# Homework 4 Solutions

## Ch 12: 1, 2, 9, 22 - 26, 60, 63

**1.** $2 \times 2$ matrices over $\mathbb{Z}_2$ is finite and non-commutative. Since

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ while } \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$2 \times 2$ matrices with entries from $2\mathbb{Z}$ would be an example of infinite, non-commutative with no unit.

**2.** Consider $R = 2\mathbb{Z}_{10} = \{0, 2, 4, 6, 8\}$. 6 is unity since $(5+1)(2m) = 10m + 2m = 2m \bmod 10$ (or by inspection if you prefer). To see that each element is a unit, check $2 \cdot 8 = 6 \bmod 10$, $4 \cdot 4 = 6 \bmod 10$.

**9.** This is sort of a standard type of result you should expect. If $R = \bigcap R_i$ then we need to show closure under operations, but this is trivial since each $R_i$ is closed.

**22.** Let $u, v \in U(R)$, then $(u \cdot v) \cdot (v^{-1} \cdot u^{-1}) = (u(vv^{-1})u^{-1}) = u1u^{-1} = uu^{-1} = 1$, so $v^{-1}u^{-1} = (uv)^{-1}$ and thus $uv$ is a unit if $u$ and $v$ are such. The rest is even simpler.

**23.** Determine $U(\mathbb{Z}[i])$ we need $(a+bi)(c+di) = 1$ so $(ac - bd) = 1$ while $(ad + bc) = 0$. The only units are $\pm 1$ and $\pm i$ are units. That these are the only units can be seen thus

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

so $a + bi \in \mathbb{Z}[i]$ iff $\frac{a}{a^2+b^2}, \frac{b}{a^2+b^2} \in \mathbb{Z}$, for this we must have $a = \pm 1$ and $b = 0$ or $b = \pm 1$ and $a = 0$.

**24.** Show that $U(R_1 \times R_2 \times \cdots \times R_n) = U(R_1) \times U(R_2) \times \cdots \times U(R_n)$.

It would suffice to consider $n = 2$ and use induction. Suppose $(r, s) \in U(R_1 \times R_2)$ so there is $(r', s')$ such that $(r, s)(r', s') = (1, 1)$, but then $(r, s) \in U(R_1) \times U(R_2)$. Essentially the same argument works in the other direction.

**25.** Determine $U(\mathbb{Z}[x])$. Let $p = a + p_1(x)x$ and $q = b + q_1(x)x$ then $pq = (ab + (aq_1(x) + bp_1(x))x + p_1(x)q_1(x)x^2 = 1$ iff $(a, b) = \pm(1, 1)$. So $U(\mathbb{Z}[x]) = U(\mathbb{Z})$.

**26.** Determine $U(\mathbb{R}[x])$. This is like the above, the only $f \in \mathbb{R}[x]$ with a multiplicative inverse is $f = a \in \mathbb{R}^* = U(\mathbb{R})$. So $U(\mathbb{R}[x]) = U(\mathbb{R})$.

**60.** Show that $4x^2 + 6x + 3$ is a unit in $\mathbb{Z}_8[x]$.

$(4x^2 + 6x + 3)(2x + 3) = 8x^3 + 12x^2 + 6x + 12x^2 + 18x + 9 = 8x^2 + 24x^2 + 24x + 9 \bmod 8 = 1$

**63.** $A \in M_2(\mathbb{Z})$ We know $\det(AB) = \det(A)\det(B)$ and so if $AB = I$, then $\det(A)\det(B) = 1$ and as $\det(A), \det(B) \in \mathbb{Z}$ it must be that $\det(A) = \pm 1$.

## Ch 13: 7, 12, 17, 30, 43, 49, 51, 56, 57, 64

**7.** Let $R$ be a finite commutative ring with unity. Show that every $r \in R$ is either a unit or a 0-divisor.

Suppose $r$ is not a zero-divisor. Consider the map $s \mapsto rs$. If $rs = rs'$, then $rs - rs' = r(s - s') = 0$. If $s \neq s'$ for any $s, s' \in R$, then $r$ is a 0-divisor. Else, the map is 1-1 and hence onto, so $rs = 1$ for some $s$. (**A counting argument.**)

Any time you have an integral domain that is not a field you have non-zero-divisor non-unit elements, like 2 in $\mathbb{Z}$.

