LECTURE APRIL 3: A CRASH COURSE IN ALGEBRAIC NUMBER THEORY

Algebraic number theory is the fusion of abstract algebra with number theory. It is largely about the structure of finite extensions of $\mathbf{Q}$.

1. The Gaussian integers

Let $\mathbf{Z}[i] = \{a + bi | a, b \in \mathbf{Z}\}$. This is a subring of $\mathbf{Q}(i)$, and thus it is an integral domain.

For an $\alpha = a + bi \in \mathbf{Z}[i]$, I let $N(\alpha) = a^2 + b^2 = \alpha\bar{\alpha}$. Then $N(\alpha)$ is the squared length of α, considered as a vector. This is called the norm of α.

Theorem 1.1 (Division algorithm)**.** *Given $\alpha, \beta \in \mathbf{Z}[i]$ with $\beta \neq 0$, then there exist $q, r \in \mathbf{Z}[i]$ such that*

$$\alpha = q\beta + r,$$

where $N(r) < N(\beta)$.

Proof. Consider where α/β lies in the complex plane. The nearest Gaussian integer, call it q, is no more than distance 1 away: $N(\alpha/\beta - q) < 1$, or $N(\alpha - q\beta) < N(\beta)$. Let $r = \alpha - q\beta$, you get the result. □

The units in $\mathbf{Z}[i]$ are $1, -1, i, -i$. A nonunit, nonzero element in $\mathbf{Z}[i]$ is *irreducible* if it can't be factored into a product of nonunits.

The same strategy we used to prove that $\mathbf{Z}$ has unique factorization into primes, can be applied to $\mathbf{Z}[i]$. (Recall that in $\mathbf{Z}$, everything flowed from the division algorithm.)

Theorem 1.2. *Every nonunit in $\mathbf{Z}[i]$ can be factored uniquely into irreducibles, up to units.*

In particular, irreducibles are prime: if π is irreducible and it divides a product $\alpha\beta$, then it must divide α or β.

The (rational) primes in $\mathbf{Z}$ sometimes factor in $\mathbf{Z}[i]$:

$$\begin{aligned} 2 &= (1+i)(1-i) \\ 3 &= 3 \\ 5 &= (1+2i)(1-2i) \\ 7 &= 7 \\ 11 &= 11 \\ 13 &= (2+3i)(2-3i) \end{aligned}$$

The factors appearing on the right side are all irreducible.

There is a simple pattern governing this behavior.

Theorem 1.3. *Let p be an odd (rational) prime. Then p remains prime in $\mathbf{Z}[i]$ if $p \equiv 3 \pmod 4$. Otherwise, $p = \pi\overline{\pi}$, where π is a prime in $\mathbf{Z}[i]$.*

Proof. Suppose $p \equiv 1 \pmod 4$. Then $(p-1)/2$ is an even number. Therefore $(-1)^{(p-1)/2} = 1$. From your HW: if a is not divisible by p, then $a^{(p-1)/2} \equiv 1 \pmod p$ if a is a square modulo p, and is -1 otherwise. Therefore -1 is a square modulo p: there exists n with $n^2 + 1 \equiv 0 \pmod p$.

Thus p divides $n^2 + 1$. In $\mathbf{Z}[i]$, we have that p divides $(n+i)(n-i)$. If p were still prime in $\mathbf{Z}[i]$, then it would divide $n + i$ or $n - i$, but this is impossible. Therefore p is not prime in $\mathbf{Z}[i]$, it factors $p = \alpha\beta$. Take norms and get $N(p) = p^2 = N(\alpha)N(\beta)$, so $N(\alpha) = p$. Let $\pi = \alpha$, and then $p = N(\pi) = \pi\overline{\pi}$. □

As a corollary, we get that if $p \equiv 1 \pmod 4$, then $p = a^2 + b^2$ is a sum of two perfect squares (Fermat).

2. The Legendre symbol

Given an odd prime p, and an integer a not divisible by p, we set

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square modulo } p \\ -1 & \text{if not.} \end{cases}$$

Euler's criterion is:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Some rules about this:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

3. Some other quadratic rings

Consider $R = \mathbf{Z}[\sqrt{-3}] = \left\{a + b\sqrt{-3} | a, b \in \mathbf{Z}\right\}$. This is a subring of $\mathbf{Q}(\sqrt{-3})$. Division algorithm fails in R, as does unique factorization:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

expresses 4 as a product of irreducibles in two different ways.

