Math 241

Problem Set 11 solution manual

Exercise. A11.1

Lemma 1. $\begin{pmatrix} n \\ i+1 \end{pmatrix} \begin{pmatrix} n \\ i \end{pmatrix} = \begin{pmatrix} n+1 \\ i+1 \end{pmatrix}$.

Proof. $\begin{pmatrix} n \\ i+1 \end{pmatrix} \begin{pmatrix} n \\ i \end{pmatrix} = \frac{n!}{(i+1)!(n-(i+1))!} + \frac{n}{i!(n-i)!} = \frac{n!(n-i)}{(i+1)!(n-i)!} + \frac{n!(i+1)}{(i+1)!(n-i)!} = \frac{(n+1)!}{(i+1)!((n+1)-(i+1))!} = \begin{pmatrix} n+1 \\ i+1 \end{pmatrix}$.

a- We prove the binomial formula by induction:

Base step : for $n = 1$, $(a+b)^1 = a + b = \begin{pmatrix} 1 \\ 0 \end{pmatrix} a^{1-0}b^0 + \begin{pmatrix} 1 \\ 1 \end{pmatrix} a^{1-1}b^1$

So it is true for $n = 1$

Inductive step: Suppose it is true up to n, and let us prove it for $n+1$:

$(a+b)^{n+1} = (a+b)(a+b)^n = (a+b)\sum_{i=1...n} \begin{pmatrix} n \\ i \end{pmatrix} a^{n-i}b^i$

$= \sum_{i=0...n} \begin{pmatrix} n \\ i \end{pmatrix} a^{n-i+1}b^i + \sum_{i=0...n} \begin{pmatrix} n \\ i \end{pmatrix} a^{n-i}b^{i+1}$

$= a^{n+1} + [\sum_{i=1...n} \begin{pmatrix} n \\ i \end{pmatrix} a^{n-i+1}b^i] + [\sum_{i=0...(n-1)} \begin{pmatrix} n \\ i \end{pmatrix} a^{n-i}b^{i+1}] + b^{n+1}$

$= a^{n+1} + [\sum_{i=1...n} \begin{pmatrix} n \\ i \end{pmatrix} a^{n-i+1}b^i] + [\sum_{i=1...(n-1)} \begin{pmatrix} n \\ i-1 \end{pmatrix} a^{n-i+1}b^i] + b^{n+1}$

$= a^{n+1} + [\sum_{i=1...n} (\begin{pmatrix} n \\ i \end{pmatrix} + \begin{pmatrix} n \\ i-1 \end{pmatrix}) a^{n-i+1}b^i] + b^{n+1}$

$= a^{n+1} + [\sum_{i=1...n} \begin{pmatrix} n+1 \\ i \end{pmatrix} a^{n-i+1}b^i] + b^{n+1}$

$= \sum_{i=0...n+1} \begin{pmatrix} n+1 \\ i \end{pmatrix} a^{(n+1)-i}b^i$

b- For non-commutative rings, the binomial formula fails.

$(a+b)^2 = a^2 + ab + ba + b^2$
$(a+b)^3 = (a+b)^2(a+b) = (a^2+ab+ba+b^2)(a+b) = a^3 + a^2b + aba + ab^2 + ba^2 + bab + b^2a + b^3$

Section. 19

Exercise. 9
We first notice that for any element $x \in \mathbb{Z}_3 \times \mathbb{Z}_4$ $x.12 = 0$, but since we know that the order of $(1,1)$ is 12, hence 12 is the smallest such number, and hence the char($\mathbb{Z}_3 \times \mathbb{Z}_4$)=12.

Exercise. 11
Using the binomial formula we get the following:
$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$, but since the ring is of char 4, and since $a^3b, a^2b^2, ab^3 \in R$, we get the following :
$(a+b)^4 = a^4 + (2+4)a^2b^2 + b^4 = a^4 + 2a^2b^2 + b^4 = (a^2+b^2)^2$

Exercise. 14
Consider the element $\begin{bmatrix} 2 & -1 \\ 2 & -1 \end{bmatrix} \in M_2(\mathbb{Z})$, we can easily see that: $\begin{bmatrix} 2 & -1 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, but matrices are non-zero, hence $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a zero divisor.

Exercise. 23

It is easier to note that $a^2 = a \implies a(a-1) = 0 \implies a = 0$ or $a - 1 = 0$ (this only needs an integral domain) $\implies a \in \{0,1\}$.

Exercise. 29

Suppose that char(D)=k, with k neither 0 nor a prime number. Then we can find $m, n \in \mathbb{N} - \{0,1\}$ such that $k = m \cdot n$.
So we get $(m.1)(n.1) = 0$, and hence since D is an integral domain we have either $n.1 = 0$ or $m.1 = 0$. Suppose (WLOG) we have $m.1 = 0$, hence m has the property $m.\alpha = 0\ \forall \alpha \in D$, but since $m < m.n = k$ we get a contradiction to the fact that $char(D) = k$.
Hence $char(D)$ must be either 0 or a prime number.

