Algebraic Number Theory

A Brief Introduction

Andy Wickell

Introduction

Algebraic number theory is a rich and diverse subfield of abstract algebra and number theory, applying the concepts of number fields and algebraic numbers to number theory to improve upon applications such as prime factorization and primality testing. In this paper, we will begin with an overview of algebraic number fields and algebraic numbers. We will then move into some important results of algebraic number theory, focusing on the quadratic, or Gauss reciprocity law.

Algebraic Number Fields

We begin with a few definitions. [1]

Definition 1. An *algebraic number $field$*, or *number $field$* is a finite field extension of the field of rationals $\mathbb{Q}$.

Definition 2. A number $\alpha \in \mathbb{C}$ is an *algebraic number* if there exists $p(x) \in \mathbb{Q}[x]$ such that $p(\alpha) = 0$. A number $\alpha \in \mathbb{C}$ is an *algebraic integer* if there exists $p(x) \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$. Generalizing, a number $\alpha \in F$ is said to be *algebraic over F* if there exists $q(x) \in F[x]$ such that $q(\alpha) = 0$

Definition 3. A polynomial $f(x) \in F[x]$ is said to be *irreducible* if there does not exist $g(x)$, $h(x) \in F[x]$ such that $f(x) = g(x)h(x)$.

With these in hand, we can present the following theorem, whose proof relies on an important result from abstract algebra.

Theorem 1. Let F be a number field. If α is algebraic over F, then there exists $m_{\alpha,F}(x) \in F[x]$, m unique and minimal, called the *minimal polynomial of α over F*. If $p(\alpha) = 0$ for some irreducible, monic $p(x) \in F[x]$, then $p = m_{\alpha,F}$. Every polynomial $q(x) \in F[x]$ where $q(\alpha) = 0$ must be divisible by $m_{\alpha,F}(x)$.

Proof. Let $g(x) \in F[x]$ be a minimal polynomial of α, and let $h(x) \in F[x]$ such that $h(\alpha) = 0$. From abstract algebra, we know that if we have $f(x)$, $g(x) \in F[x]$, $g(x) \neq 0$, then $\exists q(x)$, $r(x) \in F[x]$ with q and r unique, such that

$$f(x) = q(x)g(x) + r(x)$$

where either of the following are true:

$$0 \leq \deg(r) < \deg(g)$$

or

$$r(x) = 0.$$

In this case, there exists $q(x)$, $r(x) \in F[x]$ such that

$$h(x) = q(x)g(x) + r(x).$$

We know that $g(\alpha) = h(\alpha) = 0$ so $r(\alpha) = 0$, thus g is not minimal, and therefore $r(x) = 0$. It follows that $g(x)$ divides $h(x)$. Allowing $f(x) \in F[x]$ to be any other minimal polynomial of α permits us to repeat the above argument to yield that $g(x)$ divides $f(x)$. This implies that $f(x) = cg(x)$, $c \in F$. Since $f(x)$ is monic, $c = 1$, and thus $f(x) = g(x)$. Denote this polynomial as $m_{\alpha,F}(x)$.[1]
□

Corollary 1. An irreducible polynomial over a number field has no repeated roots in $\mathbb{C}$.

Proof. Let $f(x) \in F[x]$ be irreducible and have two identical roots, α. Then

$$f(x) = (x - \alpha)^2 g(x)$$

for $g(x) \in F[x]$. By Theorem 1, $m_{\alpha,F}(x)$ divides $f(x)$, thus $f(x) = am_{\alpha,F}(x)$ for $a \in F$. Differentiating,

$$f'(x) = (x - \alpha)g(x) + (x - \alpha)^2 g'(x).$$

It follows that $f'(\alpha) = 0$. But by Theorem 1, $m_{\alpha,F}(x)$ divides $f'(x)$, which contradicts the fact that deg(f')<deg(f). Thus f can have no repeated roots.
□

We now move to some notation. Let $\overline{\mathbb{Q}}$ denote the field of all algebraic numbers in $\mathbb{C}$. Let $\mathbb{A}$ denote all algebraic integers in $\overline{\mathbb{Q}}$. We need the following facilities in order to show some important properties of algebraic numbers.

Definition 4. An injective map $f : G \to F$ of sets G and F is called a *monomorphism*.

Definition 5. Let F be a number field. Then an *embedding* θ of F in $\mathbb{C}$ is a ring monomorphism.

We present the following theorem regarding embeddings without proof.

Theorem 2. If F is a number field of degree d, then there exists exactly d embeddings θ_j for $j = 1,\ 2, 3\ \ldots,\ d$ of F in $\mathbb{C}$.

Definition 6. Let F be an number field of degree d, and let θ_j be the set of embeddings of F in $\mathbb{C}$. The *trace of* α *from* F is

$$T_F(\alpha) = \sum_{j=1}^{d} \theta_j(\alpha).$$

The *norm of* α *from* F is

$$N_F(\alpha) = \prod_{j=1}^{d} \theta_j(\alpha).$$

The following theorem illuminates an important property of algebraic integers.

