California State University
SAN MARCOS

Integral Bases for Radical Cubic Extensions

Alejandro Leon Figueroa, Carmen Gutierrez, Noah Lowery, Brittany Russell
Grad Mentor: Dylan Scofield
Faculty Advisor: Hanson Smith

HOLOGIC®
DEPARTMENT OF EDUCATION ★ UNITED STATES OF AMERICA ★
The Lawrence E. & Neva B. Fenstermaker Foundation

Background and Motivation

Number theory is focused on studying the *integers*. This fundamental set of numbers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is denoted $\mathbb{Z}$ for the German word "Zahlen" which means "numbers". We can add, subtract, and multiply integers; however, if we want to divide any integer by another non-zero integer, we need a larger set of numbers. This set is the *rational numbers*. They are denoted by $\mathbb{Q}$ for "quotient". Explicitly,

$$\mathbb{Q} = \left\{ \frac{a}{b} \ : \ a, b \in \mathbb{Z}, \ b \neq 0 \right\}.$$

To answer number theoretic questions, mathematicians such as Gauss, Germain, Dirichlet, Kummer, and Dedekind realized that there are numbers that are not integers or rationals, but behave similar to integers and rationals. For example, $\sqrt{2}$ is not an integer, but it is a solution to the integer polynomial $x^2 - 2$. Therefore, $\sqrt{2}$ is considered an *algebraic integer*. Throwing $\sqrt{2}$ into the rationals, we get a larger analog of the rationals $\mathbb{Q}(\sqrt{2})$, called a *number field*. This number field also has a larger analog of the integers $\mathbb{Z}[\sqrt{2}]$ that is called a *number ring* or the *ring of integers of* $\mathbb{Q}(\sqrt{2})$.

Quadratic number fields like the one above have been well-studied. However, cubic polynomials serve as a natural progression from quadratic polynomials. Thus, we began our research by looking into *radical cubics*, polynomials of the form $x^3 - c$ with $c \in \mathbb{Z}$. A root $\sqrt[3]{c}$ generates a number field $\mathbb{Q}(\sqrt[3]{c})$, and we wished to describe the ring of integers of this number field. Diagrammatically, our question was

$$\begin{tikzcd}
? \arrow[r, "\subset"] \arrow[d, dash] & \mathbb{Q}(\sqrt[3]{c}) \arrow[d, dash] \\
\mathbb{Z} \arrow[r, "\subset"] & \mathbb{Q}
\end{tikzcd}$$

What is the ring of integers of $\mathbb{Q}(\sqrt[3]{c})$?

Generalizing the integers means extending the concept of integers to more abstract and versatile structures. *Algebraic integers* are the solutions to integer polynomials with leading coefficient 1. Though technical, this definition allows our new rings of integers to retain a version of prime factorization. As we will see in our proof, prime factorization allows us to break the infinitude of the integers into manageable finite pieces.

Our Main Theorem

Theorem. *Let $x^3 - c$ in $\mathbb{Z}[x]$ be an irreducible polynomial and suppose c is cube-free. Write $c = hk^2$ with $\gcd(h, k) = 1$ and h, k square-free.*

CASE 1: *If c does not have remainder 1 or -1 when we divide by 9, then*

$$\left\{1, \sqrt[3]{hk^2}, \sqrt[3]{h^2k}\right\}$$

is an integral basis for the ring of integers of $\mathbb{Q}(\sqrt[3]{c})$. In other words, the elements in the ring of integers have the form

$$a_1 + a_2\sqrt[3]{hk^2} + a_3\sqrt[3]{h^2k}, \quad \textit{with} \ a_1, a_2, a_3 \in \mathbb{Z}.$$

CASE 2: *If c has remainder 1 or -1 when we divide by 9, then*

$$\left\{1, \sqrt[3]{hk^2}, \frac{\sqrt[3]{h^2k} \pm k\sqrt[3]{hk^2} + k}{3}\right\}$$

is an integral basis for the ring of integers of $\mathbb{Q}(\sqrt[3]{c})$. We take the plus when c has remainder 1 and the minus when c has remainder -1. The elements in the ring of integers have the form

$$a_1 + a_2\sqrt[3]{hk^2} + a_3\frac{\sqrt[3]{h^2k} \pm k\sqrt[3]{hk^2} + k}{3}, \quad \textit{with} \ a_1, a_2, a_3 \in \mathbb{Z}.$$

Examples

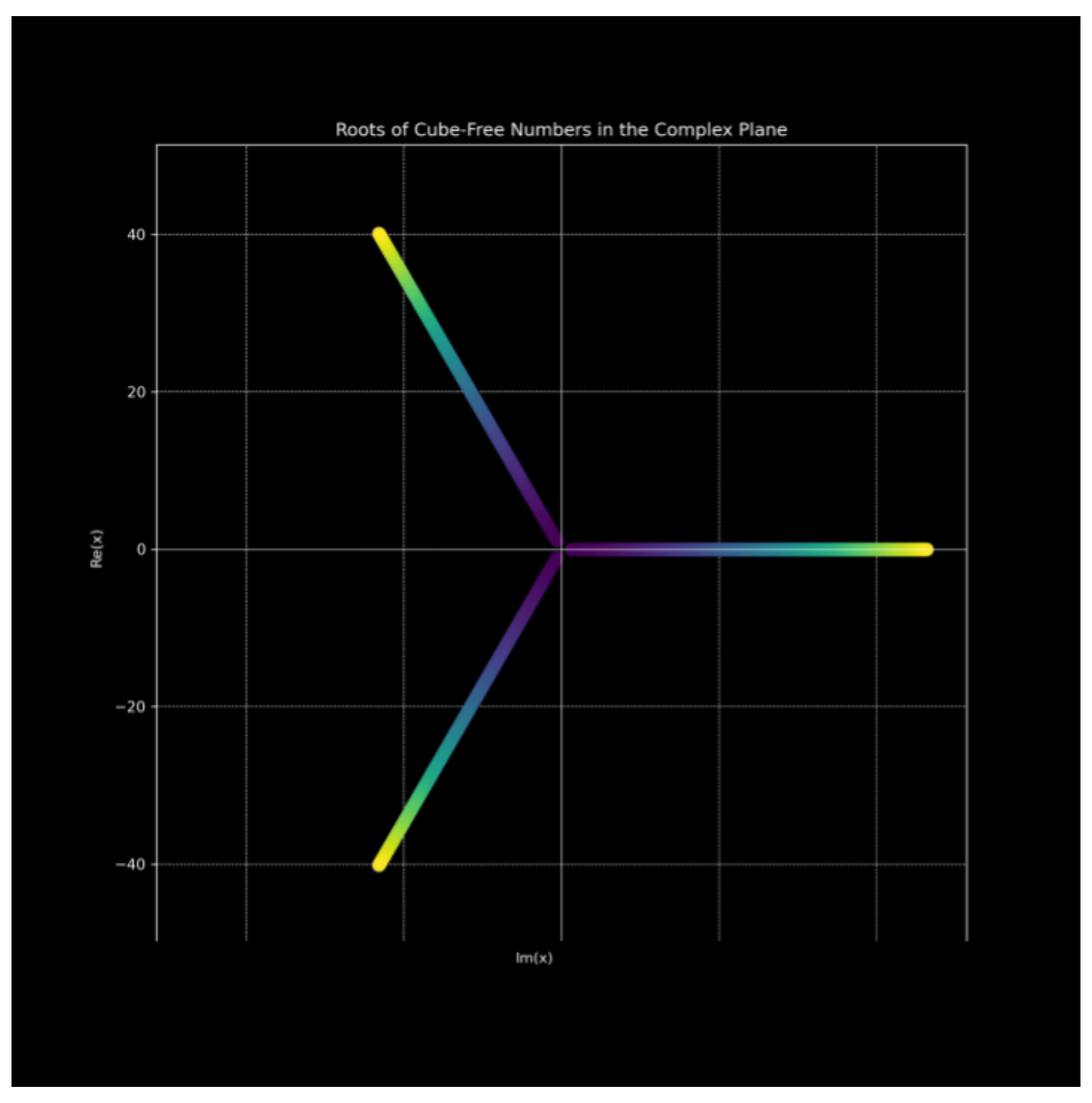

Figure 1: *The roots of $x^3 - c$ in the complex plane.*

Example 1: Consider $x^3 - 18$. Here, $c = 18 = 2 \cdot 3^2$, so $h = 2$ and $k = 3$. We are in Case 1 since 18 has remainder 0 when divided by 9. It has the integral basis

$$\left\{1, \sqrt[3]{18}, \sqrt[3]{12}\right\},$$

so elements of the ring of integers have the form

$$a_1 + a_2\sqrt[3]{18} + a_3\sqrt[3]{12}.$$

Example 2.1: Consider $x^3 - 10$. Here, $c = 10 = 10 \cdot 1^2$, so $h = 10$ and $k = 1$. We are in Case 2 since 10 has remainder 1 when divided by 9. An integral basis is

$$\left\{1, \sqrt[3]{10}, \frac{\sqrt[3]{100} + \sqrt[3]{10} + 1}{3}\right\},$$

and elements of the ring of integers have the form

$$a_1 + a_2\sqrt[3]{10} + a_3\frac{\sqrt[3]{100} + \sqrt[3]{10} + 1}{3}.$$

Example 2.2: Now let's look at the importance of c being cube-free. Consider $x^3 - 80$. We see that $\sqrt[3]{80} = 2\sqrt[3]{10}$, so $\sqrt[3]{80}$ generates the same number field as in Ex.2.1. Thus, we do not lose generality by restricting c to be cube-free.

Key Concepts for the Proof

- Primes are the building blocks of the integers, and our proof will work prime-by-prime, building from local pieces to a global result.
- Let p be a prime. If a possible integral basis $\mathcal{A}$ is sufficiently big with respect to the prime p, then we say it is *p-maximal*. If a possible integral basis is p-maximal for every prime p, then it is a true integral basis!
- Associated to a possible integral basis $\mathcal{A}$ is an integer called the *discriminant*, denoted $\operatorname{Disc}\mathcal{A}$. The highest power of a prime p dividing $\operatorname{Disc}\mathcal{A}$ tells us information about the p-maximality of $\mathcal{A}$.
- If $\mathcal{A}$ and $\mathcal{B}$ are two integral bases, they are related by the change-of-basis matrix $\underset{\mathcal{A}\to\mathcal{B}}{M}$. Their discriminants are related by the determinant, and we have the key equation

$$\operatorname{Disc}\mathcal{A} \cdot \left|\det\left(\underset{\mathcal{A}\to\mathcal{B}}{M}\right)\right|^2 = \operatorname{Disc}\mathcal{B}. \tag{1}$$

Proof Sketch

- We start with the power basis $\mathcal{B} = \{1, \sqrt[3]{hk^2}, \sqrt[3]{h^2k^4}\}$. Since $\operatorname{Disc}\mathcal{B} = -27h^2k^4$, we know that $\mathcal{B}$ is p-maximal for every prime that does not divide $3hk$.
- We use Uchida's criterion, a deep result for studying power bases, to show that $\mathcal{B}$ is p-maximal for p dividing h. Uchida's criterion also tells us $\mathcal{B}$ is 3-maximal so long as $c = hk^2 \not\equiv 0, \pm 1 \bmod 9$.
- Uchida's criterion tells us $\mathcal{C} = \{1, \sqrt[3]{h^2k}, \sqrt[3]{h^4k^2}\}$ is p-maximal for primes p dividing k. Some work with equation (1) shows that $\{1, \sqrt[3]{hk^2}, \sqrt[3]{h^2k}\}$ is p-maximal for all primes not equal to 3, and 3-maximal when $c = hk^2 \not\equiv \pm 1 \bmod 9$.
- When $c \equiv \pm 1 \bmod 9$, computation in SageMath shows $(\sqrt[3]{h^2k} \pm k\sqrt[3]{hk^2} + k)/3$ is an algebraic integer. Equation (1) finishes the proof.