Lecture 4, 6.11.

Lemma 2.42 If $K \subseteq L$ is separable and has a basis of the form $1, \theta, \dots, \theta^{n-1}$ (e.g. if $L = K(\theta)$), then

$$d_{L|K}(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0,$$

where $\theta_i = \sigma_i(\theta)$ and σ_i are the K-morphisms $L \to \Omega$, $\Omega \supseteq K$ algebraically closed.

Proof:

$$d_{L|K}(1, \theta, \dots, \theta^{n-1}) = \det\left((\sigma_i(\theta^j)) \right)^2$$

$$= \det\left((\theta_i^j) \right)^2$$

$$\overset{\text{Vandermonde}}{=} \prod_{i<j} (\theta_i - \theta_j)^2$$

$\square$

Cor 2.43 The trace form of a finite separable extension is always non-degenerate.

Proof: $L = K(\theta)$ by primitive element theorem.

$\square$

3. Ring of integers

3.1 Integral elements

Motivation. Since $\mathbb{Q} \subset \mathbb{Q}(i)$ is finite, it is algebraic, hence ever $\alpha \in \mathbb{Q}(i)$ is a root of a monic polynomial $f \in \mathbb{Q}[X]$.

How can we characterize $\mathbb{Z}[i] \subset \mathbb{Q}(i)$?

Lemma 3.1 $\mathbb{Z}[i]$ consists precisely of the elements $\alpha \in \mathbb{Q}(i)$ which are a root of a monic polynomial $f \in \mathbb{Z}[X]$.

Proof: Let $\alpha = a+bi \in \mathbb{Z}[i]$, i.e. $a, b \in \mathbb{Z}$. Then f is a root of

$$\mathbb{Z}[X] \ni f = X^2 + cX + d, \quad c = -2a, \; d = a^2+b^2$$

Conversely let $\alpha = a+bi \in \mathbb{Q}(i)$ and $f(\alpha) = 0$ for some $f \in \mathbb{Z}[X]$.

It follows from Gauss's Lemma that every monic factor of f in $\mathbb{Q}[X]$ also lies in $\mathbb{Z}[X] \Rightarrow p_\alpha \in \mathbb{Z}[X]$

p_α is of degree $\leq 2 = \dim_{\mathbb{Q}} \mathbb{Q}(i)$. If $\deg p_\alpha = 1 \Rightarrow \alpha = a \in \mathbb{Z}$.

If $\deg p_\alpha = 2$, then $p_\alpha = X^2 + cX + d$, $c, d \in \mathbb{Z}$.

$$p_\alpha(\alpha) = 0 \Rightarrow (a+ib)^2 + c(a+ib) + d = 0$$

$$\Rightarrow (a^2 - b^2 + ca + d) + (2ab + bc)i = 0$$

$$\Rightarrow a^2 - b^2 + ca + d = 0 \text{ and } 2ab + bc = 0$$

$$2ab+bc=0 \Downarrow b(2a+c) = 0$$

If $b = 0 \Rightarrow \alpha \in \mathbb{Z}$ ↯

So $b \neq 0 \Rightarrow \underline{c = -2a \Rightarrow 2a \in \mathbb{Z}}$

$$\xrightarrow{c=-2a} d = a^2 + b^2$$

$$\Rightarrow \underset{\in \mathbb{Z}}{4d} = 4a^2 + 4b^2 = \underbrace{(2a)^2}_{\in \mathbb{Z}} + (2b)^2$$

$$\Rightarrow (2b)^2 \in \mathbb{Z} \Rightarrow 2b \in \mathbb{Z} \quad (b \in \mathbb{Q})$$

Now, $(2a^2) + (2b)^2 = 4d \equiv 0 \mod 4 \Rightarrow (2a)^2 \equiv (2b)^2 \equiv 0 \mod 4$

$\Rightarrow 4a^2 = 4n \Rightarrow a^2 = n \Rightarrow a \in \mathbb{Z} \quad (a \in \mathbb{Q})$.

$\square$

This brings us to the following definition:

<u>Def.</u> 3.2: Let $R \subseteq S$ be an extension of commutative rings. An element $\alpha \in S$ is <u>integral</u> over R if $f(\alpha)=0$ for some monic $f \in R[X]$. The <u>integral closure</u> of R in S is

$$R^{int,S} := \{\alpha \in S \mid \alpha \text{ integral over } R\}.$$

The extension $R \subseteq S$ is <u>integral</u> if each $\alpha \in S$ is integral over R, i.e. $S = R^{int,S}$.

