1. Determine all the ideals in the ring $\mathbb{Z}[x]/(2, x^3+1)$.

First we are going to show that $\mathbb{Z}[x]/(2, x^3+1) \cong \mathbb{F}_2[x]/(x^3+1)$, where $\mathbb{F}_2$ is the field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. (This will simplify the discussion because $\mathbb{F}_2[x]$ is a PID, whereas $\mathbb{Z}[x]$ is not.) Consider the following ring homomorphisms.

$$\begin{array}{ccccc} \mathbb{Z}[x] & \xrightarrow{\mu} & \mathbb{F}_2[x] & \xrightarrow{\eta} & \mathbb{F}_2[x]/(x^3+1) \\ \displaystyle\sum_{i=1}^{n} a_i x^i & \longmapsto & \displaystyle\sum_{i=1}^{n} \overline{a_i} x^i & \longmapsto & \left(\displaystyle\sum_{i=1}^{n} \overline{a_i} x^i\right) + (x^3+1) \end{array}$$

(Here $\overline{a_i}$ is a_i modulo 2.) Let $\varphi : \mathbb{Z}[x] \to \mathbb{F}_2[x]/(x^3+1)$ be the composition $\varphi = \eta \circ \mu$. Notice that $\ker\varphi = (2, x^3-1)$, as follows: Any element in the ideal $(2, x^3+1)$ has form $2g(x) + (x^3+1)h(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$, and it is immediate that $\varphi\big(2g(x) + (x^3+1)h(x)\big) = 0$; Therefore $(2, x^3+1) \subseteq \ker\varphi$. Conversely, $\ker\eta = (x^3+1) \subseteq \mathbb{F}_2[x]$, so μ must send $\ker\varphi$ into the ideal $(x^3+1) \subseteq \mathbb{F}_2[x]$. Now, μ just reduces the coefficients of a polynomial modulo 2, so if $f(x) \in \ker\varphi$, then after the coefficients of $f(x)$ are reduced modulo 2, the resulting polynomial is a multiple of x^3+1. Separating the terms that reduce to 0 into a polynomial $g(x)$, we see that $f(x) = g(x) + (x^3-1)h(x)$, where the coefficients of $g(x)$ are even. Therefore $f(x) = 2g'(x) + (x^3+1)h(x)$, hence $f(x) \in (2, x^3+1)$. Therefore $\ker\varphi \subseteq (2, x^3+1)$.

The above has shown that $\ker\varphi = (2, x^3+1)$, so by the First Isomorphism Theorem we have $\mathbb{Z}[x]/(2, x^3+1) \cong \mathbb{F}_2[x]/(x^3+1)$, as desired. The problem now is to describe all ideals of $\mathbb{F}_2[x]/(x^3+1)$. By the Fourth Isomorphism Theorem, such ideas are in one-to-one correspondence with the ideals in $\mathbb{F}_2[x]$ that contain (x^3+1). Let us turn our attention to those ideals.

Notice that $x^3+1 = (x-1)(x^2+x+1)$ is a factoring of x^3+1 into irreducibles in $\mathbb{F}_2[x]$. It follows that $(x^3+1) \subset (x-1)$ and $(x^3+1) \subset (x^2+x+1)$. What other ideals contain (x^3+1)? Since $\mathbb{F}_2$ is a field, $\mathbb{F}_2[x]$ is a PID, so we are looking for ideals $(f(x))$ for which $(x^3+1) \subseteq (f(x))$. This means $x^3+1 = g(x)f(x)$. Since $\mathbb{F}_2[x]$ is a UFD (it is a PID) and $x^3+1 = (x-1)(x^2+x+1)$ is a prime factoring, it follows that the only choices for $f(x)$ (up to multiplication by a unit) are $f(x) = 1$, $f(x) = x-1$, $f(x) = x^2+x+1$, and $f(x) = (x-1)(x^2+x+1)$. Thus we have only four ideals of $\mathbb{F}_2[x]/(x^3+1)$, and only two of them are proper and nontrivial:

$$\begin{array}{lr} (1)/(x^3+1) = \mathbb{F}_2[x]/(x^3+1) & (x+1)/(x^3+1) \\ ((x+1)(x^2+x+1))/(x^3+1) = 0 & (x^2+x+1)/(x^3+1) \end{array}$$

Transferring this back to $\mathbb{Z}[x]/(2, x^3+1)$, we see that it has only two proper nontrivial ideals:

$$(2, x+1)/(2, x^3+1) \text{ and } (2, x^2+x+1)/(2, x^3+1).$$

2. Construct a field with 9 elements.

Begin with the field $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$, which has three elements. Consider the polynomial ring $\mathbb{F}_3[x]$.

The polynomial $f(x) = x^2+1 \in \mathbb{F}_3[x]$ is irreducible because if it factored into polynomials of lower degree, then the factors would have to be linear, and hence $f(x)$ would have a root in $\mathbb{F}_3$. However, there are no roots, as $f(0) = 1$, $f(1) = 2$ and $f(2) = 2$.

Since x^2+1 is irreducible, the ideal (x^2+1) is maximal in $\mathbb{F}_3[x]$, so $\mathbb{F}_3[x]/(x^2+1)$ is a field.
In this field, $\overline{x^2+1} = \overline{0}$, so $\overline{x^2} = \overline{-1} = \overline{2}$. We will henceforward drop the bars and write this as $x^2 = 2$. Consequently any even power of $x \in \mathbb{F}_3[x]/(x^2+1)$ is constant in $\mathbb{F}_3$, and any odd power of x is a constant multiple of x. Therefore, given any element $g(x)$ of $\mathbb{F}_3[x]/(x^2+1)$, we may assume that $g(x) = ax+b$. There are nine such elements:

$$0, \quad 1, \quad 2, \quad x, \quad 2x, \quad 1+x, \quad 1+2x, \quad 2+x, \quad 2+2x$$

These elements are all distinct, because the difference of any two is a linear, yet the only linear element of the ideal (x^2+1) is zero. Therefore if the difference of two of them belongs to (x^2+1), the two are equal.