I can enlarge R a little bit:

$$\mathbf{Z}[\omega] = \{a + b\omega | a, b \in \mathbf{Z}\}$$

where

$$\omega = \frac{-1 + \sqrt{-3}}{2}$$

Then $R \subset \mathbf{Z}[\omega]$. Then unique factorization holds in $\mathbf{Z}[\omega]$!

The relevant theorem about this is:

Theorem 3.1. *Let p be a prime other than 3. If $p \equiv 1 \pmod 3$, then $p = \pi\overline{\pi}$ for a prime π in $\mathbf{Z}[\omega]$. If $p \equiv 2 \pmod 3$, then p is still prime.*

$\mathbf{Z}[\omega]$ is called the ring of Eisenstein integers.

How did I know to consider $\mathbf{Z}[\omega]$?

Definition 3.2. *Let R be a subring of a ring S. Let $\alpha \in S$. We say that α is* integral *over R if it is the root of a monic polynomial $f(x) \in R[x]$.*

Therefore $\omega \in \mathbf{C}$ is integral over $\mathbf{Z}$, since it is a root of $x^2 + x + 1$.

Definition 3.3. *A finite extension of $\mathbf{Q}$ is called an* algebraic number field. *Given an algebraic number field K, the set of elements which are integral over $\mathbf{Z}$ is called $\mathcal{O}_K$, the ring of algebraic integers in K.*

(It is not completely obvious that $\mathcal{O}_K$ is a ring.) For instance, if $K = \mathbf{Q}(\sqrt{-3})$, then $\mathcal{O}_K = \mathbf{Z}[\omega]$.

If $K = \mathbf{Q}(\sqrt{-5})$, then $\mathcal{O}_K = \mathbf{Z}[\sqrt{-5}]$. If $K = \mathbf{Q}(\sqrt{5})$, then

$$\mathcal{O}_K = \mathbf{Z}[\phi],$$

where

$$\phi = \frac{-1 + \sqrt{5}}{2}.$$

We can investigate whether these rings have the unique factorization property. In fact $\mathbf{Z}[\phi]$ has this property. But $\mathbf{Z}[\sqrt{-5}]$ does not have it:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Big question: which rings of quadratic integers have the unique factorization property?

Gauss conjectured: among the imaginary ones, there are only nine of them! The "last" one is

$$\mathbf{Z}\left[\frac{-1 + \sqrt{-163}}{2}\right].$$

This was proved by Baker, Stark, Heegner (1967).

Gauss recognized that the real quadratic rings were more likely to have unique factorization. It is conjectured, but not known, whether there are infinitely many number fields K for which $\mathcal{O}_K$ has unique factorization.

4. Some generalities on rings of integers in number fields

Let $K/\mathbf{Q}$ be a finite extension. Then K is called an algebraic number field.

Let $\mathcal{O}_K$ be the set of elements of K which are roots of monic polynomials with integer coefficients. Then $\mathcal{O}_K$ is called the ring of integers of K.

For example, if $K = \mathbf{Q}(i)$, then $\mathcal{O}_K = \mathbf{Z}[i]$.

Theorem 4.1. *$\mathcal{O}_K$ is a free abelian group of rank n, where $n = [K : \mathbf{Q}]$.*

This means that the underlying abelian group of $\mathcal{O}_K$ under addition is isomorphic to $\mathbf{Z}^n$.

In fact, it's know that if $I \subset \mathcal{O}_K$ is a nonzero ideal, then I is also a free abelian group of rank n. Thus if I is nonzero then $\mathcal{O}_K/I$ is a finite ring.

