Math 241

Problem Set 13 solution manual

Exercise. A13.1

a- Consider the elements $v_1 = (1, 2, -2)$ and $v_2 = (0, 4, -3)$, it is easy to see that $v_1, v_2 \in G$ and that they are linearly independent.

Then if we prove that they span G we they would form a basis for G. So let $(a, b, c) \in G$ and let we need to write $(a, b, c) = \alpha_1 v_1 + \alpha_2 v_2$. But it is easy to see that for $\alpha_1 = a$ and $\alpha_2 = b + c$ we get that:

$\alpha_1 v_1 + \alpha_2 v_2 = (a, 2a, -2a) + (0, 4(b + c), -3(b + c)) = (a, 2a + 4b + 4c, -2a - 3b - 3c)$ but we know that $(a, b, c) \in G$ hence $2a + 3b + 4c = 0$ which implies that $2a + 4b + 4c = b$, and $-2a - 3b - 3c = c$ so we have our result , and hence we got a basis for G.

b- We have to find a basis for H. First Notice that the smallest positive a we can have is for $a = 1$ and hence we get $b = 2$, $c = -2$.

Then consider $v = (a, b, c) \in H$ $v' = v - a.(1, 2, -2)$ is of the form $(0, b', c') \in H$.

Then we look at $H \cap \{a = 0\}$, let us find the vector who have the smallest positive b' such that $3b' + 4c' \equiv 0 \ mod(12)$, so we get $b' = 4$ and $c' = -3$. The vector $(0, 4, -3) \in H \cap \{a = 0\}$.

Then $v' = (0, b', c') \in H \cap \{a = 0\}$ where $b = 4\beta$, then $v' - \beta(0, 4, -3) = (0, 0, c'') \in H \cap \{a = b = 0\}$.

So now we need to find the smallest positive c'' for $4c'' = 0$, hence $c'' = 0 \ mod(3)$, hence the vector $(0, 0, 3) \in H \cap \{a = b = 0\}$.

It is easy to see that the vectors $\{(1, 2, -2), (0, 4, -3), (0, 0, 3)\}$ are linearly independent. Finally to see that they span H, let $(a, b, c) \in H$ we are required to find α, β, and γ such that $(a, b, c) = \alpha(1, 2, -2) + \beta(0, 4, -3) + \gamma(0, 0, 3)$, then we get $\alpha = a$, and $beta = \frac{b-2a}{4}$ and this is an integer since we know that $2a + 3b + 4c \equiv 0 \ mod(12) \implies 2a - b \equiv 0 \ mod(4)$, and we get $\gamma = \frac{4c+8a+3b-6a}{12} = \frac{2a+3b+4c}{12} \in \mathbb{Z}$.

c- First For $G = < \begin{bmatrix} 1 \\ 2 \\ -2 \end{bmatrix}, \begin{bmatrix} 0 \\ 4 \\ -3 \end{bmatrix} >$. We can choose $v_1 = \begin{bmatrix} 1 \\ 2 \\ -2 \end{bmatrix}$, $v_2 = \begin{bmatrix} 0 \\ 4 \\ -3 \end{bmatrix}$ $v_3 = \begin{bmatrix} 0 \\ -1 \\ 1 \end{bmatrix}$ a basis for $\mathbb{Z}^3$. Let $A = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 4 & -1 \\ -2 & -3 & 1 \end{bmatrix}$ then $det(A) = 1$, and so $A \in GL_3(\mathbb{Z})$, with $A^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 2 & 3 & 4 \end{bmatrix}$

So
$v_1 = e_1 + 2e_2 - 2e_3$
$v_2 = 4e_2 - 3e_3$

$v_3 = -e_2 + e_3$
$\Longrightarrow$
$e_1 = v_1 + 2v_3$
$e_2 = v_2 + 3v_3$
$e_3 = v_2 + 4v_3$

Hence $G/\mathbb{Z}^3 =< v_1, v_2, v_3 > / < v_1, v_2 >\cong< v_3 >\cong \mathbb{Z}$.

As for $H =< \begin{bmatrix} 1 \\ 2 \\ -2 \end{bmatrix}, \begin{bmatrix} 0 \\ 4 \\ -3 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 3 \end{bmatrix}$. We have to find a new basis for $\mathbb{Z}^3$ and H.

Name the elements of the basis of H y_1, y_2, y_3, let v_1, v_2, v_3 a basis for $\mathbb{Z}^3$ be as above. Take a new basis for H $z_1 = y_1$, $z_2 = v_2$, $z_3 = 12v_3 = y_3 - 3y_2$, then $v_1, v_2, 12v_3$ is a basis for H , and hence :

$\mathbb{Z}^3/H =< v_1, v_2, v_3 > / < v_1, v_2, 12v_3 >\cong \mathbb{Z}_{12}$.

Section. 23

Exercise. 34
Notice that $a^p \equiv a \ mod(p)$, for all $a \in \mathbb{Z}_p$, and hence $x^p + a$ always has $-a$ as a solution. So $x^p + a$ is not irreducible for all $a \in \mathbb{Z}_a$.