<u>Example</u> 3.3:

a) $K \subseteq L$ a field extension. Then integral $\Leftrightarrow$ algebraic

b) every R is integral over R, so $R \subseteq R^{int,S}$.

c) $\mathbb{Z}^{int,\mathbb{Q}} = \mathbb{Z}$ by Gauss Lemma.

d) $\mathbb{Z}^{int,\mathbb{Q}(i)} = \mathbb{Z}[i]$ by Lemma 3.1.

e) Be careful! $\frac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ is integral over $\mathbb{Z}$: it is a zero of

$$f := X^2 - X + 1 \quad \in \mathbb{Z}[X]$$

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

$$= -\frac{4}{4} + \frac{4}{4} = 0.$$

It is thus not so obvious how $R^{int,S}$ looks like. Let's prove some general facts.

We will shortly see that $R^{int,S}$ is a ring.

It's best to view this in terms of modules.

3.2 Modules (review)

Let R be a commutative ring. "Vector space" over R?

<u>Def</u> 3.4: An <u>R-module</u> is an abelian group $(V,+)$ equipped with an action $R\times V \longrightarrow V$ of R such that

$$r(v+v') = rv + rv'$$
$$(r+r')v = rv + r'v$$
$$(rr')v = r(r'v)$$
$$1v = v$$

<u>Ex</u> 3.5:

a) K a field then K-module $\Leftrightarrow$ K-vector space

b) A an abelian group $\Leftrightarrow$ A a $\mathbb{Z}$-module:

$$n(a) = \underbrace{a+a+\dots+a}_{n \text{ times}}$$

c) R is an R-module: $r\cdot r' := rr'$ (acts on itself)

d) If $R\subseteq S$ is a ring extension, S is an R-module: $r\cdot s = rs$.

e) V a $K[X]$-module means: V K-vector space and X acts by an endomorphism of V $v\longmapsto Xv$.

<u>Def</u> 3.6: A subset $U\subset V$ is a <u>submodule</u> if $ru\in U$ $\forall u\in U$ (U stable under the action).

<u>Ex</u> 3.7:

a) K a field: submodule $\Leftrightarrow$ subspace

b) $I\subset R$ ideal $\Leftrightarrow$ submodule of R

<u>Def</u> 3.8: $U\subset V$ a subset. There is a unique smallest submodule of V containing U, namely

$$R\cdot U := \bigcap_{\substack{U'\subset V \text{ submodule} \\ U\subset U'}} U' = \left\{ \sum_{i\in I} r_i u_i \;\middle|\; r_i\in R,\, u_i\in U,\, |I|<\infty \right\},$$

= finite R-linear combination of elts of U.

This is the submodule generated by U.

Def 3.9: An R-module V is finitely generated if $V = R \cdot U$ for a finite set $U \subset V$.

Ex 3.10:

a) For K-vector spaces: finitely generated $\Leftrightarrow$ finite dimensional.

b) R as an R-module is finitely generated: $R = R \cdot 1$

c) Every ideal in $K[X]$ is a finitely generated $K[X]$-module: it is generated by a single element.

↯↯↯↯↯↯ WARNING N° 1 ↯↯↯↯↯

Submodules of f.g modules do not have to be finitely generated!

Ex 3.11:

Let $R := K[X_1, X_2, X_3, \dots]$ infinitely many variables

Then R is a fg R-module by Ex 3.10

BUT: $I = (X_1, X_2, X_3, \dots) \subset R$ is an ideal which is not finitely generated!

Def 3.12: An R-algebra is a ring A which is also an A-module such that

$$r(aa') = (ra)a' = a(ra') \quad \forall r \in R,\ a, a' \in A.$$

$$1_R \cdot a = a = a \cdot 1_R.$$

Ex 3.13:

a) The polynomial ring $R[X]$ is an R-algebra

b) $R \subseteq S$ a ring extension $\rightsquigarrow$ S is an R-algebra.

c) Every ring R is a $\mathbb{Z}$-algebra: $n \cdot r = \underbrace{r + \dots + r}_{n \text{ times}}$

Def 3.14: A <u>subalgebra</u> of A is a subring U which is also an R-submodule ($\Rightarrow$ U naturally an R-algebra)

Def 3.15: A an R-algebra, $U \subset A$ subset. Then

$$R[U] := \bigcap_{\substack{A' \subset A \text{ subalgebra} \\ U \subset A'}} A' \quad = \text{finite } R\text{-linear combinations of products of finitely many elts of } U$$

is the subalgebra <u>generated</u> by U.

Def 3.16: A is called <u>finitely generated</u> as R-algebra if $A = R[U]$ for U finite.

