Lemma 2.42 If $K \subseteq L$ is separable and has a basis of the form $1, \Theta_1, \ldots, \Theta^{n-1}$ (e.g., if $L=K(\Theta)$), then
\[ \det_{K}(1, \Theta, \ldots, \Theta^{n-1}) = \prod_{i<j} (\Theta_i - \Theta_j)^2 \neq 0, \]
where $\Theta_i = \sigma_i(\Theta)$ and $\sigma_i$ are the $K$-morphisms $L \to L$, $L \cong K$ algebraically closed.

Proof:
\[ \det_{K}(1, \Theta, \ldots, \Theta^{n-1}) = \det \left( \sigma_i(\Theta) \right)^2 \]
\[ = \det \left( \Theta_i \right)^2 \]
\[ = \prod_{i<j} (\Theta_i - \Theta_j)^2 \]

\[ \square \]

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 every \( \alpha \in \mathbb{Q}(i) \) is a root of a monic polynomial \( f \in \mathbb{Q}[X] \). How can we characterize \( \mathbb{Z}[i] = \mathbb{Q}(i) \)?

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 \( \alpha \) is a root of

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

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 \( \mathbb{Z}[X] \).

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

If \( \deg \alpha = 2 \), then \( \alpha = x^2 + cx + d, c, d \in \mathbb{Z} \).

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

\[
= (a^2 - b^2 + ca + db) + (2ab + bc)i = 0
\]

\[
= a^2 - b^2 + ca + db = 0 \quad \text{and} \quad 2ab + bc = 0
\]

\[
c = -2a \quad \Rightarrow \quad d = a^2 + b^2 \\
\Rightarrow \quad 4d = 4a^2 + 4b^2 = (2a)^2 + (2b)^2 \quad \text{in} \quad \mathbb{Z} \\
\Rightarrow \quad (2b)^2 \in \mathbb{Z} \Rightarrow 2b \in \mathbb{Z} \quad \text{in} \quad \mathbb{Z}
\]

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

\( \Rightarrow 4a^2 \equiv 0 \Rightarrow a^2 \equiv 0 \Rightarrow a \in \mathbb{Z} \quad \text{or} \quad \mathbb{Z} \). \( \square \)
This brings us to the following definition:

**Def.** Let $R \subseteq S$ be an extension of rings. An element $x \in S$ is integral over $R$ if $f(x)$ for some monic $f \in R[X]$. The integral closure of $R$ in $S$ is

$$R_{\text{int}}S := \{x \in S \mid x \text{ integral over } R\}.$$ 

The extension $R \subseteq S$ is integral if each $x \in S$ is integral over $R$, i.e., $S = R_{\text{int}}S$.

**Example:**

a) $K \subseteq \mathbb{L}$ a field extension. Then $\mathbb{L}$ is integral over $\mathbb{K}$, so $\mathbb{K} = R_{\text{int}}\mathbb{L}$.

b) Every $R$ is integral over $R$, so $R = R_{\text{int}}R$.

c) $\mathbb{Z}[\sqrt{2}] = \mathbb{Z}$ by Gauss Lemma.

d) $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ 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 root of $f = x^2 - x + 1 \in \mathbb{Z}[X]$

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

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

It is thus not so obvious how $R_{\text{int}}S$ looks like. Let's prove some general facts.

We will shortly see that $R_{\text{int}}S$ 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 $R$?

**Def.** An $R$-module is an abelian group $(V, +)$ equipped with an action $R \times V \to V$ of $R$ such that

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

**Ex.**

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

b) $A$ an abelian group $\equiv A$ a $Z$-module:

$$n(a) = a + a + \ldots + a$$

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

d) If $R \subseteq S$ is a ring extension, $S$ is an $R$-module: $1.S = SS$

e) $V$ a $K[X]$-module means: $V$ a $K$-vector space and $X$ acts by an endomorphism $V \to V$

**Def.** A subset $U \subseteq V$ is a submodule if $ru \in U \forall u \in U, r \in R$ (stably under the action).

**Ex.**

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

b) $I \subseteq R$ ideal $\equiv$ submodule of $R$

**Def.** $U \subseteq V$ a subset. There is a unique smallest submodule of $V$ containing $U$, namely

$$R.U := \bigcap_{U \subseteq V \text{ submodule}} U = \left\{ \sum_{i=1}^{l} r_i u_i \mid r_i \in R, u_i \in U, l \in \mathbb{N}, \sum_{i=1}^{l} |r_i| < \infty \right\}$$

- a $K$-linear combination of elts of $U$. 


This is the submodule generated by \( U \).

**Def.** An \( R \)-module \( V \) is **finitely generated** if \( V = R \cdot U \) for a finite set \( U \subset V \).

**Ex.**

a) For \( U \)-vector spaces, finitely generated \( \iff \) finite dimensional.

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

c) Every ideal in \( KH \) is a finitely generated \( KH \)-module: it is generated by a single element.

**WARNING**

Submodules of \( R \)-modules do not have to be finitely generated!

