Homework 8 solution

1. (a) Let $f(x) = P_1(x) \cdots P_r(x)$, $P_i(x)$ is irreducible
Since $< P_1(x) >$ is a maximal ideal in $F[x]$
Then $\frac{F[x]}{<P_1(x)>}$ is a field
Let $\phi : F \to \frac{F[x]}{<P_1(x)>}$
$F' = \{a + < P_1(x) > | a \in F\}$
Consider in $\frac{F[x]}{<P_1(x)>}$
Let $P_1(x) = a_0 + a_1 x + \cdots + a_t x^t$
$\alpha = x + < P_1(x) > \Rightarrow P_1(\alpha) = 0$

$\square$

(b) Let $f_1(x), f_2(x) \cdots$ be all polynomials in $F[x]$.
Choose $F \subseteq E_1$ such that $f_1(x)$ has a zero in E_1, then $f_2(x) \subseteq E_1$.
Choose $E_1 \subseteq E_2$ such that $f_2(x)$ has a zero in E_2, then $f_3(x) \subseteq E_2$.

$$\vdots$$

Set $E = \bigcup E_i$.
<u>Claim:</u> (1) E is a field. (2)E satisfies desired property.

$\square$

(c) Apply (b).
$\exists E_1 \supseteq F$ such that $\forall f(x) \in F[x]$, $\exists a \in E_1$ such that $f(a) = 0$ (E_1 is a field).
$\exists E_2 \supseteq E_1$ such that $\forall f(x) \in E_1[x]$, $\exists a \in E_2$ such that $f(a) = 0$ (E_2 is a field).

$$\vdots$$

Then $F \subset E_1 \subset E_2 \subset \cdots \subset E_n \subset \cdots$.
Let $E_0 = F$ and $E = \cup_i E_i$
<u>Claim:</u>

(1). E is a field.
(2). $\forall f(x) \in E[x], \exists a \in E$ such that $f(a) = 0$

pf(2):Let $f(x) \in E[x]$ of degree n
$\Rightarrow f(x) = a_0 + a_1 x + \cdots + a_n x^n, a_i \in E$
For each i, assume $a_i \in E_{k_i}$
Find the largest k_i, say "j"
$\Rightarrow a_i \in E_j$ for each i.

$\square$

2. <u>Thought:</u>

$$P_n \cdots P_2 P_1 A Q_1 Q_2 \cdots Q_m = D \text{ where } D = \begin{bmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_n \end{bmatrix}$$

$$A = P_1^{-1} \cdots P_{n-1}^{-1} P_n^{-1} D Q_m^{-1} \cdots Q_1^{-1}$$

WANT: type 1, 2, 3 and extra type are invertible.
Check extra type:
Let a, b and $gcd(a, b) = d$, then $ax + by = d$.
Consider x, y and $gcd(x, y) = 1$, then $sx + ty = 1$.

$$E_1 = \begin{bmatrix} x & -t \\ y & s \end{bmatrix} \quad E_2 = \begin{bmatrix} s & t \\ -y & x \end{bmatrix} \Longrightarrow E_1E_2 = I$$

Denote $P^{-1} = P_1^{-1} \cdots P_n^{-1}$ and $Q^{-1} = Q_m^{-1} \cdots Q_1^{-1}$.
Since A is invertible, $det(A) = 1$ and $det(D) = 1$.

$$1 = det(D) = \prod_{i=1}^{n} d_i \Longrightarrow d_i \neq 0 \text{ and } d_i \text{ are unit } \forall i$$
$$\Longrightarrow D = I_n \text{ (up to unit)}$$

Hence A is a product of elementary matrices of type 1, 2, 3 and extra type.

$$[C_{ij}] \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{bmatrix} = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$$

□

3. $f_1 = (2, 1, 3)$, $f_2 = (1, -1, 2)$

$$A = \begin{bmatrix} 2 & 1 & -3 \\ 1 & -1 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{bmatrix}$$

$$\begin{aligned} \frac{\mathbb{Z}^3}{K} &\cong \frac{\mathbb{Z} \times (1,0,0)}{((1,0,0))} \oplus \frac{\mathbb{Z} \times (0,1,0)}{((0,3,0))} \oplus \frac{\mathbb{Z} \times (0,0,1)}{((0,0,0))} \\ &\cong \mathbb{Z}^3 \oplus \mathbb{Z} \end{aligned}$$

□

4. Use structure theorem

$$\frac{D^3}{K} \cong \frac{\mathbb{Z}[i]}{(1)} \oplus \frac{\mathbb{Z}[i]}{(6)} \oplus \frac{\mathbb{Z}[i]}{(96 - 24i)}$$

$$\begin{bmatrix} f_1 \\ f_2 \\ f_3 \end{bmatrix} = \begin{bmatrix} 1 & 3 & 6 \\ 2+3i & -3i & 12-18i \\ 2-3i & 6+9i & -18i \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix}$$

$$\vdots$$

□

5. Since M_t is a torsion D-submodule of M, M/M_t is torsion-free and finite generated.
Claim: M/M_t is free.
Let $F = M/M_t$ and $u_1, u_2, \cdots, u_k, v_1, v_2, \cdots, v_{n-k}$ be generators of F, where $S = \{u_1, u_2, \cdots, u_k\}$ is a maximal linearly independent subset of these generators. Then

