## 1.7 Tutorial 5 Semester I, 2024: Factorization in $\mathbb{Z}$ and $\mathbb{F}[x]$

1. Let $I$ be an ideal of $\mathbb{Z}$. Let $m \in \mathbb{Z}_{>0}$ be minimal such that $m \in I$. Show that $m\mathbb{Z} = I$.
2. Show that if $I$ is an ideal of $\mathbb{Z}$ then there exists $m \in \mathbb{Z}_{>0}$ such that $m\mathbb{Z} = I$.
3. Show that $\mathbb{Z}_{>0}$ indexes the ideals of $\mathbb{Z}$.
4. Show that $p \in \mathbb{Z}_{>0}$ is prime if and only if there does not exist $c \in \mathbb{Z}_{>1}$ such that $p\mathbb{Z} \subsetneq c\mathbb{Z} \subsetneq \mathbb{Z}$.
5. Let $m, n \in \mathbb{Z}_{>0}$. Show that $n$ is divisible by $m$ if and only if $n\mathbb{Z} \subseteq m\mathbb{Z}$.
6. Show that $p \in \mathbb{Z}_{>0}$ is prime if and only if $\mathbb{Z}/p\mathbb{Z}$ is a simple $\mathbb{Z}$-module.
7. Let $m, n, \ell \in \mathbb{Z}_{>0}$ and assume that $m\ell = n$. Show that $\ell$ is prime if and only if $m\mathbb{Z}/n\mathbb{Z}$ is a simple $\mathbb{Z}$-module.
8. Let $n \in \mathbb{Z}_{>1}$. Show that there does not exist an infinite sequence $n > m_1 > m_2 > \cdots > 1$ such that $n\mathbb{Z} \subsetneq m_1\mathbb{Z} \subsetneq m_2\mathbb{Z} \subsetneq \cdots \subsetneq \mathbb{Z}$.
9. Show that if $M$ is a $\mathbb{Z}$-module and $N \subseteq M$ is a $\mathbb{Z}$-submodule of $M$ and $M/N$ is not simple then there exists a $\mathbb{Z}$-module $M'$ such that $N \subsetneq M' \subsetneq M$.
10. Assume that $k \in \mathbb{Z}_{>0}$ and $p_1, \ldots, p_k \in \mathbb{Z}_{>0}$ are prime. Let
$$n = p_1 \cdots p_k, \quad m_1 = p_2 \cdots p_k, \quad \ldots, \quad m_{k-1} = p_k.$$
Show that $n\mathbb{Z} \subsetneq m_1\mathbb{Z} \subsetneq \cdots \subsetneq m_{k-1}\mathbb{Z} \subsetneq \mathbb{Z}$ and that Let $m_0 = n$ and $m_k = 1$. Show that if $j \in \{1 \ldots, k\}$ then $m_j\mathbb{Z}/m_{j-1}\mathbb{Z}$ is a simple $\mathbb{Z}$-module.
11. Let $n \in \mathbb{Z}_{>0}$. Show that there exist $k \in \mathbb{Z}_{>0}$ and primes $p_1, \ldots, p_k \in \mathbb{Z}_{>0}$ such that $n = p_1 \cdots p_k$.
12. (Eisenstein criterion) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and let $p \in \mathbb{Z}_{>0}$ be a prime integer.
Assume that
    (a) $p$ does not divide $a_n$,
    (b) $p$ divides each of $a_{n-1}, a_{n-2}, \ldots, a_0$,
    (c) $p^2$ does not divide $a_0$.

    Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.
13. Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ and let $p$ be a prime integer such that $p$ does not divide $a_n$. Let
$$\begin{array}{rccc} \pi_p\colon & \mathbb{Z}[x] & \to & \mathbb{Z}/p\mathbb{Z}[x] \\ & a_n x^n + \cdots + a_0 & \mapsto & \bar{a}_n x^n + \cdots + \bar{a}_0, \end{array} \qquad \text{where } \bar{a} \text{ denotes } a \bmod p.$$
Show that if $\pi_p\big(f(x)\big)$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$ then $f(x)$ is irreducible in $\mathbb{Q}[x]$.
14. Show that if $f(x) \in \mathbb{Z}[x]$, $\deg\big(f(x)\big) > 0$, and $f(x)$ is irreducible in $\mathbb{Z}[x]$ then $f(x)$ is irreducible in $\mathbb{Q}[x]$.
15. Let $f(x) \in \mathbb{Z}[x]$. Show that $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if
$$\begin{array}{ll} & \text{either } f(x) = \pm p, \text{ where } p \text{ is a prime integer,} \\ \text{or} & f(x) \text{ is a primitive polynomial and } f(x) \text{ is irreducible in } \mathbb{Q}[x]. \end{array}$$