Section. 20
In the exercises from 11 till 14 we are using theorem 20.12 form the book.

Exercise. 11
$2x \equiv 6 mod(4)$, $GCD(2,4) = 2$, and 2 divides 6, hence the we have 2 solutions for this equation in $\mathbb{Z}_4$, they are $x = 1 + 4\mathbb{Z}$, and $x = 3 + 4\mathbb{Z}$.

Exercise. 12
$22x \equiv 5 mod(15)$, $GCD(22,11) = 1$, and hence we have only one solution for this equation in $\mathbb{Z}_{15}$, and the solution is $5 + 15\mathbb{Z}$.

Exercise. 13
$36x \equiv 15 mod(24)$ but $GCD(36,24) = 12$ and 12 doesn't divide 15, hence we have no solution.

Exercise. 14
$45x \equiv 15 mod(24)$, $GCD(45,24) = 3$, and 3 divides 15, hence we can divide the congruence by 3 to get the equation : $15x \equiv 5 mod(8)$ which is equivalent to $7x \equiv 5 mod(8)$ which is the same as solving $7x = 5$ in $\mathbb{Z}_8$, but 7 is invertible with inverse 7 in $\mathbb{Z}_8$, hence we get $x = 3$ in $\mathbb{Z}_8$, so the solutions for our equation are $3 + 24\mathbb{Z}$, $11 + 24\mathbb{Z}$, and $19 + 24\mathbb{Z}$.

Exercise. 27

For an element a to be its own inverse it must satisfy $a^2 = 1$. SO in $\mathbb{Z}_p$ the only elements that are their own ,multiplicative inverse are the solutions for the equation $x^2 - 1 = 0 \implies (x-1)(x+1) = 0$, but since $\mathbb{Z}_p$ is a field whenever p is prime, this can only happen if $x - 1 = 0$ or $x + 1 = 0$, i.e $x = 1$ or $x = -1 \equiv p - 1 \ mod(p)$. So we deduce that the only elements that are their own multiplicative inverse in $\mathbb{Z}_p$ are 1, $p - 1$.

Section. 21

Exercise. 1
We consider the function $f : F \longrightarrow F' = \{q_1 + q_2 i \mid q_1, q_2 \in \mathbb{Q}\}$, where F is the field of fractions of the integral subdomain $D = \{n + mi \mid n, m \in \mathbb{Z}\}$.

we define $f(n+mi, n'+m'i) = \frac{n+mi}{n'+m'i}$, this is a well defined function since we can write $\frac{n+mi}{n'+m'i} = \frac{nn'+mm'}{n'^2+m'^2} + \frac{mn'-m'n}{n'^2+m'^2}i$, which is an element in F', and this is possible because $(n + mi, n' + m'i) \in F$ implies that $n' + m'i$ is non-zero.

f is surjective since $q_1 + q_2 i = \frac{m}{n} + \frac{a}{b}i = \frac{mb+ani}{nb} = f(mb + ani, nb + 0i)$ where $n, m, a, b \in \mathbb{Z}$.
f is injective since by definition of F we have that $\frac{n+mi}{n'+m'i} = \frac{a+bi}{a'+b'i} \implies (n + mi, n' + m'i) = (a + bi, a' + b'i)$.

Finally we still have to prove that f is a ring homomorphism, to do that let $\alpha_1 = (n + mi, n' + m'i), \alpha_2 = (a + bi, a' + b'i) \in F$ we have to prove that $f(\alpha_1 + \alpha_2) = f(\alpha_1) + f(\alpha_2)$, and that $f(\alpha_1.\alpha_2) = f(\alpha_1.\alpha_2)$, which can be easily done through some calculations.

Hence we can describe the elements of the field F to be all complex numbers with rational components.

Section. 26

Exercise. 12
Let $R = \mathbb{Z}$,then R is an integral domain, it is easy to see that $2\mathbb{Z}$ is an ideal of R with $R/2\mathbb{Z} = \mathbb{Z}_2$ is a field.

Exercise. 13
Also Let $R = \mathbb{Z}$, and consider the ideal $4\mathbb{Z}$, then it is easy to see that $R/4\mathbb{Z}$ has zero divisors.

Exercise. 14
Consider $R = \mathbb{Z} \times \mathbb{Z}$, and let $I = \mathbb{Z} \times \{0\}$, it is easy to see that I is an ideal of R, and $R/I \cong \mathbb{Z}$ which is an integral domain, while R has zero divisors ((0,1).(1,0)=(0,0)).