Theorem 3. Let $\alpha \in \overline{\mathbb{Q}}$, and let $m_{\alpha,\mathbb{Q}}$ be the minimal polynomial of α over $\mathbb{Q}$. Then $\alpha \in \mathbb{A}$ iff $m_{\alpha,\mathbb{Q}} \in \mathbb{Z}[x]$.

Proof. $\Rightarrow$ Let $m_{\alpha,\mathbb{Q}} \in \mathbb{Q}[x]$ and $\alpha \in \mathbb{A}$. Let $f(x) \in \mathbb{Z}[x]$ such that f is monic and of least degree and $f(\alpha) = 0$. By theorem 1, $m_{\alpha,\mathbb{Q}}(x)$ divides $f(x)$ in $\mathbb{Q}[x]$. But since $m_{\alpha,\mathbb{Q}}(x)$ is monic, by Gauss' Lemma from abstract algebra, $m_{\alpha,\mathbb{Q}}(x)$ must be in $\mathbb{Z}[x]$, so $f(x) = m_{\alpha,\mathbb{Q}}(x)$.
$\Leftarrow$ Let $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$. Then by definition $\alpha \in \mathbb{A}$.
□

We will now give a necessary definition in order to motivate an important theorem about the factorization of algebraic integers.

Definition 7. Let F be a field. Then the intersection $F \cap \mathbb{A}$ is a ring called the *ring of algebraic integers in* F, denoted as $\mathfrak{O}_F$.

Theorem 4. Let F be a number field. Then any nonzero $\alpha \in \mathfrak{O}_F$ can be factored into a product of irreducible elements. Furthermore, every nonzero element $\alpha \in \mathfrak{O}_F$ has a unique factorization into irreducibles iff every irreducible element of $\mathfrak{O}_F$ is prime.

A Reciprocity Law

We shall introduce notations and definitions [3] conducive to the Gauss reciprocity law, motivated by the congruence relation:

$$x^n \equiv a \,(\operatorname{mod} p)$$

with $n \in \mathbb{N}$, p prime, and $a \in \mathbb{Z}$. We are looking for solutions $x \in \mathbb{Z}$.

Definition 8. If m, $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ with a and m relatively prime and there exists $x \in \mathbb{Z}$ such that

$$x^n \equiv a \,(\operatorname{mod} m),$$

then x is called the n^{th} *power residue modulo m*.

We will examine the case $n = 2$, which will lead us to the Gauss reciprocity law. In this case, when there exists such an x, then we say that a is a *quadratic residue* of p, or a R p. Otherwise, we say that a is a $non - residue$ of p, or a N p.

Euler's Criterion [4] Let p be an odd prime and $a \in \mathbb{Z}$ with a and p relatively prime. Then a is a quadratic residue of p iff $a^{(p-1)/2} \equiv 1 \,(\operatorname{mod} p)$.

Definition 9. Let $\left(\frac{a}{p}\right)$, called the $Legendre's\ symbol$, be defined as follows

$$\left(\frac{a}{p}\right) = +1, \text{ if } a \,\mathrm{R}\, p$$

$$\left(\frac{a}{p}\right) = -1, \text{ if } a \,\mathrm{N}\, p$$

We can draw a parallel to these definitions to finite abelian group homomorphisms with a theorem to follow shortly.[2]

Definition 10. Let G be a finite abelian group. A homomorphism $X : G \to \mathbb{C}^\times$ is called a *character*. The set of all characters of G is denoted $\hat{G}$. The order of G is denoted as n. The Identity of $\hat{G}$ is denoted as $\hat{e}$.

Theorem 5.

$$\sum_{x \in G} X(x) = n, \text{ when } X = \hat{e}$$

or

$$\sum_{x \in G} X(x) = 0, \text{ when } X \neq \hat{e}$$

Proof The proof is trivial when $X = \hat{e}$ since the identity character maps to 1. Summing over n elements produces a sum of n. Consider $X \neq \hat{e}$. Let $x_0 \in G$ such that $X(x_0) \neq 1$. Let $S = \sum_{x \in G} X(x)$. Then $S = \sum_{x \in G} X(x) = \sum_{x \in G} X(x_0 x) = \sum_{x \in G} X(x_0)X(x) = X(x_0)S$. Thus $(1 - X(x_0))S = 0$ which implies that $S = 0$ since $X(x_0) \neq 1$.□

We will now present Legendre's Symbol from the algebraic perspective.
Definition 11. Let $G = (\mathbb{Z}/p\mathbb{Z})^{\times}$. The unique character of order 2 in $\hat{G}$ is called the *Legendre character*, denoted as λ_p.

Uniqueness of the Legendre character is established with the following from abstract algebra

Theorem 6. Let G be a cyclic group of order m. Then there is a one-to-one correspondence between the subgroups of G and the divisors of m.

Since $(\mathbb{Z}/p\mathbb{Z})^{\times}$ has order $p-1$, it has a subgroup of order 2, and only one of order 2.