**Note** This shows that every finite integral domain is a field!

**12.** In $\mathbb{Z}_7$ give interpretations for $1/2$, $-2/3$, $\sqrt{-3}$, and $-1/6$.

$2 \cdot 4 = 1 \bmod 7$ so $4 = 1/2 \bmod 7$.

$1/3 = 5 \bmod 7$ since $3 \cdot 5 = 15 = 1 \bmod 7$ and so $2/3 = 10 = 3 \bmod 7$ and this makes sense as $3 \cdot 3 = 9 = 2 \bmod 7$ and so $-2/3 = -3 = 4 \bmod 7$.

$-3 = 4 \bmod 7$ so $2 = \sqrt{-3} \bmod 7$, that is, $2^2 = 4 = -3 \bmod 7$. What about $-2 = 5 \bmod 7$? $(-2)^2 = 5^2 = 25 = 4 \bmod 7$, do yes, 2 and $-2$ both satisfy $x^2 = -3$.

$1/6 = 6$ since $6 \cdot 6 = 1 \bmod 7$ and so $-1/6 = -6 = 1 \bmod 7$.

All pretty strange:)

**17.** In an integral domain if $a_1 a_2 \cdots a_n = 0$, then for some $i$, $a_i = 0$. So if $r^n = 0$, then $r = 0$.

**30.** $\mathbb{Q}[\sqrt{d}]$ is a field for $d$ an integer. Closure under addition and multiplication are obvious and

$$a + b\sqrt{d} \cdot \frac{a - b\sqrt{d}}{a^2 - b^2 \cdot d} = 1$$

so

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

**43.** Show that $\mathbb{Z}_7[\sqrt{3}]$ is a field. The additive group part is clear essentially being isomorphic to $\mathbb{Z}_7 \times \mathbb{Z}_7$.

The multiplication is $(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}$. This will satisfy all the rules except possibly having inverses, so consider

$$1 = (a + b\sqrt{3}) \left( \frac{a - b\sqrt{3}}{(a + b\sqrt{3})(a - b\sqrt{3})} \right)$$

This will be true if $\mathbb{Z}_7[\sqrt{3}]$ is a field. So the proposed inverse of $a + b\sqrt{3}$ is

$$\left( \frac{a}{a^2 - 3b^2} \right) - \left( \frac{b}{a^2 - 3b^2} \right) \sqrt{3}$$

For this to work we need that $a^2 - 3b^2 \neq 0$ in $\mathbb{Z}_7$ when $a$ and $b$ are not both 0.

Suppose $a^2 = 3b^2 \bmod 7$. In this case we would have $3 = (a/b)^2$, so we can't have $a^2 = 3b^2$ unless 3 is a square in $\mathbb{Z}_7$.

We can just check that $m^2 \bmod 7 \neq 3$ for $m = 0, 1, \ldots, 6$.

This indicates what is needed in general, $\mathbb{Z}_p[\sqrt{k}]$ is a field provided that $k$ is not a square in $\mathbb{Z}_p$.

**49.** Let $x_1, \ldots, x_n$ belong to a ring with prime characteristic $p$. First notice $(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + y^p$. All of the middle terms have a factor of $p$ and hence become 0. Thus $(x+y)^p = x^p + y^p$. Now then $(x+y)^{p^2} = ((x+y)^p)^p = (x^p + y^p)^p = (x^p)^p + (y^p)^p = x^{p^2} + y^{p^2}$, etc. By induction on $m$, $(x+y)^{p^m} = x^{p^m} + y^{p^m}$.

Now $((x_1 + x_2) + x_3)^{p^m} = (x_1 + x_2)^{p^m} + x_3^{p^m} = x_1^{p^m} + x_2^{p^m} + x_3^{p_m}$. So by induction on $k$,

$$(x_1 + \cdots + x_k)^{p^m} = x_1^{p^m} + \cdots + x_k^{p^m}$$

**Questions** Where did we use $p$ is prime? Where did we use commutativity?

This shows we need the "prime" assumption: In $\mathbb{Z}_4$ we have $(1+1)^4 = 2^4 = 0 \neq (1^4 + 1^4) = 2$.

What about the commutativity issue? Consider $M_2(\mathbb{Z}_2)$. Let $x = \left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ and $y = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$, then

$$\begin{aligned} x^2 &= \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] = I \\ y^2 &= \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \\ x^2 + y^2 &= I + I = O \\ x + y &= \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \\ (x+y)^2 &= \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] = I \end{aligned}$$

So $x^2 + y^2 \neq (x+y)^2$.

**51.** Let $F$ be a finite field of character $p$ (we know $p$ is a prime). What we need to see is the $|F| = p^m$ for some $m$. Suppose $q \mid |F|$ for some $q \neq p$, then there is a $g \in F$ with $|g| = q$, that is $qg = g + g + \cdots + g = 0$, but then $g \cdot (q \cdot 1) = 0$ and so $q \cdot 1 = 0$, but then $p \mid q$. So $|F| = p^m$ for some $m$.

**56.** Find all solutions to $x^2 - x + 2$ over $\mathbb{Z}_3[i]$.

We do have $x^2 - x + 2 = x^2 + 2x - 1 = (x+1)^2 - 2 = (x+1)^2 + 1$ so $x = 1 \pm i$. So $x = -1 - i = 2 + 2i$ and $x = -1 + i = 2 + i$ are the two roots.

**57.** Consider $x^2 - 5x + 6 = (x-2)(x-3) = 0$ Find all solutions in $\mathbb{Z}_7$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$, and $\mathbb{Z}_{14}$.

$\mathbb{Z}_7$ is a field so $x = 2$ and $x = 3 \bmod 7$ is the only solution.

In $\mathbb{Z}_8$, notice that $(x-2)(x-3) = (x+6)(x+5)$ so we have

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $x^2 - 5x + 6$ | $6 \cdot 5 = 6$ | $7 \cdot 6 = 2$ | $0 \cdot 7 = 0$ | $1 \cdot 0 = 0$ | $2 \cdot 1 = 2$ | $3 \cdot 2 = 6$ | $4 \cdot 3 = 4$ | $5 \cdot 4 = 4$ |

So in $\mathbb{Z}_8$ we have $2, 3$ as roots.

$\mathbb{Z}_{12} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3$ so we can solve these separately. In $\mathbb{Z}_3$ we have $x^2-5x+6 = x^2+x = (x)(x+1) = (x)(x-2)$ in $\mathbb{Z}_3$ so $x = 0$ and $x = 2$ in $\mathbb{Z}_3$. In $\mathbb{Z}_4$ we have $x^2-5x+6 = x^2+3x+2 = (x+2)(x+1)$ so $x = -2, x = -1$, that is $x = 2$ and $x = 3$. Thus the solutions are $(2,0), (2,2), (3,0), (3,2)$, these correspond to 6, 2, 3, 11 in $\mathbb{Z}_{12}$.

$\mathbb{Z}_{14} \simeq \mathbb{Z}_2 \times \mathbb{Z}_7$ and in $\mathbb{Z}_2$ $x^2 - 5x + 6 = x^2 + x = (x)(x+1) = (x)(x-1)$ so we have $0, 1$ for roots and in $\mathbb{Z}_7$ we have 2 and 3 so we have $(0,2)$, $(0,3)$, $(1,2)$, and $(1,3)$ which corresponds to 2, 3, 9, 10.

**64.** In a finite field $F$ with $|F| = n$, $|F^*| = n-1$ and $x^{|F^*|} = 1$ for all $x \in F^*$. (Since in any group $G$, $g^{|G|} = e$.)