Math 360 ALGEBRA HOMEWORK 10 SOLUTIONS

Problem 1. Let D be an integral domain. If n is the characteristic of D then $n1 = 0$.

If $n = pq$ for primes p and q, then $(pq)1 = 0$.

Since $(pq)1 = (p1)(q1)$ (why?), we have $(p1)(q1) = 0$. Because D has no zero divisors either $p1 = 0$ or $q1 = 0$. But since p or q are both less than n this is a contradiction with our assumption that n is the characteristic.

Problem 2. $\mathbb{Z}_3[x] = \{a_n x^n + a + n - 1x^{n-1} + \ldots + a_0 | a_i \in \mathbb{Z}_3\}$ is an infinite ring and its characteristic is 3.

Chapter 12 #1. Example of a finite non-commutative ring: Set of $k \times k$ matrices with entries from $\mathbb{Z}_n = Mat(k, \mathbb{Z}_n)$. There are n^{k^2} elements in this ring because there are k^2 entries and n choices for each entry. (multiplication principle!)

Example of an infinite non-commutative ring without unity: Set of $k \times k$ matrices with entries from $2\mathbb{Z} = Mat(k, 2\mathbb{Z})$

Chapter 12 #19. Let R be a ring. Prove that Center of $R = C = \{x \in R | rx = xr \text{ for all } x \in R\}$ is a subring of R.

1. $0 \in C$ so C is non-empty.

2. Let $a, b \in C$. (Need to prove $a - b \in R$).
Let $r \in R$. $r(a - b) = ra - rb = ar - br = (a - b)r$. The first equality holds by distributivity, the second by the assumption that a and b are in the center, and the third by distributivity again. So we get that $a - b$ commutes with any $r \in R$ hence is in the center, proving that C is a subgroup under addition.

3. Let $a, b \in C$. (Need to prove $ab \in R$).
Let $r \in R$. $r(ab) = (ra)b = (ar)b = a(rb) = a(br) = (ab)r$. These equalities hold by associativity of multiplication and our assumption that a and b are in the center. So we get that ab commutes with any $r \in R$ hence is in the center, proving C is closed under multiplication.

Chapter 12 #22. Let R be a group with unity and let $U(R)$ denote the set of units of R. Prove that $U(R)$ is a group under multiplication.

1. $1 \in U(R)$ so $U(R)$ is non-empty.

2. Let $a, b \in U(R)$. Then a and b have multiplicative inverses in R, a^{-1} and b^{-1} respectively. (Need to prove $ab \in U(R)$).

Then $(ab)(b^{-1}a^{-1}) = a(b(b^{-1})a^{-1} = a1a^{-1} = 1$. Similarly $(b^{-1}a^{-1})(ab) = 1$. This proves that $b^{-1}a^{-1}$ is the multiplicative inverse of ab. Hence ab is in $U(R)$.

3. If $a \in U(R)$ then obviously its inverse is also invertible and hence in $U(R)$
The three steps above prove that $U(R)$ is a group under multiplication of R.

Chapter 12 #23. Determine $U(\mathbb{Z}_i)$.
An element $x + yi \in \mathbb{Z}_i$ is invertible iff there exists $a + bi\ \mathbb{Z}_i$ such that $(x + yi)(a + bi) = 1$.
Consider this equation in the bigger ring (in fact field) $\mathbb{C}$. Then the multiplicative inverse of $x + yi$ would be $\frac{1}{x+yi} = \frac{x-yi}{x^2+y^2} = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}i$. Solutions have integer components (as desired) if $\frac{x}{x^2+y^2}$ and $\frac{y}{x^2+y^2}$ ar e both integers. This happens only when $x^2 + y^2 = 1$. So possibilities are: $x = 1, y = 0$, $x = -1, y = 0$, $x = 0, y = 1$, and $x = 0, y = -1$. So invertible elements in $\mathbb{Z}_i$ are $\pm 1, \pm i$.

Chapter 13 #8. Describe all zero-divisors and units of $\mathbb{Z} \otimes \mathbb{Q} \otimes \mathbb{Z}$.

