Lemma 3.23 Consider ring extensions $R \subseteq S \subseteq T$. If $R \subseteq S$ and $S \subseteq T$ are integral, so is $R \subseteq T$.

Proof: Let $t \in T$. Then there is $f = X^n + s_{n-1}X^{n-1} + \cdots + s_1X + s_0 \in S[X]$ with $f(t) = 0$. Let $S' = R[s_0, s_{n-1}] \subseteq S$. Since $R \subseteq S$ is integral, each $s_i$ is integral over $R \implies S' \subseteq \text{f.g. } R$-module by Cor 3.20.

Since $t$ is integral over $S'$ ($s \in S'$) $\implies S'[t] \subseteq S'$ is module by Cor 3.20

$\implies S'[e] \subseteq S$ is module ($S'[t]$ is $R$-module)$\implies$ integral over $R$ by Thm 3.19.

3.4 Ring of integers is integrally closed

Def 3.24: $R \subseteq S$ a ring extension. Say that $R$ is integrally closed in $S$ if

$\cap R \subseteq R$, i.e. if $x \in S$ integral over $R$ then $x \in R$.

Lemma 3.25: The integral closure of $R$ in $S$ is integrally closed in $S$.

Proof:

Note: $R' = \cap R \subseteq S$ contained in $S$ and $R \subseteq R'$ is integral.

So, if $x \in S$ integral over $R'$ $\implies$ integral over $R$ by Lemma 3.23.

$\implies x \in R'$

$\implies R'$ is integrally closed.

Ex:

a) $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$

b) $\mathbb{Z}[i] = \mathbb{Z}[\text{int}(i)]$ is integrally closed in $\mathbb{Q}(i)$.

c) $\mathbb{Z} = \mathbb{Z}[\text{int}(L)]$ ring of integers in a number field $L$ is integrally closed in $L$. 

---
Def: Let \( R \) be an integral domain. The **field of fractions** (or **quotient field**) of \( R \) is

\[
\mathbb{Q}(R) := \left\{ \frac{r}{s} \mid r, s \in R, s \neq 0 \right\}
\]

with the obvious addition and multiplication

(Formally: \( \mathbb{Q}(R) = \left\{ (r/s_1, r/s_2) \mid r_1, r_2 \in R, s_1, s_2 \neq 0 \right\} / \sim \) with \( (r_1/s_1, r_2/s_2) \sim (s_1/r_1, s_2/r_2) \) iff \( s_1r_2 = s_2r_1 \))

Ex: 3.28

a) \( \mathbb{Q}(\mathbb{Z}) = \mathbb{Q} \)

b) \( \mathbb{Q}(\mathbb{Z}[i]) = \mathbb{Q}(i) : \frac{a+bi}{c+di} \to \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2} \cdot i \in \mathbb{Q}(i) \)

c) \( \mathbb{Q}(\mathbb{W}[x]) = \left\{ \frac{f}{g} \mid (f, g) \in \mathbb{W}[x], g \neq 0 \right\} : \text{rational function field} \)

Rem: The map \( R \to \mathbb{Q}(R), r \to \frac{r}{1} \), is injective.

\( \mathbb{Q}(R) \) is the smallest field containing \( R \).

Def: \( R \) an integral domain, \( K := \mathbb{Q}(R) \).

The **integral closure** (or **normalization**) of \( R \) is \( \text{Int}_{\mathbb{K}} R \).

\( R \) is **integrally closed** (or **normal**) if \( \text{Int}_{\mathbb{K}} R = R \).

Lem: Let \( R \) be an integral domain and \( L \) an algebraic extension of \( K := \mathbb{Q}(R) \). Let \( S := R^{\text{alg}} \). Then

a) For every \( x \in L \) there is \( \alpha \in \mathbb{R} \setminus \mathbb{Q} \) such that \( \alpha \cdot x \in S \).

b) \( \mathbb{Q}(S) = L \).

c) \( S \) is integrally closed.

\[
\begin{array}{ccc}
R & \hookrightarrow & S \\
\downarrow \text{integral} & & \downarrow \text{algebraic} \\
& \nearrow L = \mathbb{Q}(S) & \\
& R \hookrightarrow \mathbb{K} = \mathbb{Q}(R) & \\
\end{array}
\]
Proof. Since U is algebraic, there is
\[ f(x) = x^n + a_1x^{n-1} + \ldots + a_n = 0 \]
with \( f(x) = 0 \), i.e.,
\[ \alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0 \]
Since \( U = Q(R) \), there is \( d \in R \) such that \( d\alpha \in R \) (common denominator).

Multiply above by \( d^n \):
\[ 0 = d^n\alpha^n + d^{n-1}a_1\alpha^{n-1} + \ldots + d\alpha + a_n = (d\alpha)^n + a_1(d\alpha)^{n-1} + \ldots + a_n(d\alpha) + a_n \]
\( d \alpha \) integral over \( R \), \( \alpha \in S \).