**Ex.**

Let \( R := KH \langle x_1, x_2, x_3, \ldots \rangle \) \( \subseteq \) \( R \) \( \subseteq \) \( R \) \( \subseteq \) \( \cdots \) infinitely many variables

Then \( R \) is a \( R \)-module by **Ex.**

**BUT:** \( I = (x_1, x_2, x_3, \ldots) \subset R \) is an ideal which is not finitely generated!

**Def.** An **\( R \)-algebra** is a ring \( A \) which is also an \( A \)-module such that

\[
(r(a))a' = r(aa') \quad \forall r \in R, a, a' \in A.
\]

\[
1_R \cdot a = a = a \cdot 1_R.
\]

**Ex.**

a) The polynomial ring \( R[x] \) is an \( R \)-algebra.

b) \( R \subseteq S \) a ring extension \( \Rightarrow \) \( S \) is an \( R \)-algebra.
c) Every ring R is a \( \mathbb{Z} \)-algebra: \( n \cdot r = \underbrace{r + \ldots + r}_{n \text{ times}} \)

\[ \text{Def.} \quad \text{A subalgebra of} \ A \text{ is a subring \( U \) which is also an} \ R \text{-submodule} \]
\( \Rightarrow U \text{ naturally an} \ R \text{-algebra} \)

\[ \text{Def.} \quad \text{A -} \ R \text{-algebra,} \ U \subset A \text{ subset. Then} \]
\[ R[U] := \bigcap A^1 \quad = \text{finite} \ R \text{-linear combinations of products of finitely many elts of} \ U \]

is the subalgebra generated by \( U \).

\[ \text{Def.} \quad A \text{ is called} \ \text{finitely generated as} \ R \text{-algebra of} \ A = R[U] \text{ for} \ U \text{ finite.} \]

\[ \text{Remark.} \quad A \text{ F.g. as} \ R \text{-module} \Rightarrow \text{F.g. as} \ R \text{-algebra. Not conversely:} \]

polynomial ring \( \mathbb{Z}[x] \) is F.g. as \( \mathbb{R} \)-algebra but not as \( \mathbb{R} \)-module.

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

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

3.3 Integral elements form a ring

\[ \text{Thm.} \quad R = S \text{ a ring extension,} \ \alpha \in S. \ TFAE \]

a) \( \alpha \) 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.

\[ \text{Proof:} \quad a \Rightarrow b: \text{ let} \ f = x^n + r_{n-1} x^{n-1} + \ldots + r_0 \in R[U] \text{ with} \ f(\alpha) = 0 \]
\[ \Rightarrow \alpha^n = - \sum_{i=0}^{n-1} r_i \alpha^i \in R \cdot \{ 1, \alpha, \ldots, \alpha^{n-1} \} \subset S \Rightarrow R[\alpha] = R[1, \alpha, \alpha^{n-1}] \]
Since $\alpha \in S'$ and $S'$ a ring $\Rightarrow \alpha x_i \in S'$ bi.

Since $S' = R[x_1, \ldots, x_n]$ here

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

Let $M := (r_{ij})_{i,j} \in \text{Mat}_n(R)$, $V = (\alpha x_i) \in (S')^n$.

Consider $S'$ as an $R[X]$-module with $X$ acting by multiplication by $\alpha$, so $X \alpha := \alpha x$. $\Rightarrow X v = (x_{\alpha i}) \cdot (\alpha x_i)$.

Then $(X \cdot I_n - M) v = 0$

Multiply with the adjugate matrix $\Rightarrow \det (X I_n - M) \cdot v = 0$ $= : f \in R[X]$ monic polynomial

$\Rightarrow f \cdot \alpha x_i = 0 \forall i$

$\Rightarrow$ Since $S' = R[x_1, \ldots, x_n]$, $f = 0 \forall \alpha \in S \Rightarrow f \cdot 1 = 0$

Hence, writing $f = \sum r_i x_i \Rightarrow 0 = f \cdot 1 = \sum r_i \alpha x_i$

$\Rightarrow \alpha$ integral.

$\square$

**Corollary 3.20:** If $x_1, \ldots, x_n \in S$ are integral over $R$, then $R[x_1, \ldots, x_n] \subseteq S$ is a $R$-module.

**Proof:** By induction on $n$. $n = 1$ is theorem 3.19.

$n > 1$: Let $S' := R[x_1, \ldots, x_{n-1}]$. By induction, $S'$ is $R$-module.

An integral over $R$ is integral over $S' \supseteq R$. 

\[ S'' = S'[x'] \text{ is a } S\text{-module.} \]

Since \( S' \) is a \( R \)-module and \( S'' \) is also a \( S\text{-module,} \)

**Corollary:** \( \text{Rint} S \) is an \( R\)-subalgebra of \( S \)

**Proof:** Let \( \alpha, \beta \in \text{Rint} S \) and \( \alpha' \in S \). \( R\)-module by \( \text{Rint} S \) is \( R\)-module by \( C_0 \Rightarrow x' \)

**Cor:** \( x' \rightarrow x' \cdot \alpha \), contained in an \( R\)-subalgebra of \( S \) that is \( \text{fg} \Rightarrow \alpha + \alpha', \alpha x', \alpha x' \text{ integral by Thm 3.19} \)

**Def. 3.22:** If \( L \) is a number field, then \( \mathcal{O}_L := \text{int} L \) is called the ring of integers in \( L \).