Exercise. 17
We proved in previous home work that R is ring, and since it is a subset of $\mathbb{R}$, then it is a subring of $\mathbb{R}$. Now let us prove that ϕ an injective homorphism whose image is R', hence we get that R' is a subring of $M_2(\mathbb{R})$.

ϕ is well defined map from R into $M_2(\mathbb{R})$. Let $a + b\sqrt{2}$,and $a' + b'\sqrt{2} \in R'$ then $\phi(a + b\sqrt{2} + a' + b'\sqrt{2}) = \phi(a + a' + (b + b')\sqrt{2}) = \begin{bmatrix} a + a' & 2(b + b') \\ b + b' & a + a' \end{bmatrix} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} a' & 2b' \\ b' & a' \end{bmatrix} = \phi(a + b\sqrt{2}) + \phi(a' + b'\sqrt{2})$.

$\phi((a+b\sqrt{2})(a'+b'\sqrt{2})) = \phi(aa'+2bb'+(ab'+ba')\sqrt{2}) = \begin{bmatrix} aa'+2bb' & 2(ab'+ba') \\ ab'+ba' & aa'+2bb' \end{bmatrix} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} a' & 2b' \\ b' & a' \end{bmatrix} = \phi(a+b\sqrt{2})\phi(a'+b'\sqrt{2})$.

Hence ϕ is a ring homomorphism.

Next suppose $\phi(a+b\sqrt{2}) = 0$, hence $a = b = 0$, hence ϕ is injective.

Finally let $g \in R'$, then $g = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ for some $a, b \in \mathbb{Z}$ so $g = f(a+b\sqrt{2}) \in f(R)$, also $f(\alpha) \in R'$ for all $\alpha \in R$, hence $f(R) = R'$ so we get that R' is a subring, and ϕ is am isomorphism between R and R'.

Exercise. 22

a- We know that $\phi(N)$ is an adidtive subgroup of $\phi(R)$, so we only have to show that for all $r' \in \phi(R)$, we have that $r'\phi(N) \subseteq \phi(N)$, and $\phi(N)r' \subseteq \phi(N)$.

   let $r' \in \phi(R)$ and $y \in \phi(N)$. Then there exists $r \in R$ and $x \in N$ such that $r' = \phi(r)$ and $y = \phi(x)$. but since $x \in N$ and N is an ideal $\implies rx \in N \implies \phi(rx) \in \phi(N), \implies r'y \in \phi(N)$ so $r'\phi(N) \subseteq \phi(N)$. Similarly we can prove that $\phi(N)r' \subseteq \phi(N)$, and hence $\phi(N)$ is an ideal of $\phi(R)$.

b- Let $R = \mathbb{Z}$ and let $R' = \mathbb{R}$, and consider $N = 2\mathbb{Z}$ an ideal of R , and let ϕ be such that $\phi(n) = n$. Then we get $\phi(N) = N$, but then $2\mathbb{Z}$ is not an ideal of $\mathbb{R}$.

c- let N' be an ideal of $\phi(R)$, then let us prove that $\phi^{-1}(N')$ is an ideal of R. We know that $\phi^{-1}(N')$ is an adidtive subgroup of R, so we only have to prove that $r\phi^{-1}(N') \subseteq \phi^{-1}(N')$, and $\phi^{-1}(N')r \subseteq \phi^{-1}(N')$ for all $r \in R$.

   let $r \in R$ and $x \in \phi^{-1}(N')$. We want to show that rx and xr belong to $\phi^{-1}(N')$. Now $x \in \phi^{-1}(N')$ means that $\phi(x) \in N'$. Since N' is an ideal of R', and $\phi(r) \in R'$, we know that $\phi(r)\phi(x)$ and $\phi(x)\phi(r)$ both belong to N'. But then $\phi(rx)$ and $\phi(xr)$ belong to N', which means that rx, $xr \in phi^{-1}(N')$, which is what we wanted to show.

Exercise. 37

First it is easy to see that ϕ is a well defined map between $\mathbb{C}$ and $M_2(\mathbb{R})$. Then let $c_1 = a_1 + b_1 i, c_2 = a_2 + b_2 i \in \mathbb{C}$, then $\phi(c_1 + c_2) = \phi((a_1 + b_1 i) + (a_2 + b_2 i)) = \phi(a_1 + a_2 + (b_1 + b_2)i) = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ -(b_1 + b_2) & a_1 + a_2 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} = \phi(c_1) + \phi(c_2)$, and $\phi(c_1.c_2) = \phi(a_1a_2 - b_1b_2 + (a_1b_2 + a_2b_1)i) = \begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} = \phi(c_1)\phi(c_2)$.

Hence we deduce that ϕ is a ring homomorphism.

Moreover, ϕ is injective since, $\phi(a + bi) = 0 \implies a = b = 0$.

Then ϕ is an isomorphism.