NOTE: ALL RINGS IN THIS CLASS ARE COMMUTATIVE WITH MULTIPLICATIVE IDENTITY 1 (1 \cdot a = a for every \( a \in A \), where \( A \) is the ring) AND ADDITIVE IDENTITY 0 (0 + a = a for every \( a \in A \) where \( A \) is the ring)

**Definition 2.1.** A ring \( R \) is called a principal ideal domain if for any ideal \( I \subset R \) there is an element \( a \in I \), such that \( I = Ra \).

Later we’ll see that for the rings we work with in this class, principal ideal domains and unique factorization domains are the same thing.

**Proposition 2.2** (Easy). Let \( A \subset B \). Then \( b \) is integral over \( A \) \( \iff \) \( A[b] \) is finitely generated as an \( A \)-module.

**Proof.** (\( \Rightarrow \)) Writing
\[
b^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0 = 0,
\]
we see that \( b^n \) is contained in the \( A \)-module generated by \( \{1, b, \ldots, b^{n-1} \} \).

Similarly, by induction on \( r > 0 \), we see that \( b^{n+r} \) is contained in the \( A \)-module generated by \( \{1, b, \ldots, b^{n-1} \} \), since
\[
b^{n+r} = (b^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0)b^r,
\]
and is therefore contained in \( A \)-module generated by \( \{1, b, \ldots, b^{n+(r-1)} \} \).

(\( \Leftarrow \)) Let \( \sum_{i=1}^{N_i} a_{ij}b^i \) generate \( A[b] \). Then for \( M \) larger than the largest \( N_i \), the element \( b^M \) can be written as \( A \)-linear combination of lower powers of \( b \). This yields an integral polynomial over \( A \) satisfied by \( b \). \( \square \)

**Definition 2.3.** We say that \( A \subset B \) is integral, or that \( B \) is integral over \( A \) if every \( b \in B \) is integral over \( A \).

**Corollary 2.4.** If \( A \subset B \) is integral and \( B \subset C \) is integral, then \( A \subset C \) is integral.

**Proof.** Exercise. \( \square \)

**Example 2.5.** The primitive \( n \)-th root of unity \( \xi_b \) is integral over \( \mathbb{Z} \) since it satisfies \( \xi^n - 1 = 0 \).

**Example 2.6.** \( i/2 \) is not integral over \( \mathbb{Z} \). Let’s look at the algebra \( B \) it generates over \( \mathbb{Z} \). Suppose it was finitely generated as an \( \mathbb{Z} \)-module. Then if \( M \) is the maximal power of 2 appearing in the denominator of a generator, then \( M \) is the maximal power of 2 appearing in the denominator of any element of \( B \). But there are arbitrarily high powers of 2 appearing in the denominator of elements in \( B \).
2

**Theorem 2.7.** (Cayley-Hamilton) Let $A \subset B$, where $A$ and $B$ are domains. Suppose that $M$ is a finitely generated $A$-module with generators $m_1, \ldots, m_n$. Suppose that $M$ is also a faithful $A[b]$-module (this means the only element that annihilates all of $M$ is 0) and that $b$ acts on the generators $m_i$ in the following way

\[
 bm_i = \sum_{j=1}^{n} a_{ij}m_j.
\]

Then $b$ satisfies the equation

\[
 \det \begin{pmatrix}
 b-a_{11} & -a_{12} & \cdots & -a_{1n} \\
 -a_{21} & b-a_{22} & \cdots & -a_{2n} \\
 \cdots & \cdots & \cdots & \cdots \\
 -a_{n2} & -a_{n1} & \cdots & b-a_{nn}
\end{pmatrix} = 0.
\]

**Proof.** Let $T$ be the matrix $bI - [a_{ij}]$. The theorem then says that $\det T = 0$. Notice that we can consider $T$ as an endomorphism of $M^n$ by writing

\[
 \begin{pmatrix}
 b-a_{11} & -a_{12} & \cdots & -a_{1n} \\
 -a_{21} & b-a_{22} & \cdots & -a_{2n} \\
 \cdots & \cdots & \cdots & \cdots \\
 -a_{n2} & -a_{n1} & \cdots & b-a_{nn}
\end{pmatrix} \begin{pmatrix}
 x_1 \\
 \vdots \\
 x_n
\end{pmatrix} = \begin{pmatrix}
 b - \sum_{j=1}^{n} a_{1j}x_j \\
 \vdots \\
 b - \sum_{j=1}^{n} a_{nj}x_j
\end{pmatrix}
\]

where the $x_i$ are elements of $M$. Let $(x_1, \ldots, x_n)$ be $(m_1, \ldots, m_n)$, we obtain

\[
 \begin{pmatrix}
 b-a_{11} & -a_{12} & \cdots & -a_{1n} \\
 -a_{21} & b-a_{22} & \cdots & -a_{2n} \\
 \cdots & \cdots & \cdots & \cdots \\
 -a_{n2} & -a_{n1} & \cdots & b-a_{nn}
\end{pmatrix} \begin{pmatrix}
 m_1 \\
 \vdots \\
 m_n
\end{pmatrix} = \begin{pmatrix}
 b - \sum_{j=1}^{n} a_{1j}m_j \\
 \vdots \\
 b - \sum_{j=1}^{n} a_{nj}m_j
\end{pmatrix} = \begin{pmatrix}
 0 \\
 \vdots \\
 0
\end{pmatrix}
\]

