Math 307 Abstract Algebra Homework 10 **Sample solution**

1. Show that every nonzero element of $\mathbb{Z}_n$ is a unit (element with multiplicative inverse) or a zero-divisor.

   Solution. Suppose $k \in \mathbb{Z}_n^*$. If $\gcd(k,n) = 1$, then there is $x, y \in \mathbb{Z}$ such that $kx + ny = 1$. Thus, x is the inverse of k in $\mathbb{Z}_n$. If $\gcd(k,n) = d > 1$. Then $n/d \in \mathbb{Z}_n$ is nonzero such that $k(n/d) = 0 \in \mathbb{Z}_n$ so that k is a zero divisor. The conclusion follows.

2. Show that every nonzero element in $\mathbb{Z}_7[i] = \{a + bi : a, b \in \mathbb{Z}_7\}$ has a multiplicative inverse.

   Solution. Note that in $\mathbb{Z}_7$, $(1^2, 2^2, \ldots, 6^2) = (1, 4, 2, 2, 4, 1)$. Thus, for any nonzero $a + ib \in \mathbb{Z}_7[i]$ we have $a^2 + b^2 \in \{1, 2, 4, 3, 5, 6\}$ and is invertible. Thus, we can always find $(x + iy)$ such that $(a + ib)(x + iy) = 1$ by solving

   $$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ so that } \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (a^2 + b^2)^{-1} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

   (Extra 5 points.) Show that not every nonzero element in $\mathbb{Z}_p[i]$ has a multiplicative inverse for a given prime p.

   Solution. Consider $2 + i \in \mathbb{Z}_5[i]$. One sees that there is no $(x + iy)(2 + i) = 1$, say, by checking all nonzero $x + iy \in \mathbb{Z}_5[i]$.

   (Extra 5 points.) Determine those prime p such that every nonzero element in $\mathbb{Z}_p[i]$ has a multiplicative inverse.

   Solution. From previous discussion, we see that every nonzero element in $\mathbb{Z}_p[i]$ has a multiplicative inverse if and only if $a^2 + b^2$ is invertible for all nonzero $(a, b) \neq (0, 0)$. [What is the condition on this? We will see later that it is equivalent to the condition that $x^2 + 1 = 0$ has no solution in $\mathbb{Z}_p$.

3. (a) Given an example of a commutative ring without zero-divisors that is not an integral domain.

   (b) Find two elements a and b in a ring such that a, b are zero-divisors, $a + b$ is a unit.

   Solution. (a) $2\mathbb{Z}$. (b) $2, 3 \in \mathbb{Z}_6$.

4. (a) Give an example to show that the characteristic of a subring of a ring R may be different from that of R.

   (b) Show that the characteristic of a subdomain of an integral domain D is the same as that of D.

   (a) $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ has unity $(1, 1)$, but the subring $\mathbb{Z} \oplus \{0\}$ has unit $(1, 0)$.

   (b) Suppose D has unit 1, and a subdomain $\hat{D}$ has unity $\hat{1}$. Then $\hat{1}\hat{1} = \hat{1}$ in $\hat{D}$ and $\hat{1}1 = \hat{1}$ in D. So, $\hat{1}(1 - \hat{1}) = 0$ implies that $\hat{1} = 1$.

5. An element a of a ring R is nilpotent if $a^n = 0$ for some $n \in \mathbb{N}$.

   (a) Show that if a and b are nilpotent elements of a commutative ring, then $a + b$ is also nilpotent.

(b) Show that a ring R has no nonzero nilpotent element if and only if 0 is the only solution of $x^2 = 0$ in R.

Solution. (a) Suppose $a^n = 0 = b^m$ with $n, m \in \mathbb{N}$. Because R is commutative, the Binomial theorem applies and

$$(a+b)^{n+m} = \sum_{j=0}^{n+m} \binom{n+m}{j} a^j b^{m+n-j} = 0$$

by the fact that $a^j = 0$ or $b^{n+m-j} = 0$ depending on $j \geq n$ or $j < n$.

(b) If there is a nonzero $x \in R$ satisfies $x^2 = 0$, then x is a nilpotent. If $y \in R$ is a nonzero nilpotent and $k > 1$ is the smallest positive integer such that $y^k = 0$, then $x = y^{k-1}$ satisfies $x^2 = y^{2k-2} = y^k y^{k-2} = 0$.

6. Show that the set S of all nilpotent elements of a communtative ring R is an ideal, i.e., S is a subring satisfying $ax \in S$ for every $a \in S$ and $x \in R$.

   Solution. Let A be the set of nilpotent elements of a commutative ring R. First, $0 \in A$; if $x, y \in A$ so that $x^n = 0 = y^m$, then $(x-y)^{m+n} = 0$ by the same proof as in (a) of the previous question. Thus, $x - y \in A$. Moreover, if $z \in R$, then $(xz)^n = x^n z^n = 0$. So, A is an ideal.

7. Suppose R is a commutative ring with unity and $\mathrm{char} R = p$, where p is a prime. Show that $\phi : R \to R$ defined by $\phi(x) = x^p$ is a ring homomorphism.

   Solution. Note that for $k = 1, \ldots, p-1$, $\binom{p}{k} = p!/(k!(p-k)!)$ is divisible by p. [To see this, note that if $m = p!/(k!(p-k)!)$, then $p! = mk!(p-k)!$ and p cannot be a prime factor of $k!(p-k)!$. So, p is a factor of m.] Thus, $\phi(x+y) = (x+y)^p = \sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j} = x^p + y^p = \phi(x) + \phi(y)$, and $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$. So, ϕ is a ring homomophism.

8. Let R_1 and R_2 be rings, and $\phi : R_1 \to R_2$ be a ring homomorphism such that $\phi(R_1) \neq \{0'\}$, where $0'$ is the additive identity of R_2.

   (a) Show that if R_1 has a unity and R_2 has no zero-divisors, then $\phi(1)$ is a unity of $\phi(R_1)$.

   (b) Show that the conclusion in (a) may fail if R_2 has zero-divisors.

   Solution. (a) Since $\phi(R) \neq \{0'\}$, there is $x \in R$ such that $\phi(x) \neq 0'$. Now for any $z \in R_2$, $\phi(x)\phi(1)z = \phi(x1)z = \phi(x)z$ so that $\phi(1)z = z$ by left cancellation, and $z\phi(1)\phi(x) = z\phi(1x) = z\phi(x)$ so that $z\phi(1) = z$ by right cancellation. Thus, $\phi(1)z = z\phi(1) = z$ for all $z \in R_2$; $\phi(1)$ is the identity in R_2.

   (b) Suppose $\phi : \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}$ such that $\phi(n) = (n, 0)$. Then $\phi(1) = (1, 0)$ is not the unity in $\mathbb{Z} \oplus \mathbb{Z}$.