Idea of the "round-2" algorithm

Suppose we can compute (generators of) $\mathrm{mul}_p(G)$. We then check whether $\mathrm{mul}_p(G) = G$. If so, then $G_p = G$ and we have found the p-maximal overorder. If not, then $\mathrm{mul}_p(G) \supsetneq G$ and we are one step closer to the p-maximal overorder. Repeat this, get G_p after finitely many steps.

Lemma 5.28:

$\mathrm{rad}_p(G)^n \subseteq pG$.

Proof: Since $\mathrm{rad}_p(G) \supseteq pG$, we can consider $I := \mathrm{rad}_p(G)/pG$.

We then get a chain

$$G/pG \supseteq I \supseteq I^2 \supseteq \dots$$

Recall that G/pG is an $\mathbb{F}_p$-vector space of dimension n. The I^i are subspaces. Hence, the chain cannot be infinite, i.e. it must become stationary.

If $I^i = I^{i+1}$, then $I^i = I^j \ \forall j \geq i$. Hence, the chain becomes stationary after at most n steps.

If $\bar{y} \in \mathrm{rad}_p(G)/pG$, there is $k \in \mathbb{N}$ such that $\bar{y}^k = 0$ (because $y^k \in pG$ for some k).

Since G/pG is a f.d. $\mathbb{F}_p$-vector space, it is a finite set.

Hence, also $\mathrm{rad}_p(G)/pG$ is finite, so we can find a single $k \in \mathbb{N}$ such that $\bar{y}^k \in pG$ for all $\bar{y} \in \mathrm{rad}_p(G)/pG$, i.e. $\mathrm{rad}_p(G)^k \subseteq pG \Rightarrow I^k = 0$. Hence, also $I^n = 0 \Rightarrow \mathrm{rad}_p(G)^n \subseteq pG$. $\square$

Proof of Theorem 5.27:

We have $G_p \supseteq \mathrm{mul}_p(G) \supseteq G$.

If $G_p = G$, then $\mathrm{mul}_p(G) = G$.

If $G_p \neq G$ we need to show that $\mathrm{mul}_p(G) \neq G$.

Since $[G_p : G]$ is a power of p by Lemma 5.16 and $[G : \mathrm{rad}_p G]$ is a power of p, so is $[G_p : \mathrm{rad}_p G]$. Hence, there is $l \in \mathbb{N}$ with $p^l \cdot G_p \subseteq \mathrm{rad}_p G$

By Lemma 5.28, have $\mathrm{rad}_p(G)^n \subseteq pG \Rightarrow \mathrm{rad}_p(G)^{n+l} \subseteq (pG)^l \subseteq p^l G$ ②

$\Rightarrow \mathrm{rad}_p(G)^{n+l} \cdot G_p \subseteq p^l G_p \subseteq \mathrm{rad}_p G$.

Let $m \in \mathbb{N}$ be minimal with $\mathrm{rad}_p(G)^m \cdot G_p \subseteq \mathrm{rad}_p(G)$.

Consider two cases.

$\underline{m=1}$: Then $\mathrm{rad}_p(G) \cdot G_p \subseteq \mathrm{rad}_p(G)$, so

$$G_p \subseteq [\mathrm{rad}_p(G)/\mathrm{rad}_p(G)] = \mathrm{mul}_p(G).$$

Since $G_p \supsetneq G$, hence also $\mathrm{mul}_p(G) \supsetneq G$. ✓

$\underline{m>1}$: By minimality of m and since $m>1$, there is $x \in \mathrm{rad}_p(G)^{m-1} \cdot G_p$ with $x \notin \mathrm{rad}_p(G)$.

We claim that $x \in \mathrm{mul}_p(G) \setminus G$, proving that $\mathrm{mul}_p(G) \neq G$.

First, since
$$x \cdot \mathrm{rad}_p(G) \subseteq \mathrm{rad}_p(G)^m \cdot G_p \subseteq \mathrm{rad}_p(G),$$
it follows that $x \in \mathrm{mul}_p(G)$.

Suppose that $x \in G$.

We have $x^2 \in \mathrm{rad}_p(G)^{2m-2} G_p \underset{\substack{\uparrow \\ 2m-2 \geq m}}{\subseteq} \mathrm{rad}_p(G)$.

Hence, there is $j \in \mathbb{N}$ with $pG \ni (x^2)^j = x^{2j}$

$\Rightarrow x \in \mathrm{rad}(pG)$ ↯ to choice of x.

Hence, $x \notin G$. $\square$

We still have to make the round-2 algorithm constructive!

We can translate verything into linear algebra problems over $\mathbb{F}_p$ and $\mathbb{Z}$.

5.7 Computing in orders

Let G be an order with basis $\alpha_1, \dots, \alpha_n$.

To be able to compute in G we need to be able to express sums, products and inverses again in the basis.

Sums is clear.

Products: $\alpha_i \alpha_j = \sum c_{ij}^k \alpha_k$ for $c_{ij}^k \in \mathbb{Z}$, but what are the c_{ij}^k?