Exercise. 35

First we notice that since F is a field then $a^n \neq 0$ for all n, and hence $(a^n)^{-1}$ exists. Then since a is a root of $f(x)$ we have that $f(a) = 0 \implies f(a).(a^n)^{-1} = 0 \implies (a_0 + a_1a + ... + a_na^n = 0)(a^n)^{-1} = 0 \implies a_0(a^n)^{-1} + a_1(a^{n-1})^{-1} + ... + a_n = 0$, which implies that $1/a = a^{-1}$ is a root of $a_0x^n + a_1x^{n-1} + ... + a_n$.

Section. 27

Notice that in a finite ring R the maximal ideals are the same as the prime ideals, since suppose I is prime ideal, then R/I is a finite integral domain and hence a maximal ideal.

Exercise. 2
The maximal and prime ideals are $\{0, 2, 4, 6, 8, 10\}$, and $\{0, 3, 6, 9\}$.

Exercise. 4
The maximal and prime ideals are $\{(0, 0), (0, 1), (0, 2), (0, 3)\}$ and $\{(0, 0), (1, 0), (1, 2), (0, 2)\}$.

Exercise. 6
We must find c such that $\mathbb{Z}_3/ < x^3 + x^2 + c >$ is a field which is equivalent to finding c such that $f(x) = x^3 + x^2 + c$ is irreducible.

$f(0) = c$, hence we want $c \neq 0$
$f(1) = 2 + c$, hence we want $c \neq -2 \ mod(3)$
$f(2) = c$
Hence c can only be equal to 2.

Exercise. 18

Notice that $x^2 - 5x + 6 = (x-3)(x-2)$, then $< x^2 - 5x + 6 >$ is not maximal, hence $\mathbb{Q}/ < x^2 - 5x + 6 >$ is not a field.

Exercise. 19

We can either use Eisenstein condition with $p = 2$, or $p = 3$ to find that $x^2 - 6x + 6$ is irreducible , or we can see it directly by noticing that the only roots for this polynomial are $3 - \sqrt{3}$ and $3 + \sqrt{3}$, and hence $< x^2 - 6x + 6 >$ is maximal so $\mathbb{Q}[x]/ < x^2 - 6x + 6 >$ is a field.

Exercise. 24

Let P be a prime ideal of R, then R/P is an integral domain. Since R is finite then R/P is a finite integral domain, and hence P is maximal ideal.

Exercise. 28

Let M be a maximal ideal, and let a, $b \in R$ such that $ab \in M$ with $a \notin M$, we are required to show that $b \in M$.

Consider $I = Ra + M = \{ra + m \mid r \in R, \text{ and } m \in M\}$.(check that I is an ideal)

Then for any $m \in M$, $m = 0.a + m \in I$, hence $M \in I$, but since $a \in I$, and $a \notin M$ we get that I must be equal to R. Hence $1 \in I$, so $1 = ra + m$ multiplying both sides with b we get that $b = rab + mb \in M$. So we deduce that M is prime.

Exercise. 32

It is easy to check that N is an ideal of $F[x]$.

Now we have f and g are of different degrees, and that $N \neq F[x]$. Suppose that f and g both irreducible then since they are also of different degrees their gcd is 1, so we can find $r_1(x), r_2(x)$ such that $1 = r_1(x)f(x) + r_2(x)g(x)$ and hence 1$\in f[x]$ so $N = F[x]$ which is a contradiction.

Exercise. 34

a- We proved before that $A + B$ is an additive group, and it is easy to see that $A + B$ is closed under right and left multiplication by elements in R.

b- For any $s \in A$ $a = a + 0$ and since $0 \in B$ we get that $a \in A + B$, and hence $A \subset A + B$, similarly $B \subset A + B$.

Exercise. 35

a- We know that $A.B$ is an additive group. let $c \in A.B$ then $c = \sum_{i=0...n} a_i b_i$ with $a_i \in A$ $b_i \in B$, then $rc = r \sum_{i=0...n} a_i b_i = \sum_{i=0...n} r a_i b_i = \sum_{i=0...n} (ra_i) b_i$ with $ra_i \in A$, and $b_i \in B$ hence $rc \in A.B$. So $A.B$ is an ideal.

b- Let c be as above, notice that for all i $a_i b_i \in A$ since A is an ideal so $c \in A$ similarly $c \in B$ hence $A.B \subset A \cap B$.

Section. 38

Exercise. 2

It is a basis since :
(1,0)=(3,1)+(-1)(2,1), and (0,1)=3(2,1)+(-2)(3,1), hence $\{(2,1),(3,1)\}$ span $\mathbb{Z} \times \mathbb{Z}$.
Also it is easy to see that they are linearly independent, hence they are a basis of $\mathbb{Z} \times \mathbb{Z}$

Exercise. 3

This is not a basis since any linear combination of these two vectors will give us an even number in the first coordinate, so this set can't span the whole ring $\mathbb{Z} \times \mathbb{Z}$.