Remark 3.17: A f.g. as R-module $\Rightarrow$ f.g. as R-algebra. Not conversely: polynomial ring $K[X]$ is f.g. as K-algebra but not as K-module

Ex 3.18: $\mathbb{Q}(i)$ is a $\mathbb{Z}$-algebra. Then $\mathbb{Z}[i] =$ subalgebra generated by $\{i\}$.
$= \{a + ib \mid a, b \in \mathbb{Z}\}$.

Note: the $\mathbb{Z}$-algebra $\mathbb{Z}[i]$ is a finitely generated $\mathbb{Z}$-module!

3.3 Integral elements form a ring

Thm 3.19: $R \subseteq S$ a ring extension, $\alpha \in S$. TFAE

a) α is integral over R

b) $R[\alpha] \subset S$ is a finitely generated R-module

c) There is an R-subalgebra S' of S with $\alpha \in S'$ and S' finitely generated R-module.

Proof:

$a \Rightarrow b$: let $f = X^n + r_{n-1} X^{n-1} + \dots + r_0 \in R[X]$ with $f(\alpha) = 0$.

$$\Rightarrow \alpha^n = -\sum_{i=0}^{n-1} r_i \alpha^i \in R \cdot \{1, \alpha, \dots, \alpha^{n-1}\} \subset S \Rightarrow R[\alpha] = R \cdot \{1, \alpha, \dots, \alpha^{n-1}\}.$$

b⇒c: $S' = S[\alpha]$.

c⇒a: $S' = R\{\alpha_1, \dots, \alpha_n\}$, $\alpha_i \in S$

Since $\alpha \in S'$ and S' a ring $\Rightarrow \alpha\alpha_i \in S'$ $\forall i$

Since $S' = R\{\alpha_1, \dots, \alpha_n\}$ have

$$\alpha\alpha_i = \sum_{j=1}^{n} r_{ij}\alpha_j \quad , \quad r_{ij} \in R$$

Let $M := (r_{ij})_{ij} \in Mat_n(R)$, $v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in (S')^n$

Consider S' as an $R[X]$-module with X acting by multiplication by α, so $Xs := \alpha s$. $\rightsquigarrow Xv = \begin{pmatrix} X\alpha_1 \\ \vdots \\ X\alpha_n \end{pmatrix} = \begin{pmatrix} \alpha\alpha_1 \\ \vdots \\ \alpha\alpha_n \end{pmatrix}$.

Then $\underbrace{(X \cdot I_n - M)}_{\text{matrix over } R[X]} v = 0$

Multiply with the adjugate matrix $\rightsquigarrow \underbrace{\det(XI_n - M)}_{=: f \in R[X] \text{ monic polynomial}} \cdot v = 0$

$\rightsquigarrow f . \alpha_i = 0$ $\forall i$

$\rightsquigarrow$ Since $S' = R\{\alpha_1, \dots, \alpha_n\}$, $f . s' = 0$ $\forall s' \in S \Rightarrow f . 1 = 0$

Hence, writing $f = \sum r_i X^i \rightsquigarrow 0 = f . 1 = \sum r_i \alpha^i$

$\rightsquigarrow \alpha$ integral.

$\square$

<u>Corollary</u>[3.20]: If $\alpha_1, \dots, \alpha_n \in S$ are integral over R, then $R[\alpha_1, \dots, \alpha_n] \subset S$ is a f.g. R-module.

<u>Proof</u>: By induction on n. $n = 1$ is theorem 3.19.

$n > 1$: Let $S' := R[\alpha_1, \dots, \alpha_{n-1}]$. By induction, f.g. R-module.

α_n integral over $R \Rightarrow$ integral over $S' \supseteq R$

$\Longrightarrow S'' := S'[\alpha_n]$ is a f.g. S'-module.

Since S' finite over R $\to$ S'' finite over R. $\square$

<u>Corollary 3.21:</u> $R^{\mathrm{int},S}$ is an R-subalgebra of S

<u>Proof:</u> Let $\alpha, \alpha' \in R^{\mathrm{int},S}$ $\rightsquigarrow$ $R[\alpha,\alpha'] \subset S$ f.g. R-module by Cor X $\longrightarrow$ $\alpha+\alpha', \alpha\alpha', r\alpha'$ contained in an R-subalg of S that is f.g. $\Longrightarrow$ $\alpha+\alpha', \alpha\alpha', r\alpha'$ integral by Thm 3.19 $\square$

<u>Def 3.22</u> If L is a number field, then $\mathcal{O}_L := \mathbb{Z}^{\mathrm{int},L}$ is called the <u>ring of integers</u> in L.