14 Number Fields

14.1 The Gaussian Integers

Last time, we discussed factorization in the Gaussian integers $\mathbb{Z}[i]$, and how it relates to the sum of squares problem. At the end of the lecture, we classified all Gaussian primes. Note that since $\mathbb{Z}[i]$ is a UFD, the primes in $\mathbb{Z}[i]$ are precisely the irreducible elements. In general, primes are defined as elements such that if $p \mid ab$, then $p \mid a$ or $p \mid b$ — but in a UFD, an element is prime if and only if it's irreducible.

Theorem 14.1
The complete list of all primes in $\mathbb{Z}[i]$, up to association, consists of:

- for each integer prime $p = 4k + 3 \in \mathbb{Z}$, the Gaussian prime p itself;
- for each integer prime $p = 4k + 1 \in \mathbb{Z}$, the two Gaussian primes $a \pm bi$ where $a^2 + b^2 = p$;
- the prime $1 + i$.

Note that we have $2 = (1 + i)(1 - i)$, but $1 + i$ and $1 - i$ are associate, so 2 only contributes *one* prime up to association.

Proof. First we'll check that all such elements are primes. For the second and third cases, where p factors as $a^2 + b^2$ for some integers a and b, it's enough to prove the following claim:

Claim. *If $a^2 + b^2 = p$ is an integer prime, then $a + bi$ is prime in $\mathbb{Z}[i]$.*

Proof. Define the norm $\mathrm{N}(a + bi) = a^2 + b^2$, which is multiplicative. Suppose $a + bi$ factors as $\alpha\beta$. Then we have

$$p = \mathrm{N}(a + bi) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta).$$

Then since p is an integer prime, $\mathrm{N}(\alpha)$ or $\mathrm{N}(\beta)$ must be 1. But if $\mathrm{N}(\alpha) = 1$, then $\alpha\overline{\alpha} = 1$, so α is a unit. This means in any factorization of $a + bi$, one factor must be a unit, so $a + bi$ is irreducible and therefore prime. □

Meanwhile, for the first case, we saw last class that every integer prime $p = 4k + 3$ is still prime in $\mathbb{Z}[i]$.

Now we will check that there are no other primes — it's enough to check that every non-unit $\alpha \in \mathbb{Z}[i]$ is divisible by some element of this list. To do so, we again use the norm — if α is not a unit, then we have $\alpha\overline{\alpha} = n$ for some integer $n > 1$. Let p be a prime divisor of n.

Then if $p \equiv 3 \pmod 4$, we must have $p \mid \alpha$ (or $p \mid \overline{\alpha}$, which also implies $p \mid \alpha$), since p is prime. Otherwise, we can write $p = (a + bi)(a - bi)$ where $a \pm bi$ are both primes. Then $a + bi$ must divide α or $\overline{\alpha}$, and therefore $a + bi$ or $a - bi$ must divide α. □

Student Question. *Does this still work when $p = 2$?*

Answer. *Yes, the argument still works as written — in fact, we don't even need the last step, since if $1 + i$ divides $\overline{\alpha}$, then $1 + i$* itself *also divides α.*

As a corollary, we can find the complete answer to the sum of squares question.

Corollary 14.2
If n has prime factorization $n = p_1^{d_1} \cdots p_r^{d_r}$ in $\mathbb{Z}$, then n is a sum of squares if and only if the exponent d_i is even for all primes $p_i \equiv 3 \pmod 4$.

For example, 21 has odd exponents of 3 and 7, so it cannot be written as a sum of squares.

Proof. First, to show that all n of this form work, we've seen earlier that if m and n are sums of squares, then so is mn. For all $p \not\equiv 3 \pmod 4$, we've seen that p is a sum of squares; and for all $p \equiv 3 \pmod 4$, we have that p^2 is trivially a sum of squares. Since n is the product of such terms, it must be a sum of squares as well.

Conversely, suppose n can be written as a sum of squares, so $n = (a + bi)(a - bi)$. Let d be the power of a given prime $p \equiv 3 \pmod 4$ in the prime factorization of $a + bi$ in the Gaussian integers. Since $p \in \mathbb{Z}$, then d is also

the power of p in the prime factorization of $a - bi$, so the power of p in the factorization of n is $2d$. Therefore, the power of each prime $p \equiv 3 \pmod 4$ in the prime factorization of n must be even. □

Student Question. *Why doesn't this statement have a condition involving $p = 2$?*

Answer. *This is because 2 is a sum of squares, as $2 = 1 + 1$. So 2 is allowed to have either odd or even power in the prime factorization of n.*

This is just one example of how such considerations can be applied to number theory. It is possible to go even further — for example, it is possible to determine how many different presentations as a sum of squares there are for a given n.

14.2 Fermat's Last Theorem, as an Aside

The ideas used to analyze solutions to $n = a^2 + b^2$ have some relevance to a more difficult equation as well, Fermat's Last Theorem.

