Exercise sheet 5

1a) $f := X^3 - X^2 - 2X - 8$, $L := \mathbb{Q}(\alpha)$ where α is a root of f

Compute the maximal order using the round-2 algorithm.

Let $G = \mathbb{Z}[\alpha] = \mathbb{Z} \cdot \{1, \alpha, \alpha^2\}$ be the equation order.

$d_G = -2^2 \cdot 503$

Only need to consider $p=2$.

Compute the p-radical.

Choose k such that $p^k \geq n = \dim_{\mathbb{Q}} L$. Here $p=2$, $n=3$

$\rightsquigarrow$ Can choose $k=2$.

Compute $\varphi : G/pG \longrightarrow G/pG$, $x \longmapsto x^4$.

Have to compute 4-th power.

Basis of G/pG is $\{\bar{1}, \bar{\alpha}, \bar{\alpha}^2\}$

$\bar{1}^4 = \bar{1}$

$\bar{\alpha}^4$. First from equation, have $\bar{\alpha}^3 = \bar{\alpha}^2 + 2\bar{\alpha} + 8$

$\rightsquigarrow \bar{\alpha}^4 = \bar{\alpha}^2$ $\qquad = \bar{\alpha}^2 \pmod{2G}$

$\rightsquigarrow \bar{\alpha}^4 = \bar{\alpha} \cdot \bar{\alpha}^2 = \bar{\alpha}^3 = \bar{\alpha}^2$

$(\bar{\alpha}^2)^4 = \bar{\alpha}^8 = (\bar{\alpha}^4)^2 = (\bar{\alpha}^2)^2 = \bar{\alpha}^4 = \bar{\alpha}^2$

So, matrix of φ is

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{(row-form)}$$

$\rightsquigarrow$ Kernel is $\{(0 \ 1 \ +1)\}$, so $\ker \varphi = \langle \bar{\alpha} + \bar{\alpha}^2 \rangle$

Hence, $\operatorname{rad}_p G = G \cdot \{2, \alpha + \alpha^2\} = \mathbb{Z} \cdot \{2, 2\alpha, 2\alpha^2, \alpha + \alpha^2\}$

Write this as matrix:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{(row form)}$$

Now compute HNF:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

$\rightsquigarrow$ Basis of $\mathrm{rad}_p G$ is $\{2, \alpha+\alpha^2, 2\alpha^2\}$

Now, the multiplier Ham basis $\{1, \alpha, \alpha^2\}$ of G and $\{2, \alpha+\alpha^2, 2\alpha^2\}$ of $\mathrm{rad}_2 G$.

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

Multiplication by 2 on basis of G:

$$A_2 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Multiplication by $\alpha+\alpha^2$ on G.

$(\alpha+\alpha^2)\cdot \underline{1} = \alpha+\alpha^2$

$(\alpha+\alpha^2)\cdot\alpha = \alpha^2+\alpha^3 = \alpha^2+\alpha^2+2\alpha+\beta = 2\alpha^2+2\alpha+\beta$

$(\alpha+\alpha^2)\alpha^2 = \alpha^3+\alpha(\alpha^3) = \alpha^2+2\alpha+\beta+\alpha(\alpha^2+2\alpha+\beta)$

$= \alpha^2+2\alpha+\beta+\alpha^3+2\alpha^2+\beta\alpha$

$= \alpha^2+2\alpha+\beta+\alpha^2+2\alpha+\beta+2\alpha^2+\beta\alpha$

$$= 4\alpha^2 + 12\alpha + 16$$

$$\rightsquigarrow A_{\alpha+\alpha^2} = \begin{pmatrix} 0 & 1 & 1 \\ 8 & 2 & 2 \\ 16 & 12 & 4 \end{pmatrix}$$

Multiplication by $2\alpha^2$, ...

$$A_{2\alpha^2} = \begin{pmatrix} 0 & 0 & 2 \\ 16 & 4 & 2 \\ 16 & 20 & 6 \end{pmatrix}$$

Now build B:

$$\left(A_2 \cdot A^{-1}\right)^t = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & -1 & 1 \end{pmatrix}$$

$$\left(A_{\alpha+\alpha^2} \cdot A^{-1}\right) = \begin{pmatrix} 0 & 4 & 8 \\ 1 & 2 & 12 \\ 0 & 0 & -4 \end{pmatrix}$$

$$\left(A_{2\alpha^2} \cdot A^{-1}\right) = \begin{pmatrix} 0 & 8 & 8 \\ 0 & 4 & 20 \\ 1 & -1 & -7 \end{pmatrix}$$

So

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & -1 & 1 \\ 0 & 4 & 8 \\ 1 & 2 & 12 \\ 0 & 0 & -4 \\ 0 & 8 & 8 \\ 0 & 4 & 20 \\ 1 & -1 & -7 \end{pmatrix} \qquad HNF(B) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \\ 0 & & \\ & \vdots & \\ & 0 & \end{pmatrix} \quad :: C$$

$$C^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1/2 \\ 0 & 0 & 1/2 \end{pmatrix} \rightsquigarrow (C^{-1})^t = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1/2 & 1/2 \end{pmatrix}$$

$$\rightsquigarrow \underline{\mathrm{mul}_2 G = \mathbb{Z} \cdot \left\{ 1, \alpha, -\tfrac{1}{2}\alpha + \tfrac{1}{2}\alpha^2 \right\}}$$