Theorem 4.2. *Let P be a nonzero prime ideal of $\mathcal{O}_K$. Then P is maximal.*

Proof. If P is a nonzero prime ideal, then $\mathcal{O}_K/P$ is a finite integral domain. But then $\mathcal{O}_K/P$ is also a field, and so P is maximal. □

Recall that it is not always the case that $\mathcal{O}_K$ has unique factorization. For instance, in $\mathbf{Z}[\sqrt{-5}]$ we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Theorem 4.3. *Every nonzero ideal I in $\mathcal{O}_K$ admits a unique factorization into prime ideals in $\mathcal{O}_K$.*

If $\alpha, \beta \in \mathcal{O}_K$, I let (α, β) be the ideal generated by those elements. For instance, if $K = \mathbf{Q}$, then $\mathcal{O}_K = \mathbf{Z}$, and then

$$(8, 12) = (4)$$

with 4 as the gcd of 8 and 12. But in general, not every ideal is principal. Thus in $\mathbf{Z}[\sqrt{-5}]$, the ideal

$$P_2 = (2, 1 + \sqrt{-5})$$

is not principal. You cannot solve the equation

$$2x + (1 + \sqrt{-5})y = 1$$

for $x, y \in \mathcal{O}_K$. In fact we have in $\mathcal{O}_K$:

$$(2) = P_2^2 = (2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5}).$$

The right hand side is

$$\begin{aligned}(2,1+\sqrt{-5})(2,1+\sqrt{-5}) &= (4,2(1+\sqrt{-5}),-4+2\sqrt{-5})\\ &= (2)(2,1+\sqrt{-5},-2+\sqrt{-5})\\ &= (2)(2,1+\sqrt{-5},\sqrt{-5})\\ &= (2)(2,1,\sqrt{-5})\\ &= (2).\end{aligned}$$

Let

$$\begin{aligned}P_3 &= (3,1+\sqrt{-5})\\ \overline{P}_3 &= (3,1-\sqrt{-5})\end{aligned}$$

Then

$$(3) = P_3\overline{P}_3.$$

How does the ideal 6 factor?

$$(6) = (2)(3) = P_2^2 P_3\overline{P}_3.$$

Note that $(1+\sqrt{-5}) = P_2P_3$ and $(1-\sqrt{-5}) = P_2\overline{P}_3$ (check this!). Thus unique factorization is "saved" by introducing prime ideals.

Kummer invented the notion of "ideal number" in this context, the right setting for unique factorization.

In some cases, such as $K = \mathbf{Q}(\sqrt{5})$, the ring of integers $\mathcal{O}_K$ is a principal ideal domain, meaning that every ideal is principal. In such rings, elements have the property of unique factorization into irreducibles.

Given two nonzero ideals I and J in $\mathcal{O}_K$, we say that I and J are *equivalent* if there exists an $\alpha, \beta \in \mathcal{O}_K$ such that $(\beta)I = (\alpha)J$. For instance

$$(3)(2,1+\sqrt{-5}) = (1-\sqrt{-5})(1+\sqrt{-5},3)$$

Multiplying this out gives

$$(6,3(1+\sqrt{-5})) = (6,3(1-\sqrt{-5})).$$

Therefore P_2 and P_3 are equivalent ideals.

The principal ideals are just the ones which are equivalent to the unit ideal.

Theorem 4.4. *The set of equivalence classes of nonzero ideals of $\mathcal{O}_K$ is a finite set. It forms a finite group under mutliplication.*

The group of nonzero ideals modulo equivalence is called the *class group* H_K of K. It is a finite abelian group. If $H_K = \{e\}$, it means that $\mathcal{O}_K$ is a principal ideal domain.

- If $K = \mathbf{Q}(\sqrt{5})$, then $H_K = \{e\}$.
- If $K = \mathbf{Q}(\sqrt{-5})$, then $H_K \cong \mathbf{Z}_2$.
- $K = \mathbf{Q}(\sqrt{-23})$ then $H_K \cong \mathbf{Z}_3$.

Theorem 4.5. *(Kummer, 1850) Let p be an odd prime. Let $K = \mathbf{Q}(\zeta_p)$. Consider the group H_K. Assume that p does not divide the order of H_K. Then $x^p + y^p = z^p$ has no solutions in nonzero integers x, y, z.*

If p does not divide the order of H_K, we call p a *regular prime*. Otherwise, it's *irregular*. The first irregular prime is 37.

Kummer also found an easy way to check whether a number is regular, using Bernoulli numbers.

5. Cyclotomic rings

If $m \geqslant 3$, we have the field $\mathbf{Q}(\zeta_m)$, where $\zeta_m = e^{2\pi i/m}$.