We therefore have a field with nine elements. Since $x^2 = 2$, multiplication and addition work as follows:

$$\begin{aligned} (a+bx) + (a'+b'x) &= (a+a') + (b+b')x, \\ (a+bx)(a'+b'x) &= (aa'+2bb') + (ab'+ba')x, \end{aligned}$$

where, of course, $a, a', b, b' \in \mathbb{F}_3$, so the arithmetic is done modulo 3.

3. Let z be a fixed element in the center of a ring R with 1, and let M be a (left) R-module.
Prove: The map $\mu_z : M \to M$ given by $\mu_z(m) = zm$ is an R-module homomorphism.
Prove: If R is commutative, then the map $\varphi : R \to \mathrm{End}_R(M)$ given by $\varphi(r) = \mu_r$ is a ring homomorphism.

Proof. For the first statement, note that given any $m, n \in M$ we have

$$\mu_z(m+n) = z(m+n) = zm + zn = \mu_z(m) + \mu_z(n).$$

Also, for $r \in R$ and $m \in M$ it follows that $\mu_z(rm) = zrm = rzm = r\mu_z(m)$. (Notice that here we needed z in the center, so that it commutes with r.) We have now verified that μ_z is an R-module homomorphism.

Next, suppose R is commutative. Then it is its own center, and, by the above, $\mu_r : M \to M$ is an R-module homomorphism for any $r \in R$. In other words, $\mu_r \in \mathrm{End}_R(M)$ for any r. Therefore we have a well-defined map $\varphi : R \to \mathrm{End}_R(M)$ given by $\varphi(r) = \mu_r$. We need to confirm that this is a ring homomorphism.

First we will show that $\varphi(r+s) = \varphi(r) + \varphi(s)$, that is, we will show that $\mu_{r+s} = \mu_r + \mu_s$. Simply note that $\mu_{r+s}(x) = (r+s)x = rx + sx = \mu_r(x) + \mu_s(x)$. Next we confirm $\varphi(rs) = \varphi(r) \circ \varphi(s)$, which amounts to showing $\mu_{rs} = \mu_r \circ \mu_s$. Simply note that $\mu_{rs}(x) = (rs)x = r(sx) = r\mu_s(x) = \mu_r(\mu_s(x)) = (\mu_r \circ \mu_s)(x)$. ■

4. Prove that if M is a finitely generated R-module that is generated with n elements, then every quotient of M is finitely generated by n or fewer elements.

Proof. Suppose M is generated by elements $m_1, m_2, \ldots, m_n$. Then given any $m \in M$, it follows that $m = \sum_{i=1}^{n} r_i m_i$ for appropriate elements $r_i \in R$. Now let $N \subseteq M$ be a submodule, and consider the quotient M/N. Given any element $m + N$ of this quotient, we have

$$\begin{aligned} m + N &= \left(\sum_{i=1}^{n} r_i m_i\right) + M \\ &= \sum_{i=1}^{n} (r_i m_i + M) \\ &= \sum_{i=1}^{n} r_i(m_i + M). \end{aligned}$$

This means that M/N is generated by the n elements $m_1 + N,\ m_2 + N,\ \ldots,\ m_n + N$. Thus M/N can be generated by n or fewer elements. ■

5. Suppose V is a finite dimensional vector space and $\varphi : V \to V$ is a linear transformation.
Prove that there is an integer m for which $\varphi^m(V) \cap \ker \varphi^m = 0$.

Proof. Observe that for any n we have the following chain of subspaces:

$$\{0\} \subseteq \varphi^{n+1}(V) \subseteq \varphi^n(V) \subseteq \varphi^{n-1}(V) \subseteq \varphi^{n-2}(V) \subseteq \cdots \subseteq \varphi^2(V) \subseteq \varphi(V).$$

Therefore

$$0 \leq \dim \varphi^{n+1}(V) \leq \dim \varphi^n(V) \leq \dim \varphi^{n-1}(V) \leq \cdots \leq \dim \varphi^2(V) \leq \dim \varphi(V).$$

Since V is finite dimensional, it follows that $\dim \varphi^{n+1}(V) = \dim \varphi^n(V)$ for some sufficiently large n. Combining this with $\varphi^{n+1}(V) \subseteq \varphi^n(V)$, it follows that $\varphi^{n+1}(V) = \varphi^n(V)$, that is, $\varphi(\varphi^n(V)) = \varphi^n(V)$.

Thus $\varphi : \varphi^n(V) \to \varphi^n(V)$ is a surjective linear map between spaces of the same dimension, so it (i.e. the restriction of φ to $\varphi^n(V)$) is an isomorphism. Composing it with itself n times gives an isomorphism $\varphi^n : \varphi^n(V) \to \varphi^n(V)$.

Take $x \in \varphi^n(V) \cap \ker \varphi^n$. Then $\varphi^n(x) = 0$ because $x \in \ker \varphi^n$. But also $\varphi^n : \varphi^n(V) \to \varphi^n(V)$ is an isomorphism, so $\varphi^n(x) = 0$ (from the previous sentence) implies $x = 0$. This proves $\varphi^n(V) \cap \ker \varphi^n = 0$. ■