Theorem 14.3 (Fermat)
For an integer $n > 2$, the equation

$$a^n + b^n = c^n$$

has no solutions where a, b, and c are all nonzero integers.

Mathematicians have been trying to prove this theorem for a long time. Fermat famously proposed the theorem in the margin of a book, stating, "I have a truly marvelous demonstration of this proposition that this margin is too narrow to contain." He most likely did not have a truly marvelous demonstration of the proposition.

Mathematician Gabriel Lamé announced a proof on March 1 of 1847. This proof was later found to be incorrect, then partially corrected to be valid in certain cases by Ernst Kummer.

The initial steps of Lamé's proof proceed in a similar fashion as our analysis for Gaussian integers. Assume n is odd (in fact, we can assume that n is prime — it suffices to prove the theorem for $n = 4$ and n prime, and Fermat did have a proof for the case $n = 4$). When considering sums of squares, we used the factorization $a^2 + b^2 = (a + bi)(a - bi)$. In general, when n is odd we have a similar factorization

$$a^n + b^n = (a + b)(a + \zeta b)(a + \zeta^2 b) \cdots (a + \zeta^{n-1} b),$$

where $\zeta = e^{2\pi i/n}$. This gives a factorization of $a^n + b^n$ in the ring $\mathbb{Z}[\zeta]$, the ring of *cyclotomic integers*.

In many cases, it is possible to check that the factors are pairwise coprime; that is, that they do not have a common divisor. In the usual integers, if an nth power is factored as a product of coprime factors, then every factor must be also an nth power (up to multiplication by ± 1). In this case, we similarly want to conclude that each factor is an nth power (up to multiplication by units). This would eventually lead to a contradiction.

The key point is that if $\mathbb{Z}[\zeta]$ were a UFD, then we could obtain our conclusion. This is what Lamé didn't show — we're so used to dealing with the integers, where unique factorization *does* hold, that even a major mathematician initially missed that unique factorization doesn't have to hold in this setting (though it was realized later). Unfortunately, this method doesn't work — when n is an odd prime, $\mathbb{Z}[\zeta]$ is *almost never* a UFD.

However, Kummer showed that under a weaker condition than $\mathbb{Z}[\zeta]$ being a UFD, it's still possible to obtain this conclusion. This weaker condition is that p is a *regular* prime — not every prime is regular, but many are. In order to explain what a regular prime is, we need more theory, which we'll see in future classes. As a glimpse into what this theory will be, when unique factorization fails, we can still analyze *how much* it fails. This leads to the definition of the *ideal class group*, which in some sense controls the non-uniqueness of prime factorization; then the regularity of a prime is a property of the ideal class group of $\mathbb{Z}[\zeta]$.

14.3 Number Fields

Now we will move on to a more general case.

Guiding Question
How does factorization work in rings like $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta]$?

Both rings sit inside a larger field: $\mathbb{Z}[i] \subset \mathbb{Q}[i]$ and $\mathbb{Z}[\zeta] \subset \mathbb{Q}[\zeta]$. This is helpful because fields can be easier to work with than rings. The concept of a *number field* generalizes this.

Definition 14.4
A **number field** is a subfield in $\mathbb{C}$ that is finite-dimensional as a vector space over $\mathbb{Q}$.

Example 14.5
The number field $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ is two-dimensional over $\mathbb{Q}$.

14.3.1 Algebraic Numbers and Integers

An important observation is that every element in a number field is algebraic.

Definition 14.6
A number is an **algebraic number** if it is a root of a polynomial with rational coefficients.

If F is a number field, and $\alpha \in F$, then there is a linear dependence between 1, α, α^2, $\ldots$, α^n for any $n \geq \dim_{\mathbb{Q}}(F)$. So α is a root of some polynomial $P \in \mathbb{Q}[x]$, and therefore α is algebraic. Conversely, $\mathbb{Q}[\alpha]$ is a number field if α is algebraic — if α is the root of a polynomial of degree d, then we can express powers α^i with $i \geq d$ in terms of lower powers, so the only possible terms we have are 1, α, $\ldots$, α^{d-1}. This argument generalizes to show that $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ is also a number field if $\alpha_1, \ldots, \alpha_n$ are all algebraic, since there are only finitely many terms $\alpha_1^{e_1} \cdots \alpha_n^{e_n}$ which we need to consider (if a term contains a high power of some α_i, we can rewrite it in terms of lower powers).

If α is algebraic, then $\{P \mid P(\alpha) = 0\}$ is an ideal in $\mathbb{Q}[x]$. Since $\mathbb{Q}[x]$ is a PID, it has the form (P), where P is a monic polynomial of minimal degree. Such a P is called the **minimal polynomial** for α over $\mathbb{Q}$.