Clearly \( Q(S) \leq L \). Above shows \( L \subseteq Q(S) \), so \( L = Q(S) \).

By Lemma 3.25, \( S \) is integrally closed in \( L \). Since \( L = Q(S) \), \( S \) is integrally closed.

\[ \square \]

Cor: Rings of integers are integrally closed.

3.5 Integrality of minimal polynomial, norm, trace

Let \( R \) be an integrally closed domain, \( U = Q(R) \), \( L \leq K \) a finite extension.

Lemma: \( \alpha \in L \) is integral over \( R \) iff \( \alpha \) has coefficients in \( R \).

Proof: If \( \alpha \) has coefficients in \( R \), then \( \alpha \) is integral.

Conversely, let \( \alpha \) be integral. Then
\[ \alpha^n + r_1\alpha^{n-1} + \ldots + r_{n-1} \alpha + r_n = 0 \]
for some \( r_i \in R \).

Let \( \alpha' \) be another root of \( \alpha \) (in some splitting field).

Then \( K(\alpha') \) and \( K(\alpha) \) are both stem fields of \( \alpha \).

\[ \alpha \in \alpha \Rightarrow K(\alpha') \cong K(\alpha) \text{ with } \alpha(\alpha') = \alpha' \]

Applied to equation above:
\[ (\alpha')^n + r_1(\alpha')^{n-1} + \ldots + r_{n-1}(\alpha') + r_n = 0 \]
\[ \alpha^{1} \text{ integral over } R. \]

As integral elements form a ring by Cor 3.21, all coefficients of \( \alpha \) are integral over \( R \).

Coeffs of \( \alpha \) are in \( K \), they are integral over \( R \) \( \iff \) coeffs in \( R \) since \( R \) integrally closed. \( \therefore \) \( \alpha \in R[x] \)

3.34

Cor: Suppose \( K \leq L \) separable. If \( \alpha \in L \) integral over \( R \) then:

a) \( \alpha \) has coefficients in \( R \)

b) \( \alpha \) integral over \( R \) then \( N_{L/K}(\alpha), Tr_{L/K}(\alpha) \in R \).

Proof: \( X_{\alpha} = p_{\alpha}^{d} \) by Prop 2.31 \( \iff \alpha \in R[x] \) by Lema 3.33

\( N_{L/K}(\alpha) \) and \( Tr_{L/K}(\alpha) \) are coefficients of \( \alpha \) by Lema 2.26

\( \therefore \) both \( \in R. \)

3.6 Ring of integers is finitely generated

Let \( R \) be a ring.

Def: An \( R \)-module \( V \) is noetherian if every submodule of \( V \) is finitely generated.

Prop: The following are equivalent:

a) \( V \) is noetherian

b) Every ascending chain of submodules of \( V \) eventually becomes stationary:

\[ 0 = V_{0} \subseteq V_{1} \subseteq V_{2} \subseteq \ldots \iff V_{i} = V_{i+1} \forall i \geq N \]

c) Every non-empty set of submodules of \( M \) has a maximal element

Proof:
(3.37) Lemma If $U$ is a submodule of $V$, then:

a) the abelian group $V/U$ is naturally an $R$-module with $r \cdot \overline{v} = \overline{rv}$.

b) $\Phi$ submodule of $V$ containing $U$ if and only if submodule of $V/U$.

Proof: Straightforward.

(3.38) Lemma: $U$ a submodule of $V$. Then $V$ noetherian if and only if both $U$ and $V/U$ noetherian.

Proof: $\Rightarrow$ clear.
Claim: $V' \subseteq V''$ submodules of $V$ with $V' + V''U = V'' + V'U$ and $V' \cap U = V'' \cap U$.

Let $V' \subseteq V''$. Then there is $v' \in V'$ s.t. $v' + V''U = V'' + V'U \\
\Rightarrow v' = v'' + u \\
\Rightarrow v'' \in V' \cap V'' \subseteq V'' \cap U \subseteq V'' \cap U \subseteq V'$.

Now, suppose there is an ascending chain of submodules of $V$. The image of this chain in $V/U$ becomes stationary since $V/U$ Noetherian. The intersection of the chain with $U$ becomes stationary since $U$ Noetherian. The chain itself becomes stationary by claim.

3.39

Def: A morphism $f: V \rightarrow W$ of $R$-modules $V, W$ is a map such that

- $f(v + v') = f(v) + f(v')$
- $f(rv) = r f(v)$

Lemma: Kernel, image, isomorphism theorem as for vector spaces.

3.40

Def: $R$ is called Noetherian if Noetherian as $R$-module, i.e. every ideal is f.g.

Prop: If $R$ is Noetherian then every f.g. $R$-module is Noetherian.

Proof: By induction on the minimum number of generators for $V$.

If $n = 1$, $V \cong R \cdot v_1$. Let $f: R \rightarrow V, 1 \mapsto v_1$, is surjective.

Then $R/I \cong V$ as $R$-modules, $I = \ker f$.

Since $R$ Noetherian, so is $R/I$, hence $V$.

If $n > 1: V = R \cdot v_1, \ldots, v_n$. Then $U = R \cdot v_1 \cup \ldots \cup \cup v_n$ Noetherian by induction.

Also $V/U$ Noetherian since generated by one element, $v_n$.

Lemma: $V$ Noetherian.

3.41

Def: $R$ is called Noetherian if Noetherian as $R$-module, i.e. every ideal is f.g.

Prop: If $R$ is Noetherian then every f.g. $R$-module is Noetherian.

Proof: By induction on the minimum number of generators for $V$.

If $n = 1$, $V \cong R \cdot v_1$. Let $f: R \rightarrow V, 1 \mapsto v_1$, is surjective.

Then $R/I \cong V$ as $R$-modules, $I = \ker f$.

Since $R$ Noetherian, so is $R/I$, hence $V$.

If $n > 1: V = R \cdot v_1, \ldots, v_n$. Then $U = R \cdot v_1 \cup \ldots \cup \cup v_n$ Noetherian by induction.

Also $V/U$ Noetherian since generated by one element, $v_n$.

Lemma: $V$ Noetherian.
(3.43)

a) Every principal ideal domain is noetherian.
   \( K, K[X], \mathbb{Z}, \ldots \)

b) \( K[X_1, X_2, \ldots] \) infinitely many vars is not noetherian.
   has the submodule \( I = (X_1, X_2, \ldots) \) which is not f.g.

Prop 3.44: If \( R \) is noetherian, it has a maximal ideal.

Remark: Also holds if \( R \) not noetherian! (Zorn's Lemma)

Without proof (but possible with your knowledge):

Theorem (Hilbert Basis Theorem): If \( R \) is noetherian, then every \( R \)-algebra
is noetherian.

Now, back to business:

Theorem 3.47: Let \( R \) be integrally closed and noetherian, \( K := \mathbb{Q}(R) \).
Let \( L \) be a finite separable extension of \( K \).
Then \( S := R \cap L \) is a finitely generated \( R \)-module and a noetherian ring.

Proof: Let \( \alpha_1, \ldots, \alpha_n \) be a \( K \)-basis of \( L \). By Lemma 3.31 there is
\( \alpha \in R \backslash \text{ord} \) s.t. \( \alpha i \in \mathbb{Q} \). Then \( \{ \alpha_1, \ldots, \alpha_n, \alpha \} \) is still a \( K \)-basis of \( L \).
Can thus assume \( \alpha \in S \).
The trace form on \( K \cap L \) is non-degenerate by Corollary 2.43
\( \Rightarrow \) The \( K \)-basis \( \alpha_1, \ldots, \alpha_n, \alpha \) of \( L \) has a dual basis \( \beta_1, \ldots, \beta_n, \alpha^* \),
\( \beta_i \in R \cap L \).
\( \text{Tr}_{K}(\alpha \cdot \alpha_i) = \delta_{ij} \).
Let \( \alpha \in S \). Then \( \alpha = \sum \beta_i \alpha_i \) with \( \beta_i \in K \).
Since $\alpha_i, \alpha \in S \Rightarrow \alpha \cdot \alpha_i \in S$.

3.24. Corollary

Hence $R \ni \text{Tr}_R(\alpha \alpha_i) = \text{Tr}_R(\sum_{j=1}^n \beta_i \cdot \alpha_j \cdot \alpha_i) = \sum_{j=1}^n \beta_i \cdot \delta_{ij} \cdot \beta_j$,

$\Rightarrow \alpha \in R_S \langle \alpha_1^\prime, \ldots, \alpha_n^\prime \rangle$.

$\Rightarrow S \subseteq R_S \langle \alpha_1^\prime, \ldots, \alpha_n^\prime \rangle \ni S$ submodule of a free $R$-module.

$\Rightarrow S$ free $R$-module since $R$ noetherian.

By Hilbert's Basis Theorem: $S$ is noetherian. $\Box$

3.48. Corollary: Every ring of integers $G$ is a finitely generated $\mathbb{Z}$-module and a noetherian ring. $\Box$

3.7 Ring of integers is free

Note: $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$, every element of the form $a + bi$ with unique $a, b \in \mathbb{Z}$.

3.49. Let $V$ be an $R$-module. A subset $S \subseteq V$ is linearly independent if whenever

$$\sum_{i \in S} r_i v_i = 0 \Rightarrow r_i = 0 \text{ for } i \in S,$$

A basis of $V$ is a linearly independent generating set.

$V$ is called free if it has a basis.

Note: $V$ free $\Rightarrow$ every $v \in V$ is of the form $\sum_{i \in S} r_i v_i$ with unique $r_i \in R$.

Ex: 3.50

a) $R$ itself is a free $R$-module.

So is $R^+ = \bigoplus_{i \in S} R = \{ (r_i)_{i \in S} \mid r_i \in R \}$ for some $I$.

In fact: $V$ free $\Leftrightarrow V \cong R^I$ for some $I$.

b) Every $K$-vector space is a free $K$-module.