Can do the following. Everything lives in $L(\alpha)$, and this has the standard basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. Computing with this basis is easy.

Assume, we can express the α_i in the standard basis (in practice this is usually known). Write this as rows into a matrix $A \in \mathrm{Mat}_n(\mathbb{Q})$, i.e.

$\uparrow$! Because $\mathbb{Z}[\alpha] \neq G_L$ can happen

$$\alpha_i = \sum_j A_{ij} \alpha^j$$

Now, to compute $\alpha_i \alpha_j$, compute this in terms of α^j in the std basis and transform back using $A^{-1} \in \mathrm{Mat}_n(\mathbb{Q})$.

Remark 5.29

Computer algebra systems usually write vectors in rows consider $v \cdot A$, e.g. the kernel of a matrix A is $\{v \mid v \cdot A = 0\}$

We use the same convention in this course.

Example 5.30

Consider $L = \mathbb{Q}(\alpha)$ for α a root of $f = X^3 - X^2 - 2X - 8$.

Let G be the order with basis $\{\underbrace{1}_{=:\omega_1}, \underbrace{\alpha}_{=:\omega_2}, \underbrace{\frac{\alpha^2-\alpha}{2}}_{=:\omega_3}\}$ ← yes, it's integral

What is ω_3^2?

Compute in standard basis

$$\omega_3^2 = \left(\frac{\alpha^2-\alpha}{2}\right)^2 = \frac{1}{4}\left(\alpha^4 - 2\alpha^3 + \alpha^2\right)$$

From f get $\alpha^3 = \alpha^2 + 2\alpha + 8 \Rightarrow \alpha^4 = \alpha^3 + 2\alpha^2 + 8\alpha = (\alpha^2+2\alpha+8) + 2\alpha^2 + 8\alpha$
$= 3\alpha^2 + 10\alpha + 8$

so
$$\omega_3^2 = \frac{1}{4}\left(3\alpha^2 + 10\alpha + 8 - 2(\alpha^2 + 2\alpha + 8) + \alpha^2\right)$$
$$= \frac{1}{4}\left(2\alpha^2 + 6\alpha - 8\right) = \underline{\frac{1}{2}\left(\alpha^2 + 3\alpha - 4\right)}$$

Now transform back:

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

$$\frac{1}{2}\begin{pmatrix} -4 & 3 & 1 \end{pmatrix} \cdot A^{-1} = \begin{pmatrix} -2 & 2 & 1 \end{pmatrix},$$

so $\underline{\omega_3^2 = -2\omega_1 + 2\omega_2 + \omega_3}$.

Computation of inverses can be done similarly by base change to std basis.

5.8 Computing the p-radical

Lemma 5.31

If k is such that $n \leq p^k$, then $\mathrm{rad}_p(G)/pG$ is the kernel of the $\mathbb{F}_p$-vector space map $G/pG \longrightarrow G/pG$, $x \longmapsto x^{p^k}$.

Proof: Suppose $x \in G$ s.t. $\overline{x}^{p^k} = 0 \Rightarrow x^{p^k} \in pG \Rightarrow x \in \mathrm{rad}_p(G) \Rightarrow \overline{x} \in \mathrm{rad}_p(G)/pG$.
Conversely, if $\overline{x} \in \mathrm{rad}_p(G)/pG$, then $\overline{x}^n = 0$ since $\mathrm{rad}_p(G)^n \subseteq pG$ by Lemma 5.28, so $\overline{x}^{p^k} = 0$ since $p^k \geq n$. $\square$

So, to compute $\mathrm{rad}_p(G)$ do the following.

Step 1: Choose $k \in \mathbb{N}$ such that $n \leq p^k$

Step 2: The elements $\overline{\alpha}_1, \dots, \overline{\alpha}_n$ are an $\mathbb{F}_p$-space basis of G/pG.
For each i, compute $\overline{\alpha}_i^{p^k}$ and express in basis (use § 5.6)
Write these vectors as rows into a matrix A.

Step 3: Compute the (right) kernel of A. (linear algebra over $\mathbb{F}_p$!)
$\rightsquigarrow$ Get a $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$-basis $\overline{\beta}_1, \dots, \overline{\beta}_r$ of $\ker A$ in terms of the α_i.

Step 4: Let β_i be representatives of the $\overline{\beta}_i$ (obtained by taking the reps α_i of $\overline{\alpha}_i$)
Then $\mathrm{rad}_p G = pG + \mathbb{Z} \cdot \{\beta_1, \dots, \beta_r\} = \mathbb{Z} \cdot \{p\alpha_1, \dots, p\alpha_n, \beta_1, \dots, \beta_r\}$.

Step 5: Write the $p\alpha_1, \dots, p\alpha_n, \beta_1, \dots, \beta_r$ as rows in a matrix A and compute the HNF B of A.
Then the non-zero rows of B form a basis of $\mathrm{rad}_p G$.