Lecture 8, 20.11.

Another really useful fact:

Cor 4.11: Let V be a f.g. free $\mathbb{Z}$-module and $U \subseteq V$ a submodule of the same rank. Then V/U is finite and

$$[V:U] := |V/U| = |\det(A)|,$$ where A is the matrix of $U \hookrightarrow V$ in some bases of U and V

Proof:

By Smith normal form there are $\mathcal{U}, \mathcal{V}$ s.t. $\mathcal{U} A \mathcal{V} = \begin{pmatrix} D_r & \\ & 0 \end{pmatrix}$, Smith normal form, $D_r = \mathrm{diag}(s_1, \ldots, s_r)$.

Then
$$V/U \simeq \bigoplus_{i=1}^{r} \mathbb{Z}/(s_i) \Rightarrow |V/U| = \prod_{i=1}^{r} s_i.$$

Also, since $\mathcal{U}, \mathcal{V} \in GL(\mathbb{Z}) \rightsquigarrow \det(\mathcal{U}), \det(\mathcal{V}) = \pm 1$, so

$$|\det(A)| = |\det(\mathcal{U}) \det(A) \det(\mathcal{V})| = \prod_{i=1}^{r} s_i. \qquad \square$$

5. Finding an integral basis

Throughout, L a number field, $n = \dim_{\mathbb{Q}} L$.

5.1 Orders, discriminants, a sufficient condition

Lemma 5.1: $L = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_L$.

Proof:

Know from Lemma 3.31: every $\alpha \in L$ is of the form $\alpha = \frac{s}{r}$ with $s \in \mathcal{O}_L$ and $r \in \mathbb{Z}$. $\rightsquigarrow L = \mathbb{Q} \cdot \mathcal{O}_L$. Hence, if $\mathcal{O}_L = \mathbb{Z} \cdot \{\alpha_1, \dots, \alpha_n\}$, then $L = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$. By the proof of the primitive element theorem, can replace α_1, α_2 by $\alpha_{12} = \alpha_1 + c\alpha_2$ for $c \in \mathbb{Q}$ away from finitely many numbers. Can thus choose $c \in \mathbb{Z} \rightsquigarrow \alpha_{12} \in \mathcal{O}_L$. Inductively, $L = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_L$.

$\square$

So, assume from now on that

$$L = \mathbb{Q}(\alpha), \quad \alpha \in \mathcal{O}_L.$$

Then $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$!

Note: $\mathbb{Z}[\alpha]$ has $\mathbb{Z}$-basis $1, \alpha, \dots, \alpha^{n-1} \Rightarrow \dim_{\mathbb{Z}} \mathbb{Z}[\alpha] = n = \dim_{\mathbb{Z}} \mathcal{O}_L$

Is $\mathbb{Z}[\alpha] = \mathcal{O}_L$?? Would be excellent!

But: not true in general, see Exercise 4.2.

How far away are we? By Cor 4.11, $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$ is finite.

Let's look at this closer.

<u>Def</u> 5.2: An <u>order</u> in L is a subring $\mathcal{O}$ of L which is a finitely generated $\mathbb{Z}$-module and $\dim_{\mathbb{Z}} \mathcal{O} = \dim_{\mathbb{Q}} L$ ($\Leftrightarrow \mathbb{Q}(\mathcal{O}) = L$).

Obviously, $\mathbb{Z}[\alpha]$ and $\mathcal{O}_L$ are orders.

$\mathbb{Z}[\alpha]$ is called the <u>equation order</u>.

Since an order $\mathcal{O}$ is a f.g. $\mathbb{Z}$-module $\Rightarrow \mathcal{O}$ is integral over $\mathbb{Z}$ by Thm 3.19

$\Rightarrow \mathcal{O} \subseteq \mathcal{O}_L$

$\Rightarrow \mathcal{O}_L$ is <u>the</u> <u>maximal order</u>.

Let $\beta_1, \dots, \beta_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}$. Then this is also a $\mathbb{Q}$-basis of L and we have

$$d_{L|\mathbb{Q}}(\beta_1, \dots, \beta_n) \in \mathbb{Z}$$

by Cor 3.34.