$\{v_i, u_1, \cdots, u_k\}$ is linearly dependent for each v_i, that is, there exist $a_i, r_1, \cdots, r_k \in D$ such that

$$a_i v_i + r_1 u_1 + \cdots + r_k u_k = 0$$

Let $a = a_1 a_2 \cdots a_{n-k}$, then $av_i \in Span(S), \forall 1 \leq i \leq n-k$
Hence $aF := \{av | v \in F\}$ is a D-submodule of $Span(S)$. Since $Span(S)$ is a free D-submodule with basis S, aF is also free.
Define a surjective homomorphism

$$\tau : F \to aF \text{ by } \tau(v) = av \text{ for all } v \in F$$

Since F is torsion-free, τ is also $1-1$. Hence τ is an isomorphism and thus $F \cong aF$. Therefore, F is free. Consider a surjective homomorphism

$$\pi : M \to M/M_t \text{ from } M \text{ onto the free module } M/M_t$$

Let $\mathbb{B}$ be a basis of M/M_t. Note $ker(\pi) = M_t$. For each $b \in \mathbb{B}$, choose one $b^{'} \in M$ with the property that $\pi(b^{'}) = b$. Let $\mathbb{B}^{'} = \{b^{'} \in M | \pi(b^{'}) = b, b \in \mathbb{B}\} \subseteq M$. Note $\mathbb{B}^{'}$ is linearly independent. Hence $Span(\mathbb{B}^{'})$ is a free D-submodule of M with basis $\mathbb{B}^{'}$.
<u>Claim:</u> $M_t \cap Span(\mathbb{B}^{'}) = \{0\}$.

$$\vdots$$

□

6. (a) By Theorem 1.15

$$\{A_i | i \in I\} = \begin{cases} 1. A = \Sigma\{A_i\} \\ 2. A_t \cap A_{t^*} = 0, \forall t \in I \text{ where } A_{t^*} = \Sigma_{i \in I, i \neq t} A_i \end{cases} \Longrightarrow A \cong \Sigma A_i$$

1. M_{p_i} is a M-submodule, $\forall p_i$
   A. $a, b \in M_{p_i} \Rightarrow p^r a = 0$ and $p^s b = 0$, where $r, s \in \mathbb{N}$
   Let $t = max\{r, s\} \Rightarrow p^t(a+b) = 0 \Rightarrow a + b = M_p$
   B. $r \in \mathbf{R}, a \in M_p \Rightarrow p^s a = 0$
   $\therefore p^s ra = r(p^s a) = r0 = 0$
2. Let $0 \neq a \in M$, $O_a = r$ PID $\Rightarrow$ UFD
   $\therefore$ Let $r = p_1^{n_1} \cdots p_k^{n_k}$
   Let $r_i = p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}$
   $i \neq j$ r_i, r_j are relatively prime $\overset{\text{Thm 3.11}}{\Longrightarrow} 1_R = \Sigma s_i r_i$
   $a = a \cdot 1_R = \Sigma s_i r_i a$
   $p_i^{n_i}(s_i r_i a) = s_i r a = 0$
   $\therefore s_i r_i a \in M_{p_i}$

□

(b) Clearly.

□

(c) $|G| < \infty, \forall g \in G$ $|G| \cdot g = \underbrace{g + g + \cdots + g}_{|G|} = 0$

Let $m, n \in \mathbb{Z}$ and $x, y \in G$

$n > 0, nx = \overbrace{x + x + \cdots + x}^{n}$
$n = 0, nx = 0$
$n < 0, nx = \underbrace{(-x) + (-x) + \cdots + (-x)}_{-n}$

i. A. $n > 0$

$$
\begin{aligned}
n(x+y) &= \underbrace{(x+y)+\cdots+(x+y)}_{n} \\
&= \underbrace{x+x+\cdots+x}_{n}+\underbrace{y+y+\cdots+y}_{n} \\
&= nx+ny
\end{aligned}
$$

B. $n = 0$

$$n(x+y) = 0 = 0+0 = nx+ny$$

C. $n < 0$

$$
\begin{aligned}
n(x+y) &= \underbrace{((-x)+(-y))+\cdots+((-x)+(-y))}_{-n} \\
&= \underbrace{(-x)+(-x)+\cdots+(-x)}_{-n}+\underbrace{(-y)+(-y)+\cdots+(-y)}_{-n} \\
&= nx+ny
\end{aligned}
$$

ii. $(n+m)x = nx+mx$

iii. $(mn)x = m(nx)$

$\square$

(d) Method 1: factor decomposition

$$
\begin{aligned}
72 &\longleftrightarrow \mathbb{Z}_{72} \\
2,36 &\longleftrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_{36} \\
3,24 &\longleftrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_{24} \\
6,12 &\longleftrightarrow \mathbb{Z}_6 \oplus \mathbb{Z}_{12} \\
2,2,18 &\longleftrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{18} \\
2,6,6 &\longleftrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6
\end{aligned}
$$

By factor decomposition, there are six finite groups of order 72 up to isomorphism.

Method 2: primary decomposition

$$
\begin{aligned}
72 &= 2^3 \times 3^2 \\
M &= M_2 \oplus M_3 \\
|M_2| &= 8 \to \mathbb{Z}_8, \mathbb{Z}_2 \oplus \mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\
|M_3| &= 9 \to \mathbb{Z}_9, \mathbb{Z}_3 \oplus \mathbb{Z}_3
\end{aligned}
$$

By primary decomposition, there are $3 \times 2 = 6$ finite groups of order 72 up to isomorphism.

$\square$