Lemma 6.24

Let M be a free $\mathbb{Z}$-module with basis $b_1,..,b_n$. Let $x=\sum_{i=1}^{n} a_i b_i$.
Let $i\in\{1,..,n\}$. If $\gcd(a_i,..,a_n)=1$, then $b_1,..,b_{i-1},x$ can be supplemented to a basis of M.

Proof:

Let $g=\gcd(a_i,..,a_n)=1$. By Lemma 6.20 there is $T\in GL_{n-i+1}(\mathbb{Z})$ such that $(a_i,..,a_n)T=(1,0,..,0)$.

Let

$$\tilde{T}:=\left(\begin{array}{c|cc} I_{i-1} & \begin{matrix} a_1 \\ \vdots \\ a_{i-1}\end{matrix} & \begin{matrix} 0 & & \\ \vdots & 0 & \\ 0 & & \end{matrix} \\ \hline 0 & \multicolumn{2}{c}{(T^{-1})^t} \end{array}\right)\in GL_n(\mathbb{Z})$$

Then

$$(b_1,...,b_n)\cdot\tilde{T}=\underbrace{(b_1,..,b_i,x,*,*,..,*)}_{\substack{\text{This is a basis since}\\ b_1,..,b_n \text{ is a basis and}\\ \tilde{T}\in GL_n(\mathbb{Z}).}}$$

$\square$

Now, we can come back to:

Proof of Lemma 6.22

Let $b_1,..,b_n$ be a basis of Λ. Let $0\neq x=\sum x_i b_i\in\Lambda$ be a shortest vector, i.e. $\|x\|=\lambda_1(\Lambda)$. Let $g:=\gcd(x_1,..,x_n)$. If $g>1$, then $\frac{1}{g}x\in\Lambda$. But this is shorter than x, so $\lightning$. We must therefor have $g=1$. Now, it follows from Lemma 6.24 that x can be supplemented to a basis.
$\square$

This just makes one basis vector short, however (even though as short as possible).
<u>One</u> starting point to make more vectors short is Gram-Schmidt orthogonalization

Let $b_1, \dots, b_n$ be a basis of Λ. Perform Gram-Schmidt

$$b_1^* := b_1$$

$$b_i^* := b_i - \sum_{j<i} \mu_{ij} b_j^* \quad \text{with} \quad \mu_{ij} := \frac{\langle b_i, b_j^* \rangle}{\| b_j^* \|} \qquad \underline{\text{GSO coefficients}}$$

Then $b_1^*, \dots, b_n^*$ is an orthogonal basis of $\mathbb{R}^n$.

<u>Lemma 6.25</u>

$\| b_i^* \| \leq \| b_i \| \; \forall i$ and $d(\Lambda) \leq \prod_{i=1}^{n} \| b_i \|$ (<u>Hadamard</u> inequality),

with equality iff the b_i are pairwise orthogonal.

<u>Proof</u>: By Gram-Schmidt, there is $Q \in GL_n(\mathbb{Q})$, $\det Q = 1$, with

$$b_i^* = b_i Q \quad \forall i.$$

We have

$$b_i = b_i^* + \sum_{j<i} \mu_{ij} b_j^*,$$

so

$$\| b_i \| = \Big\| b_i^* + \sum_{j<i} \mu_{ij} b_j^* \Big\| \underset{\substack{\text{since the}\\ \text{vectors are}\\ \text{orthogonal}}}{=} \| b_i^* \| + \underbrace{\sum_{j<i} |\mu_{ij}| \| b_j^* \|}_{\substack{=0 \text{ iff the } b_i\text{'s}\\ \text{are orthogonal}}} \geq \| b_i^* \|.$$

Moreover,

$$d(\Lambda)^2 = \det\big((b_i b_j^t)_{i,j} \big) = \underbrace{(\det Q)^2}_{=1} \det\big((b_i^* b_j^{*t}) \big) = \prod_{i=1}^{n} \| b_i^* \|^2.$$

$\square$

Note that the Hadamard inequality relates shortness of basis to orthogonality.

In general, $b_i^* \notin \Lambda$ because the μ_{ij} won't be integral.