by equation (1). Now, recall from linear algebra (exercise) that there is a matrix $U$, called the adjoint of $T$, for which $UT = \det TI$. We obtain

\[
 \begin{pmatrix}
 \det T & 0 & \cdots & 0 \\
 0 & \det T & \cdots & 0 \\
 \cdots & \cdots & \cdots & \cdots \\
 0 & 0 & \cdots & \det T
\end{pmatrix} \begin{pmatrix}
 m_1 \\
 \vdots \\
 m_n
\end{pmatrix} = \begin{pmatrix}
 \det T \\
 \vdots \\
 \det T
\end{pmatrix} = \begin{pmatrix}
 0 \\
 \vdots \\
 0
\end{pmatrix}
\]
so \((\det T)m_i = 0\) for each \(m_i\). Hence \((\det T) = 0\), since \((\det T) \in A[b] \) and \(A[b]\) acts faithfully on \(M\).

\[\Box\]

**Corollary 2.8.** Let \(A \subset B\) and let \(b \in B\). If \(A[b] \subset B' \subset B\) for a ring \(B\) that is finitely generated as an \(A\)-module, then \(b\) is integral over \(A\).

**Proof.** Since \(b \in B'\), multiplication by \(b\) sends \(B'\) to \(B'\). Moreover, the resulting map is \(A\)-linear (by distributivity of multiplication). Let \(m_1, \ldots, m_n\) generated \(B'\) as an \(A\)-module. Then, for each \(i\) with \(1 \leq i \leq n\), we can write

\[bx_i = \sum_{j=1}^{i} a_{ij} x_j,\]

Clearly, the equation

\[
\begin{vmatrix}
 b - a_{11} & -a_{21} & \cdots & -a_{1n} \\
-a_{12} & b - a_{22} & \cdots & -a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
-a_{1n} & -a_{2n} & \cdots & b - a_{nn}
\end{vmatrix} = 0
\]

is integral.

\[\Box\]

For now, let’s note the following corollary.

**Corollary 2.9.** Let \(A \subset B\). Then the set of all elements in \(B\) that are integral over \(A\) is a ring.

**Proof.** We need only show that the elements in \(B\) that are integral over \(A\) forms a ring. If \(\alpha\) and \(\beta\) are integral over \(A\), then \(A[\alpha, \beta]\) is finitely generated as an \(A\)-module. Hence, \(-\alpha, \alpha + \beta, \) and \(\alpha\beta\) are all integral over \(A\) since they are contained in \(A[\alpha, \beta]\), by the Cayley-Hamilton theorem above.

\[\Box\]

The following is immediate.

**Corollary 2.10.** Let \(K\) be an extension of \(\mathbb{Q}\). Then the set of all elements in \(K\) that are integral over \(\mathbb{Z}\) is a ring.

Again let \(A \subset B\). The set \(B'\) of elements of \(B\) that are integral over \(A\) is a ring. We call this ring \(B'\) the integral closure of \(A\) in \(B\).

**Definition 2.11.** Let \(K\) be a number field (a finite extension of \(\mathbb{Q}\)). The ring of integers of \(K\) is integral closure of \(\mathbb{Z}\) in \(K\). We denote is as \(\mathcal{O}_K\).

Ask if people have seen localization.

**Definition 2.12.** We say that a domain \(B\) is integrally closed if it is integrally closed in its field of fractions.
Proposition 2.13. Let $A \subset B$, where $A$ and $B$ are domains. The ring $B$ is integrally closed over $A$ if and only if $B$ is integrally closed in its field of fractions.

Proof. Exercise. \qed

Example 2.14. Any unique factorization domain is integrally closed.

Let’s do a preview of what properties we want rings of integers to have. First let’s recall some features of $\mathbb{Z}$:

1. $\mathbb{Z}$ is Noetherian.
2. $\mathbb{Z}$ is 1-dimensional.
3. $\mathbb{Z}$ is a unique factorization domain.
4. $\mathbb{Z}$ is a principal ideal domain.

Recall what a Noetherian ring is.

Definition 2.15. A ring $R$ is Noetherian if every ideal is finitely generated as an $R$-module. Equivalently, $R$ is if every ascending chain of ideals terminates.

Incidentally, we will later see that the conditions (1) and (2) are often equivalent in the situations we examine.

The rings $\mathcal{O}_K$ will have the properties that

1. $\mathcal{O}_K$ is Noetherian.
2. $\mathcal{O}_K$ is 1-dimensional.
3. $\mathcal{O}_K$ has unique factorization for ideals.
4. $\mathcal{O}_K$ is locally a principal ideal domain.
5. It is possible that $\mathcal{O}_K$ is not a unique factorization domain and that it is not a principal ideal domain.

In fact, any subring $B$ of a number field $K$ that is integral over $\mathbb{Z}$ will be Noetherian and 1-dimensional. That is the Krull-Akizuki theorem which we will eventually prove.

We used the work “locally” above. Let’s define it.