$, there exists $k \in \mathbb{N}$ such that $s \in I_k$, so $rs \in I_k \subseteq \cup_{i \in \mathbb{N}} I_i$.

   We conclude $\cup_{i \in \mathbb{N}} I_i$ is an ideal.

4. An ideal I in a ring R is called a **prime ideal** if for any $ab \in I$, either $a \in I$ or $b \in I$.

   (i). $n > 1$, prove $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is a prime.

   (ii). Prove R/I is an integral domain if and only if I is a prime ideal.

   (iii). Prove that every maximal ideal is a prime ideal.

   Solution:

   (i). If p is a prime, $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$ such that $\bar{a} \neq \bar{0}$ and $\bar{b} \neq \bar{0}$, then p doesn't divide a and p doesn't divide b, so p doesn't divide ab, $\overline{ab} \neq \bar{0}$. We see $\mathbb{Z}/p\mathbb{Z}$ is an integral domain.

If $n = ab$ such that $a > 1$ and $b > 1$, then $\bar{a} \neq \bar{0}$ and $\bar{b} \neq \bar{0}$, but $\bar{a}\bar{b} = \bar{n} = \bar{0}$, so $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.

(ii). If R/I is an integral domain, then for any $ab \in I$, $(a+I)(b+I) = ab+I = I$, we have either $a + I = 0 + I$ or $b + I = I$, i.e. $a \in I$ or $b \in I$, so I is a prime ideal.

Conversely, if I is a prime ideal, for any $(a+I)(b+I) = 0+I$, i.e. $ab+I = 0+i$, $ab \in I$, it follows $a \in I$ or $b \in I$, $a + I = 0 + I$ pr $b + I = 0 + I$, we see R/I is an integral domain.

(iii). If I is a maximal ideal of R, then R/I is a field, hence an integral domain, so I is a prime ideal.

5. (i). Prove $\mathbb{F} = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ with addition and multiplication same as those in $\mathbb{R}$ is a field.

   (ii). Prove $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{F}$

   Solution:

   (i). We see addition and multiplication are well-defined on $\mathbb{F}$ since $(a + b\sqrt{2}) + (c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2}$, $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$, they are closed.

   $\mathbb{F}$ with addition forming an abelian group is easy to see.

   Multiplication is associative follows from that in $\mathbb{R}$, and $1 \in \mathbb{F}$.

   The distributive law also follows from that of $\mathbb{R}$.

   We conclude $\mathbb{F}$ is a ring. Next we will check all the nonzero elements are units.

   For any $a + b\sqrt{2} \neq 0$ with $a, b \in \mathbb{Q}$, we see

$$(a + b\sqrt{2})(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}) = (a + b\sqrt{2})\frac{a - b\sqrt{2}}{a^2 - 2b^2} = 1$$

   and note $a^2 \neq 2b^2$ since $a + b\sqrt{2} \neq 0$, so we found the inverse of $a + bi$ in $\mathbb{Q}[\sqrt{2}]$, so $\mathbb{F}$ is a field.

   (ii). Define $F : \mathbb{Q}[x] \longrightarrow \mathbb{R}$ by $F(f) = f(\sqrt{2})$. By Substitution Principle, we know it is a ring homomorphism.

   Note $(\sqrt{2})^2 = 2$, so $(\sqrt{2})^k$ is either a power of 2 or the product of a power of 2 with $\sqrt{2}$, which implies the Image of F is $\mathbb{F}$.

   $\mathbb{Q}$ is a field, so $\mathbb{Q}[x]$ is a Principal Ideal Domain, so $\ker(f)$ is a principal ideal. Note $x^2 - 2 \in \ker(f)$ is a polynomial of lowest degree in $\ker(f)$, so $\ker(f) = (x^2 - 2)$.

   Applying First Isomorphism Theorem for Rings, we get

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}[x]/\ker(f) \cong Im(f) \cong \mathbb{F}$$

6. $\mathbb{F} \subseteq \mathbb{E}$ are fields. $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$ with minimal polynomial $p(x) \in \mathbb{F}[x]$. Prove that $p(x)$ is irreducible.

   Solution: Suppose $p(x)$ is not irreducible, $p(x) = f(x)g(x)$ for some non-constant polynomials $f(x)$ and $g(x)$. Then $f(\alpha)g(\alpha) = p(\alpha) = 0$, and $\mathbb{F}$ is a field, in particular an integral domain, so $f(\alpha) = 0$ or $g(\alpha) = 0$, which contradicts to p being the minimal polynomial of α. We conclude $p(x)$ is irreducible.

7. $f(x) = x^3 + 2x^2 + 4x + 5$. Let $I = (x^2 - 3)$. Determine $a_0, a_1 \in \mathbb{Q}$ such that

   $$f(x) + I = a_0 + a_1 x + I$$

   Solution:

   $$f(x)+I = x^3+2x^2+4x+5+I = x^2(x+2)+4x+5+I = 3(x+2)+4x+5+I = 7x+11+I$$

8. $I = \{p(x) \in \mathbb{Z}[x] | p(0) \in 2\mathbb{Z}\}$. How many elements are there in the quotient ring $\mathbb{Z}[x]/I$?

   Solution: Note that $x \in I$ and $2 \in I$, but $1 \notin I$. Let $p(x) = a_x^n + ... + a_1 x + a_0$, then

   $$p(x) + I = a_x^n + ... + a_1 x + a_0 + I = a_0 + I = \begin{cases} 1 + I, & \text{if } a_0 \text{ is odd} \\ 0 + I, & \text{if } a_0 \text{ is even} \end{cases}$$

   So there are two elements in $\mathbb{Z}[x]/I$.