Algebraic Number Theory

ants in your pants

Jay Zhao

Contents

§1. Algebraic Integers

§1. 1. Algebraic Numbers and Algebraic Integers

Minimal Polynomial For $\alpha \in \mathbb{C}$ α's minimal polynomial P over $\mathbb{Q}$ is such that:

1. The leading coefficient of P is 1.
2. $P(\alpha) = 0$.
3. $\deg P$ is minimal.

We refer to $\deg P$ as **the degree** of α.

Example:

- $\sqrt{2}$ has the minimal polynomial $x^2 - 2$.
- i has the minimal polynomial $x^2 + 1$.

☂ **Theorem 1.1.1**: $A(\alpha) = 0$ then there exists Q(x) such that $A(x) \equiv Q(x)P(x)$.

Proof: For the sake of contradiction assume otherwise

By polynomial division $A(x) \equiv P(x)Q(x) + R(x)$ where $\deg R(x) < \deg P(x)$ and $R(x) \not\equiv 0$. Then $0 = A(\alpha) = 0Q(\alpha) + R(\alpha) = R(\alpha)$. $R(\alpha) = 0$, this contradicts the minimality of $\deg P(x)$. ∎

💔 **Corollary 1.1.1.1**: P(x) is the minimal polynomial if and only if it is irreducible.

Algebraic Number An algebraic number is any $\alpha \in \mathbb{C}$ which is the root of some polynomial with coefficients in $\mathbb{Q}$. The set of algebraic numbers is denoted $\overline{\mathbb{Q}}$

Algebraic Integer Consider an algebraic number α and its minimal polynomial P. If it turns out the coefficients of P are integers, then we say that α is an algebraic integer.

☂ **Theorem 1.1.2** (Gauss's Lemma): A polynomial is irreducible over the integer if and only if it is irreducible over the rational.

A result of this is that to check that a number is an algebraic integer, it is sufficient to find a monic polynomial with it as a root with integer coefficient.

Rational Integer the elements of $\mathbb{Z}$ are referred to as rational integers.

Example:

$$4, i, \sqrt[3]{2}, \sqrt{2} + \sqrt{3}$$

are all algebraic integers because they are the roots of $x-4$, x^2+1, x^3-2 and $(x^2-5)^2-24$.

The number $\frac{1}{2}$ has minimal polynomial $x-\frac{1}{2}$, so it's an algebraic number but not ans algebraic integer. It also implies that no monic integer polynomial has $\frac{1}{2}$ as a root.

🟪 **Lemma 1.1.3** (Rational algebraic integers are rational integers): An algebraic integer is rational if and and only if it is a rational integer. $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$

Proof: For all $n \in \mathbb{Z}$, n is the root of $x-n$. Conversely the minimal polynomial of $\frac{p}{q}$ is $x-\frac{p}{q}$ and so $\frac{p}{q}$ is an algebraic integer only if $\frac{p}{q}$ is an integer. ∎

🟪 **Lemma 1.1.4**: The algebraic integers $\overline{\mathbb{Z}}$ forms a ring. The algebraic numbers $\overline{\mathbb{Q}}$ forms a field

Proof: ∎

§1. 2. Number Fields

Number Field A number field K is field containing $\mathbb{Q}$ as a subfield which is a *finite-dimensional* $\mathbb{Q}$ vector space. The **degree** of K is its dimension.

Example: Consider the field $K = Q\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$. This is a field extension of $\mathbb{Q}$, and has degree 2 (the basis being 1 and $\sqrt{2}$).

Note that (□) *over* [□] *means that it is a field of fractions. This difference doesn't matter though because they are the same thing in this context.*

☂ **Theorem 1.2.1** (Artin's primitive element theorem): Every number field K is isomorphic to $\mathbb{Q}(\alpha)$ for some algebraic number α.

§1. 3. Problems

Exercise I: Find a polynomial with integer coefficients which has $\sqrt{2}+\sqrt[3]{3}$ as a root

Solution: Let $x = \sqrt{2}+\sqrt[3]{3}$. It must be the case that $\left(x-\sqrt{2}\right)^3 = 3$. Expanding this we get that $x^3 - 3\sqrt{2}x^2 + 6x - 2\sqrt{2} = 3$. Hence $x^3 + 6x - 3 = \sqrt{2}(3x^2+2)$. Squaring both sides:

$$\begin{aligned}(x^3+6x-3)^2 &= 2(3x^2+2)^2\\ (x^3+6x-3)^2 - 2(3x^2+2)^2 &= 0\\ x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1 &= 0\end{aligned}$$

Exercise II (Brazil 2006): Let p be an irreducible polynomial in $\mathbb{Q}[x]$ and degree larger than 1. Prove that if p has two roots r and s whose product is 1 then the degree of p is even.

Solution: Since $p(r) = 0$, $p\left(\frac{1}{r}\right)$ and p is irreducible it must be that p is the minimal polynomial of p and $\frac{1}{p}$.

Let $d = \deg$. Let $a = \frac{[x^0]p}{[x^d]p}$. Consider $ap(x) - x^d p\left(\frac{1}{x}\right)$, the leading coefficient of both $p(x)$ and $x^d p\left(\frac{1}{x}\right)$ is $[x^d]p$ and their degrees are both d. This means that there exists a polynomial with degree less than d for which r is root. Since p is the minimal polynomial of r that polynomial has to be 0.

Hence $ap(x) \equiv x^d p\left(\frac{1}{x}\right)$. First note that 0, 1 and –1 cannot be roots of $p(x)$ as that would mean the polynomial p has a factor of x, $x-1$ or $x+1$.

If $q(x) \mid p(x)$ where $q \in \mathbb{C}[x]$ then $q(x) \mid x^d p\left(\frac{1}{x}\right)$. So $p(x)$ and $p\left(\frac{1}{x}\right)$ must have the same multi-set of roots counting multiplicity.

Consider the classes of roots $a \equiv b$ if $a = b$ or $a = \frac{1}{b}$. The number of times a appears in the multi-set of roots must be the same as number of time $\frac{1}{a}$ appears. So the number of roots that is a part of each class is even. Thus the total number of roots in the multi-set is even.

So the degree of the polynomial is even.

Exercise III: Consider n roots of unity $\varepsilon_1, ..., \varepsilon_n$. Assume the average $\frac{1}{n}(\varepsilon_1 + ... + \varepsilon_n)$ is an algebraic integer. Prove that either the average is 0 or $\varepsilon_1 = \cdot = \varepsilon_n$

Solution: Consider when the sum of the roots of unity is not 0 and when not all the roots of unity are the same, we have by the triangle inequality that if the average is $x = \frac{1}{n}(\varepsilon_1 + \varepsilon_2 + ... + \varepsilon_n)$ then $|x| < 1$.

Now consider any conjugate of x, again it it is the sum of roots of unity and $|x'|$ is ≤ 1. Consider the minimal polynomial of x now. The magnitude of the constant term is equal to the magnitude of the product of all the roots. Hence the magnitude of the constant term is less than 1. But it is not 0. So it must not be an integer. So this cannot happen.

The sum of the roots of unity can only be 0 or a root of unity itself, which only happens when all the roots are the same.

Exercise IV: Which rational numbers q satisfy $\cos(q\pi) \in \mathbb{Q}$

Solution:

$$\cos\left(\frac{2a}{b}\pi\right) = \frac{\varepsilon_b^a + \varepsilon_b^{-a}}{2}$$

$$2\cos\left(\frac{2a}{b}\pi\right) = \varepsilon_b^a + \varepsilon_b^{-a}$$

We have that $\Phi_b(\varepsilon_b^a) = 0$ If there is an integer polynomial P such that $P\left(x + \frac{1}{x}\right) = 0$ where x is ε_b^{-a} then $2\cos(2\frac{a}{b}\pi)$ must be a algebraic integer.

Luckily the cyclotomic polynomial is symmetric. Which means there does exist such a polynomial.

So $2\cos(q\pi)$ is an integer. But it's also bounded between -1 and 1. This means $\cos(q\pi) = -1, -\frac{1}{2}, \frac{1}{2}, 1$.

§2. The Ring of Integers

Galois Conjugates Let α be an algebraic number, and let $P(x)$ be its minimal polynomial of degree m. Then the m roots of P are the galois conjugates of α.

🟪 **Lemma 2.1**: An irreducible polynomial in $\mathbb{Q}[x]$ has no repeated roots

Norm Let $a \in K$ have degree m, so $\mathbb{Q}(a) \subseteq K$, set $k = \frac{\deg K}{n}$ defined as

$$N_{K/\mathbb{Q}}(\alpha) \coloneqq \left(\prod \text{Galois conj of } \alpha\right)^k$$

Trace

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \coloneqq k \cdot \left(\sum \text{Galois conj of } \alpha\right)$$

These are both "weighted averages" the add up to a weight of k. k is actually an integer because when we adjoin other things to $\mathbb{Q}(a)$ it is a tensor product.

🟪 **Lemma 2.2**: If α is an algebraic integer, it's norm and trace are rational integers.

Proof: Vieta's Formulas ∎

☂ **Theorem 2.3**: Let K be a field of degree n, and let $\alpha \in K$. Let $\mu_\alpha : K \to K$ denote the map $x \mapsto \alpha x$ viewed as a linear map of $\mathbb{Q}$-vector space. Then,

- The **norm** is the determinant $\det \mu_\alpha$
- The **trace** is the trace $\mathrm{Tr}\ \mu_\alpha$