But we can do an "integral GSO" which instead of computing b_i^* replaces b_i by $b_i - \sum_{j<i} a_j b_j$ with certain $a_j \in \mathbb{Z}$ by repeating the following:

Assume there is $l < i$ with $|\mu_{ij}| \leq \frac{1}{2} \; \forall l < j < i$ (initially $l = i$, so empty condition).

Then replace b_i by $b_i - \mathrm{round}(\mu_{il}) b_l$.

Such a replacement modifies the GSO coefficients and shortens b_i.
The $\mu_{i,j}$ for $j > \ell$ are not modified because b_j^* is orthogonal to b_ℓ for $\ell < j$. $\mu_{i,\ell}$ is replaced by $\mu_{i,\ell} - \text{round}(\mu_{i,\ell})$, so the new GSO coefficients satisfy $|\mu_{i,j}| \le \frac{1}{2}$ $\forall$ $\ell - 1 < j < i$.

By repeating this process one obtains a basis $b_1, \dots, b_n$ of Λ such that $|\mu_{ij}| \le \frac{1}{2}$ $\forall j < i$. Such a basis is called <u>size reduced</u> (and the process is called <u>size reduction</u>).

Lenstra, Lenstra, and Lovács (<u>LLL</u>) observed in 1982 that combined with a swapping of basis vectors one can efficiently compute a basis of the following type

<u>Def 6.27</u>

A basis $b_1, \dots, b_n$ of a lattice Λ is δ-<u>LLL-reduced</u> for a real parameter $1/4 < \delta < 1$ if

a) the basis is <u>size reduced</u> (i.e. $|\mu_{ij}| \le 1/2$ $\forall i, j$)

b) $(\delta - \mu_{i+1\,i}^2)\|b_i^*\|^2 \le \|b_{i+1}^*\|^2$ $\forall i$ (LLL condition).

Basic algorithm to turn a basis $b_1, \dots, b_n$ of Λ into an LLL basis:

1. Size reduce the basis
2. If there is i for which the LLL condition does not hold, i.e. $(\delta - \mu_{i+1,i}^2)\|b_i^*\|^2 > \|b_{i+1}^*\|^2$, then swap b_i and b_{i+1}, and go back to <u>1</u>.

It is clear that if this terminates, the basis is LLL reduced.
One can show that it indeed terminates.

If the basis is LLL reduced, then, as $|\mu_{i,i+1}| \le \frac{1}{2}$ we have

$$\|b_i^*\|^2 \le \alpha \|b_{i+1}^*\|^2, \quad \alpha = \frac{1}{\delta - \frac{1}{4}} \quad \text{(e.g. for } \delta = 3/4 \text{ we have } \alpha = 2\text{)}$$

so, by repeated application:

$$\|b_1^*\|^2 \leq \alpha^{i-1}\|b_i^*\|^2 \leq \alpha^{n-1}\|b_n^*\|^2$$

Since $b_1 = b_1^*$, it follows that

$$\|b_1\| \leq \alpha^{(n-1)/2} \min \|b_i^*\|^2 \leq \alpha^{(n-1)/2} \lambda_1(\Lambda)$$

More generally

<u>Lemma 6.29</u>

If $b_1, \ldots, b_n$ is LLL reduced then $\|b_i\| \leq \alpha^{(n-1)/2} \lambda_i(\Lambda) \ \forall i$

<u>Proof:</u>

See exercises. $\square$

Hence, the lengths of the vectors of an LLL reduced basis are not too far from the successive minima in a precise sense.

7. Units

Let L be a number field. The units of an order $\mathcal{O}$ in L form an abelian group $\mathcal{O}^*$ (subgroup of L^*). We want to investigate the structure of this group.
As in §6.4 we denote the complex embeddings $L \to \mathbb{C}$ by

$$\underbrace{\sigma_1, \dots, \sigma_r}_{\text{real embeddings}}, \sigma_{r+1}, \dots, \sigma_{r+s}, \sigma_{r+1+s} = \overline{\sigma_{r+1}}, \dots, \sigma_{r+2s} = \overline{\sigma_{r+s}}$$

7.1 Torsion units

Prop 7.1
Let $\mathcal{O}$ be an order and let $\alpha \in \mathcal{O}$. The following are equivalent:
a) $\alpha^k = 1$ for some $k > 0$ (i.e. α is torsion element of $\mathcal{O}^*$)
b) $|\sigma_i(\alpha)| = 1 \;\forall i$
c) $\langle j(\alpha), j(\alpha)\rangle = n$ (j the Minkowski map, $n = \dim L$).