Next round:

$$G' := \mathrm{mul}_2 G = \mathbb{Z} \cdot \left\{ 1, \alpha, \frac{\alpha^2 - \alpha}{2} \right\}$$

To compute $\mathrm{rad}_2 G'$ need to consider

$$\varphi : G'/2G' \longrightarrow G'/2G'$$
$$x \longmapsto x^4 \quad , \quad 2^2 \geq n = 3$$

Need to express α^2 in basis of G'. To this end, express in std basis of L and change back basis:

Base change from G' to std basis is

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1/2 & 1/2 \end{pmatrix} \Rightarrow A^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

so α^4 in std basis is $8 + 10\alpha + 3\alpha^2$

Get this in basis of G' by

$$(8 \;\; 10 \;\; 3) \cdot A^{-1} = (8 \;\; 13 \;\; 6),$$

So

$$\alpha^4 = 8 + 13\alpha + 6 \cdot \left(\frac{\alpha^2 - \alpha}{2} \right)$$

$\frac{\alpha^2-\alpha}{2}$ in std basis is $-\frac{1}{2}\alpha + \frac{1}{2}\alpha^2$

Compute $\left(-\frac{1}{2}\alpha + \frac{1}{2}\alpha^2\right)^4 = \frac{1}{2}\left(5\alpha^2 - \alpha + 36\right)$

Get this in basis of G' by

$$\tfrac{1}{2}\begin{pmatrix}36 & -1 & 5\end{pmatrix}\cdot A^{-1} = \begin{pmatrix}18 & 2 & 5\end{pmatrix},$$

so

$$\left(\frac{\alpha^2-\alpha}{2}\right)^4 = 18 + 2\alpha + 5\cdot\left(\frac{\alpha^2-\alpha}{2}\right)$$

So, matrix of φ is

$$\begin{pmatrix}1 & 0 & 0\\ 8 & 13 & 6\\ 18 & 2 & 5\end{pmatrix} \overset{\text{char } 2}{\rightsquigarrow} \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

Kernel is trivial, i.e.

$$\mathrm{rad}_2 G'/2G' = 0$$

$$\left(G' \mathbb{Z}\cdot\left\{\underset{\omega_1}{1}, \underset{\omega_2}{\alpha}, \underset{\omega_3}{\frac{\alpha^2-\alpha}{2}}\right\}\right.$$

$$\Rightarrow \underline{\mathrm{rad}_2 G' = 2G' = \mathbb{Z}\cdot\{2, 2\alpha, \alpha^2-\alpha\}}$$

Matrix for $\mathrm{rad}_2 G'$:

$$A = \begin{pmatrix}2 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 2\end{pmatrix} \quad ; \quad A^{-1} = \tfrac{1}{2}\cdot\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

Mult by 2 on G':

$$A_2 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Mult by 2α:

$2\alpha \cdot 1 = 2\alpha = 2\omega_2$

$2\alpha \cdot \alpha = 2\alpha^2 = -2\omega_2 + 4\omega_3$

$2\alpha \cdot \omega_3 = 8 + 2\omega_2$

so

$$A_{2\alpha} = \begin{pmatrix} 0 & 2 & 0 \\ 0 & -2 & 4 \\ 8 & 2 & 0 \end{pmatrix}$$

Mult by $\alpha^2 - \alpha$:

$(\alpha^2 - \alpha) \cdot \omega_1 = 2\omega_3$

$(\alpha^2 - \alpha)\omega_2 = 8\omega_1 + 2\omega_2$

$(\alpha^2 - \alpha)\omega_3 = -4\omega_1 + 4\omega_2 + 2\omega_3$

$$A_{\alpha^2-\alpha} = \begin{pmatrix} 0 & 0 & 2 \\ 8 & 2 & 0 \\ -4 & 4 & 2 \end{pmatrix}$$

$$(A_2 \cdot A^{-1})^t = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (A_{\alpha+\alpha^2} \cdot A^{-1})^t = \begin{pmatrix} 0 & 4 & -2 \\ 0 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}$$

$$(A_{2\alpha} \cdot A^{-1})^t = \begin{pmatrix} 0 & 0 & 4 \\ 1 & -1 & 1 \\ 0 & 2 & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 4 \\ 1 & -1 & 1 \\ 0 & 2 & 0 \\ 0 & 4 & -2 \\ 0 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix} \sim \mathrm{HNF}(B) = \begin{pmatrix} \boxed{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}} \\ 0 \end{pmatrix} \quad C$$

$\Rightarrow \mathrm{mul}_2 G' = G'$

$\Rightarrow G' = G_2$.

Hence $\underline{G_L = \mathbb{Z} \cdot \left\{1, \alpha, \frac{\alpha^2 - \alpha}{2}\right\}}$.