A number field is a generalization of fields like $\mathbb{Q}[i]$ or $\mathbb{Q}[\zeta]$, but we really want to analyze factorization in *rings* like $\mathbb{Z}[i]$ or $\mathbb{Z}[\zeta]$, not the underlying fields. To describe the generalization of such rings to an arbitrary number field, we need to define an *algebraic integer*.

Definition 14.7
An algebraic number is an **algebraic integer** if its minimal polynomial has integer coefficients.

Lemma 14.8
The element α is an algebraic integer if and only if $P(\alpha) = 0$ for *some* monic polynomial $P \in \mathbb{Z}[x]$.

It is evident that a polynomial with rational coefficients can be scaled to either be monic or have integer coefficients, but an algebraic integer requires that both can be achieved simultaneously.

Proof. The proof is another application of Gauss's Lemma and the ideas from last lecture. One direction is obvious: if the minimal polynomial P is in $\mathbb{Z}[x]$, then $P(\alpha) = 0$, so the condition is clearly satisfied.

For the other direction, suppose there exists a monic polynomial $P \in \mathbb{Z}[x]$ such that $P(\alpha) = 0$. Now consider the minimal polynomial $P_{\min}$. By clearing denominators and pulling out the gcd of its coefficients, rescale it to a polynomial $Q = aP_{\min}/b$ which is primitive and in $\mathbb{Z}[x]$.

Then Q divides P in $\mathbb{Q}[x]$, since $P_{\min}$ divides P. But Q is primitive, so by the results in the last lecture, Q must also divide P in $\mathbb{Z}[x]$. But then the leading coefficient of Q must divide the leading coefficient of P. Since P is monic, $\pm Q$ must be monic as well. Then since $P_{\min}$ is also monic, we have $Q = \pm P_{\min}$, so $P_{\min}$ has integer coefficients. □

Example 14.9
A rational number $\alpha \in \mathbb{Q}$ has minimal polynomial $x - \alpha$, so α is be an algebraic integer if and only if α is a usual integer.

The next example is the primary setting that we will work with.

Example 14.10 (Quadratic Number Fields)
What are the algebraic integers in the number field $\mathbb{Q}[\sqrt{d}]$? (Here d may or may not be positive.)

Proof. Without loss of generality, we can assume d is squarefree (since factoring squares out of d doesn't change the number field). Then let $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. The minimal polynomial of α is

$$(x - a - b\sqrt{d})(x - a + b\sqrt{d}) = x^2 - 2a + (a - b^2 d),$$

so α is an algebraic integer if and only if $2a \in \mathbb{Z}$ and $a^2 - b^2 d \in \mathbb{Z}$.

Now we have two cases:

Case 1 ($a \in \mathbb{Z}$). Then we must have $b^2 d \in \mathbb{Z}$ as well, and since d is squarefree, $b \in \mathbb{Z}$ as well.

Case 2 ($a = k + \frac{1}{2}$ for $k \in \mathbb{Z}$). Then we must have $2b \in \mathbb{Z}$ as well, and $b = m + \frac{1}{2}$. In this case, we have

$$a^2 - b^2 d = \frac{1}{4}((2k+1)^2 - (2m+1)^2 d).$$

This is an integer if and only if $d \equiv 1 \pmod 4$.

So the conclusion is that if $d \not\equiv 1 \pmod 4$, the algebraic integers are precisely $a + b\sqrt{d}$ for $a, b \in \mathbb{Z}$ — for example, the algebraic integers in $\mathbb{Q}[i]$ and $\mathbb{Q}[\sqrt{-5}]$ are $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-5}]$. Meanwhile, if $d \equiv 1 \pmod 4$, the algebraic integers are precisely $a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$ or $a + \frac{1}{2}, b + \frac{1}{2} \in \mathbb{Z}$ — for example, the algebraic integers in $\mathbb{Q}[\sqrt{-3}]$ are $\mathbb{Z}[\omega]$ for a primitive third root of unity ω, which are exactly the elements of this form. □

In general, the algebraic integers of a number field have quite a bit of additional structure.

Theorem 14.11
For a number field F, the set of algebraic integers in F is a subring of F. Furthermore, this is the largest subring that is finitely generated as an abelian group under addition.

We won't prove this in general; but it's fairly straightforward in our specific example $F = \mathbb{Q}[\sqrt{d}]$.

Next time, we will study factorization in rings of algebraic integers. The general idea is that if a statement fails to be true, mathematicians often try to generalize it to find a version that *is* true. In this case, where unique factorization fails for a general ring of algebraic integers, we can consider a more general version of it which works.

To motivate what this more general version will be, note that in the cases where unique factorization works, primes are considered up to association. In fact, an element in a ring $\alpha \in R$ up to association is equivalent to the ideal (α). So in the more general case, we actually consider products of *ideals* rather than *elements*. We will show that in a ring of algebraic integers, there is unique factorization, not into prime elements, but into prime ideals.

Resource: Algebra II Student Notes

Spring 2022

Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng