Math 361 lecture for Wednesday, Week 2

Algebraic integers

Definition 1. Let A and B be integral domains (rings with no zero divisors) with $A \subseteq B$. An element of $\alpha \in B$ is *integral over* A if there exists a monic polynomial $p \in A[x]$ such that $p(\alpha) = 0$.

Note that if A in the definition is a field, then $a \in B$ is integral over A if and only if a is algebraic over A.

Our main interest will be in elements of $\mathbb{C}$ that are integral over $\mathbb{Z}$. These are integer solutions in $\mathbb{C}$ to monic polynomials with coefficients in $\mathbb{Z}$. For example $(1 + \sqrt{5})/2$ is integral over $\mathbb{Z}$ since it is a root of $x^2 - x - 1$. Similarly, i is integral over $\mathbb{Z}$ since it is a root of $x^2 + 1$. The word "monic" in the definition of integrality is crucial. For instance, consider the case $B = \mathbb{Q}$ and $A = \mathbb{Z}$. Every rational number is a root of a polynomial with integer coefficients, e.g., a/b satisfies $bx - a \in \mathbb{Z}[x]$. However, as the following proposition shows, a rational solution to a monic polynomial over the integers must be an integer.

Proposition 2. A rational number is integral over $\mathbb{Z}$ if and only if it is an integer.

Proof. One direction is immediate: if $a \in \mathbb{Z}$, then a is integral over $\mathbb{Z}$ since it satisfies $x - a \in \mathbb{Z}[x]$. For the other direction, suppose a/b is a rational number that is integral over $\mathbb{Z}$. Without loss of generality, assume a/b is in lowest terms and that $b > 0$. Since a/b is integral over $\mathbb{Z}$, there exists a polynomial $p = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ with $c_i \in \mathbb{Z}$ such that $p(a/b) = 0$. So

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0.$$

Clear denominators by multiplying through by b^n:

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n = 0.$$

We see that

$$a^n = 0 \bmod b.$$

If $b \neq 1$, then some prime in the factorization of b must divide a, However, that cannot happen since a/b is in lowest terms. It follows that $b = 1$ and $a/b = a \in \mathbb{Z}$. □

Exercise 3. The number $\sqrt{2}$ is integral over $\mathbb{Z}$ since it is a zero of the monic polynomial $x^2 - 2 \in \mathbb{Z}[x]$. Show that $1/\sqrt{2}$ is not integral over $\mathbb{Z}$ by imitating the method used in the proof of Proposition 2 (clearing denominators and getting a contradiction).

Theorem 4. Let A and B be domains with $A \subseteq B$, and let $\alpha \in B$. Then the following are equivalent.

1. α is integral over A.
2. $A[\alpha] := \{f(\alpha) : f \in A[x]\}$ is a finitely generated A-module.
3. There exists a finitely generated A-module M in B such that $\alpha M \subseteq M$. (Here, $\alpha M = \{\alpha m : m \in M\}$).

Proof. ($1 \Rightarrow 2$) Since α is integral over A, it is the root of a monic polynomial $p \in A[x]$. Say $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in A$. Then since $p(\alpha) = 0$, we have

$$\alpha^n = -a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1}.$$

It follows that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ generates $A[\alpha]$ as an A-module.

($2 \Rightarrow 3$) Let $M = A[\alpha]$. Then $\alpha M \subseteq M$.

($3 \Rightarrow 1$) Here is the most interesting part of the proof. Suppose M is a finitely generated A-module in B and $\alpha M \subseteq M$. Say M is generated by $b_1, \ldots, b_n \in B$ as an A-module. Since $\alpha M \subseteq M$, there exist $a_{ij} \in A$ such that

$$\begin{aligned}
\alpha b_1 &= a_{11}b_1 + \cdots + a_{1n}b_n \\
\alpha b_2 &= a_{21}b_1 + \cdots + a_{2n}b_n \\
&\vdots \quad \vdots \\
\alpha b_n &= a_{n1}b_1 + \cdots + a_{nn}b_n.
\end{aligned}$$

Letting $T = (a_{ij})$ and $b = (b_1 \ \ldots \ b_n)^t$ (where the superscript of t denotes the transpose) we can write these equations more succinctly as

$$\alpha b = Tb.$$

Hence, $(\alpha I_n - T)b = 0$, which implies $\det(\alpha I_n - T) = 0$. Let $p(x) := \det(xI_n - T)$. Then

$$p(x) = \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix} = x^n + \text{ lower order terms }.$$

So p is a monic polynomial with coefficients in A and having α as a root. Therefore, α is integral over A. □

Lemma 5. Let $A \subseteq B \subseteq C$ be rings. If B is finitely generated as an A-module and C is finitely generated as a B-module, then C is finitely generated as an A-module.

Proof. If $\{b_i\}$ is a finite generating set for B as an A-module and $\{c_j\}$ is a finite generating set for C as a B-module, it is straightforward to check that $\{a_i b_j\}$ is a finite generating set for C as an A-module. □

Corollary 6. Let $A \subseteq B$ be domains. The set of elements of B that are integral over A forms a subring of B.

Proof. It suffices to show that the set of elements of B that are integral over A is closed under addition and multiplication. Let $\alpha, \beta \in B$ be integral over A. Consider the *tower* of rings

$$A \subseteq A[\alpha] \subseteq A[\alpha, \beta].$$

(To be clear, $A[\alpha, \beta] := \{f(\alpha, \beta) : f(x, y) \in A[x, y]\}$, all polynomials in α and β with coefficients in A. It is the subring of B generated by α and β.) By Theorem 4, we have that $A[\alpha]$ and $A[\beta]$ are finitely generated as A-modules. It is straightforward to check that since $A[\beta]$ is finitely generated as an A-module, say by $b_1, \ldots, b_n$, it follows that $A[\alpha, \beta]$ is finitely generated as a $A[\alpha]$-module by $b_1, \ldots, b_n$. By Lemma 5, it follows that $A[\alpha, \beta]$ is a finitely generated A-module.

Next, let $M := A[\alpha, \beta]$. Apply Theorem 4, part 3, noting that since $A[\alpha, \beta]$ is a ring,

$$(\alpha + \beta)M \subseteq M \quad \text{and} \quad (\alpha\beta)M \subseteq M.$$

It follows that $\alpha + \beta$ and $\alpha\beta$ are integral over A. □

Exercise 7. Is there a converse to Lemma 5?

Next time, we will start to focus on an object of central interest in this course—the algebraic integers:

Definition 8. The *algebraic integers* are the elements of $\mathbb{C}$ that are integral over $\mathbb{Z}$:

$$\mathfrak{O} := \{\alpha \in \mathbb{C} : p(\alpha) = 0 \text{ for some monic } p \in \mathbb{Z}[x]\}.$$

Corollary 9. The algebraic integers, $\mathfrak{O}$, are a ring.

For example, this corollary tells us that since $\sqrt[3]{2}$ and i are algebraic integers (roots of $x^3 - 2$ and $x^2 + 1$, respectively), there must be a monic polynomial p with integer coefficients such that $p(\sqrt[3]{2} + i) = 0$. The proof of Theorem 4 shows how to calculate p.