Zero divisors:
An element of the form $(0, r, a)$ with $r \in \mathbb{Q}$ and $a \in \mathbb{Z}$ is a zero divisor because $(0, r, a)(1, 0, 0) = (0, 0, 0)$
An element of the form $(a, 0, b)$ with $a, b \in \mathbb{Z}$ is a zero divisor because $(a, 0, b)(0, 1, 0) = (0, 0, 0)$
An element of the form $(a, r, 0)$ with $r \in \mathbb{Q}$ and $a \in \mathbb{Z}$ is a zero divisor because $(a, r, 0)(0, 0, 1) = (0, 0, 0)$

Units:
$U = \{(a, b, c) \in \mathbb{Z} \otimes \mathbb{Q} \otimes \mathbb{Z} | a = \pm 1, b \neq 0, c = \pm 1\}$. (What is the inverse?)

Chapter 13 #12. Consider 3 and 4 in $\mathbb{Z}_{12}$. Since $3 \times 4 = 0$ in $\mathbb{Z}_{12}$ they are both zero-divisors however 7=3+4 is not zero and not a zero divisor in $\mathbb{Z}_{12}$.

Chapter 13 #14. Let R be a ring with 1 and $N = \{a \in R | a^n = 0 \text{ for some } n \in \mathbb{Z}^+\}$.

1. $0 \in N$ so N is non-empty.

2. Let $a, b \in N$. (Need to prove $a - b \in N$.)
Then there exists $m, n \in \mathbb{Z}^+$ such that $a^n = 1$ and $b^m = 1$.
Then

$$(a - b)^{m+n} = a^{m+n} - \binom{m+n}{1} a^{m+n-1}b + \binom{m+n}{2} a^{m+n-2}b^2 + \dots$$

$$+(-1)^m \binom{m+n}{m+n-m} a^n b^m + (-1)^{m+1} \binom{m+n}{m+n-m-1} a^{n-1}b^{m+1} + \dots$$

$$+(-1)^{m+n-1} \binom{m+n}{m+n-m-n+1} ab^{m+n-1} + (-1)^{m+n} b^{m+n}$$

Notice that each term in the expansion has either a^n or b^m as a factor and hence is zero. Therefore $(a-b)^{m+n} = 0$ and is in N.

3. Let $a, b \in N$ and R be commutative. (Need to prove $ab \in N$.) Let m, n be as in part 2. Then $(ab)^{mn} = a^{mn}b^{mn} = (a^n)^m = (b^m)^n = 0$. So $ab \in N$ and N is closed under multiplciation.

Chapter 13 #18. $1+3i$ and $1+2i$ are in $\mathbb{Z}_5[i]$ and $(1+3i)(1+2i) = -5+5i$ which is 0 in $\mathbb{Z}_5[i]$.

Chapter 13 #22. Let $R = \{f | f : \mathbb{R} \to \mathbb{R} \text{ is a function }\}$
We know R is a commutative ring under function addition and multiplication.

a. Zero divisors of R: $f(x)$ is a zero divisor of R iff $f(x) = 0$ has a solution in $\mathbb{R}$.
Suppose $f(x)$ is a non-zero function and $f(c) = 0$ for some $c \in \mathbb{R}$. Define

$$g(x) = \begin{cases} 0 & \text{if } x \neq c \\ 1 & \text{if } x = c \end{cases}$$

Then $f(x)g(x) = 0$ for all $x \in R$ and neither $f(x)$ nor $g(x)$ is zero.

b. Nilpotent elements of R: The only nilpotent element of R is the function zero because $(f(x))^n = 0$ holds iff $f(x) = 0$

c. Every non-zero element is a zero divisor or a unit: Let $f(x)$ be in R. As discussed in part1 if $f(x) = 0$ for some $x \in R$, then $f(x)$ is a zero divisor. Otherwise we can define the multiplicative inverse of $f(x)$ to be $\frac{1}{f(x)}$.

Chapter 13 #25. Let R be a ring with unity 1 and product of any two non-zero elements is non-zero in R.
If $ab = 1$ then $(ab)a = a$. By associativity of multiplication and cancelation of addition this implies $a(ba) - a = 0$. By distributivity we get $a(ba-1) = 0$. By the assumption on the ring, either $a = 0$ or $ba - 1 = 0$. Since $ab = 1$, a cannot be zero so $ba - 1 = 0$, that is $ba = 1$.

Chapter 13 #38. Let R be a commutative ring and ab be a zero-divisor. Then there exists $x \in R$ such that $x \neq 0$ and $(ab)x = 0$. Then by associativity $a(bx)$=0.
If $bx \neq 0$ then a is a zero-divisor. If $bx = 0$ then b is a zero divisor.
(We need R is commutative because otherwise we would have to distinguish between left zero-divisor and right-zero divisor).