Such elements are called torsion units of $\mathcal{O}$. There are just finitely many and they form a cyclic subgroup $TU(\mathcal{O})$ of $\mathcal{O}^*$.

Proof:
Let $\sigma : L \to \mathbb{C}$ be an embedding. Then

$$\alpha^k = 1 \Rightarrow \sigma(\alpha)^k = 1$$

$$\Rightarrow \sigma(\alpha) = e^{2\pi i \ell/k} \text{ is a } k\text{-th root of unity}$$

$$\Rightarrow |\sigma(\alpha)| = 1$$

$$\Rightarrow \langle j(\alpha), j(\alpha)\rangle = n.$$

This proves $a \Rightarrow b \Rightarrow c$. Since $j(\mathcal{O}_L) \subset \mathbb{R}^n$ is a lattice, it follows from Cor 6.17 that there are only finitely many $\alpha \in \mathcal{O}_L$ with $\langle j(\alpha), j(\alpha)\rangle \le n$.
Assume now, $\alpha \in \mathcal{O}_L$ with $\langle j(\alpha), j(\alpha)\rangle = n$. Then

$$n = \langle j(\alpha), j(\alpha)\rangle = \langle j_{\mathbb{C}}(\alpha), j_{\mathbb{C}}(\alpha)\rangle = \sum_{i=1}^{n} |\sigma_i(\alpha)|^2$$

$$\Rightarrow 1 = \frac{1}{n}\sum_{i=1}^{n} |\sigma_i(\alpha)|^2$$

In Lemma 6.16 we have proven that

$$|N_{L|\mathbb{Q}}(\alpha)| \leq \left(\frac{1}{n} \langle j(\alpha), j(\alpha)\rangle\right)^{n/2}$$

Hence, our assumption implies $|N_{L|\mathbb{Q}}(\alpha)| \leq 1$. On the other hand, α is non-zero and integral, hence $N_{L|\mathbb{Q}}(\alpha)$ is a non-zero integer.

$$\Rightarrow 1 = |N_{L|\mathbb{Q}}(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)|^2$$

$$\Rightarrow \sqrt[n]{\prod_{i=1}^{n} |\sigma_i(\alpha)|^2} = 1 = \frac{1}{n}\sum_{i=1}^{n} |\sigma_i(\alpha)|^2$$

This is the geometric and the arithmetic mean of $|\sigma_i(\alpha)|^2$. They are equal iff their parts are equal, hence

$$|\sigma_1(\alpha)|^2 = |\sigma_2(\alpha)|^2 = \dots = |\sigma_n(\alpha)|^2$$

Hence, $|\sigma_i(\alpha)|^2 = 1 \Rightarrow |\sigma_i(\alpha)| = 1 \;\forall i$. This proves $c \Rightarrow b$.

For any $k \in \mathbb{N}_{>0}$ we then have

$$|\sigma_i(\alpha^k)| = |\sigma_i(\alpha)^k| = |\sigma_i(\alpha)|^k = 1$$

$$\Rightarrow \langle j(\alpha^k), j(\alpha^k)\rangle = n$$

$$\Rightarrow \{\alpha^k \mid k \in \mathbb{N}_{>0}\} \text{ is finite by Cor 6.17}$$

$$\Rightarrow \exists l: \alpha^k = \alpha^l \underset{\substack{\text{wlog} \\ k \geq l}}{\Rightarrow} \alpha^{k-l} = 1.$$ This proves $b \Rightarrow a$.

We have proven that the torsion units form a finite subgroup $TU(G)$ of L^*

$$\overset{\text{Exercise 8.4}}{\Longrightarrow} TU(G) \text{ is cyclic.} \qquad \square$$

We can explicitly compute $TU(G)$ by finding all elements in the Minkowski lattice of G whose squared norm is equal to n (see §6.5).