There are several parallels between Legendre characters and Legendre symbols. They are in fact identical as we will soon see. Here we present Euler's Criterion for Legendre characters:

Theorem 7. Let p be and odd prime. Let $a \in \mathbb{Z}$ such that p does not divide a, then

$$\lambda_p(a) \equiv a^{(p-1)/2} \pmod{p}.$$

We can now draw the rigorous connection between the Legendre symbol and the Legendre character, which will allow us to proceed to the Gauss reciprocity law.

Theorem 8. Euler's Criterion Let p be an odd prime. Let $a \in \mathbb{Z}$ such that p does not divide a. Then for a primitive root modulo p, r,

$$\lambda_p(a) = (-1)^{\mathrm{ind}_r a}$$

from which must follow $\lambda_p(a) = 1$ iff there exists an $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{p}$.

Proof. Observing the map $a \to (-1)^{\mathrm{ind}_r a}$, we can see that it is a homomorphism between G and $\mathbb{C}^{\times}$. Thus it is a character by definition. Since $\mathrm{ind_r(r)} = 1$, it follows that a maps to -1, and thus the map is of order 2. Since it was established that any character of order 2 is unique, $\lambda_p(a) = (-1)^{\mathrm{ind}_r a}$. The second part of the theorem follows from the definition of $\mathrm{ind}_r a$.□

Thus the Legendre symbol $\left(\frac{a}{p}\right)$ must be identical to $\lambda_p(a)$, which of course affords us the presentation of the Gauss reciprocity law

Theorem 9. Gauss Reciprocity Law For odd primes p, q,

$$\lambda_p(q)\lambda_q(p) = (-1)^{\frac{1}{4}(p-1)(q-1)}$$

Lemma 1.
$$\lambda_p(-1) = (-1)^{(p-1)/2}.$$

Proof. From Theorem 7, let $a = 1$. Then $\lambda_p(-1) \equiv (-1)^{(p-1)/2} \pmod{p}$. But both sides of this equation are ±1 and p is an odd prime, equality must follow.□

Definition 12. Let p be an odd prime and let $z = e^{2\pi i/p}$. For $a \in \mathbb{Z}$, let τ_a denote

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}^\times} \lambda_p(x) z^{ax},$$

called the *Gauss sum*. τ denotes τ_1.

We shall extend λ_p to $\mathbb{Z}/p\mathbb{Z}$ by setting $\lambda_p(0) = 0$.

Lemma 2. For $a \in \mathbb{Z}$, $\tau_a = \lambda_p(a)\tau$.

Lemma 3. Let $\hat{p}$ denote $(-1)^{(p-1)/2}p$. Then $\lambda_q(\hat{p}) = (-1)^{(q-1)(p-1)/4}\lambda_q(p)$.

Proof. Using Lemma 1, we can see that

$$\begin{aligned} \lambda_q(\hat{p}) &= \lambda_q((-1)^{(p-1)/2}p) \\ &= (\lambda_q(-1))^{(p-1)/2}\lambda_q(p) \\ &= (-1)^{(q-1)(p-1)/4}\lambda_q(p) \end{aligned}$$

□

Lemma 4. For odd prime p that does not divide a, then $\tau_a^2 = \hat{p}$

With the preceding lemmas, we are able to prove the Gauss Reciprocity Law. [2]

Proof of Theorem 9. From Lemma 4 and Euler's Criterion, we see that

$$\begin{aligned} \tau^{q-1} &= (\tau^2)^{q-1}/2 \\ &= \hat{p}^{(q-1)/2} \\ &\equiv \lambda_q\hat{p} \pmod{q} \end{aligned}$$

Thus

$$\tau_q \equiv \lambda_q(\hat{p})\tau \pmod{q}$$

Utilizing Freshman's Dream, we can deduce the following

$$\begin{aligned}
\tau^q &= \left(\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \lambda_p(x) z^x \right)^q \\
&\equiv \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \lambda_p(x)^q z^{xq} \pmod q \\
&= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \lambda_p(x) z^{xq}
\end{aligned}$$

which is $\tau_q \pmod q$. By Lemma 2, this is equal to $\lambda_p(q)\tau$. From the above steps, this again is equal to $\lambda_q(\hat{p})\tau \pmod q$ Thus, multiplying the last equality by τ, we obtain

$$\lambda_p(q)\hat{p} \equiv \lambda_q(\hat{p}) \pmod q$$

which leads us to

$$\lambda_p(q) = \lambda_q(\hat{p})$$

which results in the Gauss reciprocity law by Lemma 3.□

Conclusion

In summary, using the tools gained via abstract algebra, we are able to take on a different field of mathematics, extending what the reader might already be familiar with known as elementary number theory. We created an abstract algebra analogue to a familiar theorem, and shed more light on its properties.

Bibliography

1. Mollin, Richard: Algebraic Number Theory. Chapman and Hall/CRC Press. 1999

2. Ono, Takashi: An Introduction to Algebraic Number Theory. Plenum Publishing Corporation. 1990

3. Hardy and Wright: An Introduction to the Theory of Numbers. Oxford Science Publications. 1938

4. Burton, David: Elementary Number Theory. Allyn and Bacon Inc. 1980

License