If $\gamma_1, \dots, \gamma_n$ is another basis of $\mathcal{O}$, then by §2.7

$$d_{L|\mathbb{Q}}(\gamma_1, \dots, \gamma_n) = \det(U)^2 \, d_{L|\mathbb{Q}}(\beta_1, \dots, \beta_n)$$

where U is the base change matrix. But $U \in GL_n(\mathbb{Z})$, so $\det U = \pm 1$, so

$$d_{L|\mathbb{Q}}(\gamma_1, \dots, \gamma_n) = d_{L|\mathbb{Q}}(\beta_1, \dots, \beta_n). \quad !$$

<u>Def</u> 5.3: The discriminant wrt to one (hence any) basis of $\mathcal{O}$ is called the <u>discriminant</u> of $\mathcal{O}$, denoted $d_{\mathcal{O}}$

The discriminant $d_{\mathcal{O}_L}$ of the maximal order is also called the <u>discriminant</u> of L, denoted d_L.

Prop 5.4: Let $G \subset L$ be an order. Then
$$d_G = [G_L : G]^2 d_L$$

Proof: Let A be the matrix of $G \hookrightarrow G_L$ in some bases. Then
$$d_G = \det(A)^2 d_L$$
by §2.7.
By Cor 4.11, $|\det(A)| = [G_L : G]$. $\square$

Cor 5.5 $G = G_L$ iff $d_G = d_L$.

Cor 5.6: If d_G is square-free, then $G = G_L$. $\square$

Cor 5.7: If $d_{\mathbb{Z}[\alpha]}$ is square-free, then $\mathbb{Z}[\alpha] = G_L$. $\square$

5.2 Discriminant of an equation order

Recall from Exercise 3.4 that

Galois conjugates of α_i

$$d_{\mathbb{Z}[\alpha]} = d_{L|\mathbb{Q}}(1, \alpha, .., \alpha^{n-1}) = \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} \prod_i \Big(\prod_{j \neq i} (\alpha_i - \alpha_j) \Big)$$
$$= (-1)^{n(n-1)/2} \prod_j p_\alpha'(\alpha_j) = (-1)^{n(n-1)/2} N_{L|\mathbb{Q}}(p_\alpha'(\alpha)).$$

There is away to compute this just from the coefficients of p_α without knowing the Galois conjugates.

Def 5.8: Let R be a commutative ring. Let
$$f = \sum_{i=0}^{n} a_{n-i} X^i, \quad g = \sum_{j=0}^{m} b_{n-j} X^j \in R[X]$$
with $a_0 b_0 \neq 0$. The <u>resultant</u> $\mathrm{Res}(f,g)$ is the determinant of the <u>Sylvester matrix</u>

$$
\mathrm{Syl}(f,g) := \left.\begin{pmatrix} a_0 & \cdots & a_n & & \\ & \ddots & & \ddots & \\ & & a_0 & \cdots & a_n \\ b_0 & \cdots & b_m & & \\ & \ddots & & \ddots & \\ & & b_0 & \cdots & b_m \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a\\ a\\ a\end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix} a\\ a\\ a\end{matrix}}\right\} n \end{matrix}\right.
$$

<u>Lemma:</u> 5.9 If $f(x) = 0 = g(x)$ for some $x \in R$, then $\mathrm{Res}(f,g) = 0$.

<u>Proof:</u> We have

$$
\mathrm{Syl}(f,g) \cdot \begin{pmatrix} X^{n+m-1} \\ X^{n+m-2} \\ \vdots \\ X^n \\ X^{n-1} \\ \vdots \\ X \\ 1 \end{pmatrix} = \begin{pmatrix} f \cdot X^{m-1} \\ f X^{m-2} \\ \vdots \\ f \\ g X^{n-1} \\ \vdots \\ g \cdot X \\ g \end{pmatrix}
$$

Plugging in $X = x$ shows that $\mathrm{Syl}(f,g)$ has non-trivial kernel $\Rightarrow \det \mathrm{Syl}(f,g) = 0$. $\square$

<u>Prop:</u> 5.10 Let K be a field and

$$f = a_0 \prod_{i=1}^{n} (X - \alpha_i), \quad g := b_0 \prod_{j=1} (X - \beta_j).$$

Then $\mathrm{Res}(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$.

<u>Proof.</u> Let $R := K[X,Y]$ and let $\mathrm{Res}(Y) := \mathrm{Res}(f, g - Y) \in K[Y]$.
When plugging in an element $y \in K$ for Y we set

$$\mathrm{Res}(y) = \mathrm{Res}(f, g - y) \in K$$

Let $\gamma_i := g(\alpha_i) \in K$. Then $\mathrm{Res}(\gamma_i) = \mathrm{Res}(f, g - \gamma_i)$

Now, $f, g - \gamma_i \in K[X]$ have a common zero, namely α_i :

$$f(\alpha_i) = 0 \ ; \ (g-\gamma_i)(\alpha_i) = g(\alpha_i) - \underset{= g(\alpha_i)}{\gamma_i} = 0$$

$\Rightarrow \mathrm{Res}(\gamma_i) = 0$ by Lemma 5.9

$\Rightarrow \gamma_i$ is a zero of $\mathrm{Res}(Y) \in K[Y]$

$\Rightarrow Y - \gamma_i$ divides $\mathrm{Res}(Y)$ $\forall i$

$= \prod_{i=1}^{n} (Y - \gamma_i)$ divides $\mathrm{Res}(Y)$

$\mathrm{Res}(Y)$ has degree n and leading coefficient $(-1)^n a_0^m$

$$\Rightarrow \mathrm{Res}(Y) = (-1)^n a_0^m \prod_{i=1}^{n} (Y - \gamma_i) = a_0^m \prod_{i=1}^{n} (\gamma_i - Y)$$

Hence,

$$\mathrm{Res}(f,g) = \mathrm{Res}(0) = a_0^m \prod_{i=1}^{n} \gamma_i = a_0^m \prod_{i=1}^{n} g(\alpha_i) = a_0^m \prod_{i=1}^{n} b_0 \prod_{j=1}^{m} (\alpha_i - \beta_j)$$

$$= a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

□

<u>Cor</u> 5.12 (I can't count):

$$d_{\mathbb{Z}[\alpha]} = d_{L|\mathbb{Q}}(1, \alpha, .., \alpha^{n-1}) = (-1)^{n(n-1)/2} \prod_j p_\alpha'(\alpha_j)$$

$$= (-1)^{n(n-1)/2} \mathrm{Res}(p_\alpha, p_\alpha')$$

□

Ex 5.13: Let α be a root of $f := X^3 - X - 1$.

Then $f' = 3X^2 - 1$ and

$$Sy((f,f)) = \begin{pmatrix} 1 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & -1 & -1 \\ 3 & 0 & -1 & 0 & 0 \\ 0 & 3 & 0 & -1 & 0 \\ 0 & 0 & 3 & 0 & -1 \end{pmatrix}$$

$$Res(f,f') = \det Sy((f,f')) = \dots = 23$$

$$\rightarrow disc_{\mathbb{Z}[\alpha]} = (-1)^{3\cdot(3-1)/2} \cdot 23 = -23.$$

This is square-free, hence $\mathcal{O}_L = \mathbb{Z}[\alpha]$ and $\{1, \alpha, \alpha^2\}$ is an integral basis.

Ex 5.14: Let $\alpha = \sqrt{D}$

By Lemma 2.42:

$$d_{\mathbb{Z}[\alpha]} = (\sqrt{D} - (-\sqrt{D}))^2 = 4D$$

This is not square-free. Nonetheless, if $D \equiv 2,3 \mod 4$ then $\mathcal{O}_L = \mathbb{Z}[\alpha]$ by Exercise 2.4.

Unfortunately, it is rarely the case that d_L is square-free.

5.3 Zassenhaus approach (1967)

Start with a known order G in L (e.g. the equation order $\mathbb{Z}[\alpha]$)

Recall that $d_G = [G_L : G]^2 d_L$.

Write $d_G = a^2 \cdot b$ with $a, b \in \mathbb{Z}$, b squarefree.

Let $p_1, \dots, p_r$ be the distinct prime factors of a.

Then $[G_L : G] = \prod_{i=1}^{r} p_i^{m_i}$, $m_i \leq n_i$ where $a = \prod_{i=1}^{r} p_i^{n_i}$.

$m^k x = y \in G \Rightarrow x = y$

Def 5.15: For $m \in \mathbb{Z} \setminus \{0\}$ let

$$G_m := \{ x \in G_L \mid m^k x \in G \text{ for some } k \} = \{ \tfrac{y}{m^k} \mid y \in G, k \in \mathbb{N} \}$$

This is called the <u>m-maximal overorder of G</u>. for the following reasons

Lemma 5.16:

a) G_m is an order containing G.

b) $[G_m : G] \mid m^k$ and $\gcd([G_L : G^m], m) = \underline{1}$

Before we prove this, note that for $m = p_i$:

$$[G_{p_i} : G] \text{ is a power of } p_i \text{ and } p_i \nmid [G_L : G_{p_i}]$$

$\rightsquigarrow$ G_{p_i} removes the p_i in $[G_L : G]$. Hence by the structure theorem of f.g. abelian groups, Thm 4.9,

$$G_L / G = \bigoplus_{i=1}^{r} G_{p_i} / G. \leftarrow p_i\text{-torsion part of } G_L/G$$

We will see that we can iteratively construct a generating set of G_{p_i}. Putting all these together $\forall p_i$ gives a generating set of G_L. Can then compute a basis from this using HNF.