Theorem 5.1. *The ring of integers in $\mathbf{Q}(\zeta_m)$ is just $\mathbf{Z}[\zeta_m]$.*

Let's focus on the case that $m = p$ is an odd prime. Then $\mathbf{Z}[\zeta_p]$ consists of elements, which can be written as linear combinations

$$a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1},$$

with $a_1, \ldots, a_{p-1} \in \mathbf{Z}$. We have $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong \mathbf{Z}_p^\times$. Recall that if $a \in \mathbf{Z}_p^\times$, we have an automorphism σ_a, which has the effect:

$$\sigma_a(\zeta_p) = \zeta_p^a.$$

Thus the Galois group acts on $\mathbf{Z}[\zeta_p]$.

There is a unique subgroup $H \subset \mathbf{Z}_p^\times$ of index 2, namely the *squares*. We have $\#H = (p-1)/2$. If I let $K = \mathbf{Q}(\zeta_p)^H$, then $[K : \mathbf{Q}]$ is degree 2.

Theorem 5.2. *(Gauss)* $K = \mathbf{Q}(\sqrt{p^*})$*, where* $p^* = p$ *if* $p \equiv 1 \pmod 4$*, and* $p^* = -p$ *if* $p \equiv -1 \pmod 4$*.*

In other words,

$$p^* = (-1)^{(p-1)/2}p.$$

In fact, Gauss proved the following:

$$\sqrt{p^*} = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a.$$

Let q be an odd prime distinct from p.

Theorem 5.3. *Let* $\alpha \in \mathbf{Z}[\zeta_p]$*. Then*

$$\sigma_q(\alpha) \equiv \alpha^q \pmod q$$

Proof. The idea is that modulo q, raising to the power of q distributes over addition.

Given an element

$$\alpha = a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1},$$

we have

$$\begin{aligned}
\alpha^q &= (a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1})^q \\
&\equiv a_1^q\zeta_p^q + a_2^q\zeta_p^{2q} + \cdots + a_{p-1}^q\zeta_p^{(p-1)q} \pmod q \\
&\equiv a_1\zeta_p^q + a_2\zeta_p^{2q} + \cdots + a_{p-1}\zeta_p^{(p-1)q} \pmod q \\
&\equiv a_1\sigma_q(\zeta_p) + a_2\sigma_q(\zeta_p)^2 + \cdots + a_{p-1}\sigma_q(\zeta_p)^{p-1} \pmod q \\
&\equiv \sigma_q(a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1}) \\
&\equiv \sigma_q(\alpha) \pmod q
\end{aligned}$$

□

In particular,

$$\sigma_q(\sqrt{p^*}) \equiv (\sqrt{p^*})^q \equiv \sqrt{p^*}\sqrt{p^*}^{q-1} \equiv \sqrt{p^*}(p^*)^{(q-1)/2} \pmod q$$

By Euler's criterion:

$$\sigma_q(\sqrt{p^*}) \equiv \left(\frac{p^*}{q}\right)\sqrt{p^*} \pmod q$$

Now let's figure out what $\sigma_q(\sqrt{p^*})$ is, using Galois theory. Since σ_q must take $\sqrt{p^*}$ to a conjugate, we must have $\sigma_q(\sqrt{p^*}) = \pm\sqrt{p^*}$.

We have $\sigma_q(\sqrt{p^*}) = \sqrt{p^*}$ if and only if σ_q lies in the subgroup H of $\mathbf{Z}_p^\times$ consisting of the squares modulo q. Thus this happens if any only if q is a square modulo p. Otherwise, we get the minus sign appearing. Thus:

$$\sigma_q(\sqrt{p^*}) = \left(\frac{q}{p}\right)\sqrt{p^*}.$$

We can equate the two signs appearing here:

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

(This takes a small amount of justification: you need to know that $2\sqrt{p^*}$ is invertible modulo q. This is true because $2p$ is invertible mod q, as $2p$ and q are relatively prime.) Let's remember that

$$p^* = (-1)^{(p-1)/2}p.$$

We get

$$\left(\frac{q}{p}\right) = \left(\frac{(-1)^{(p-1)/2}p}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2}\left(\frac{p}{q}\right)$$

Now recall that

$$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}.$$

We get

$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{p}{q}\right).$$

This is called the Law of Quadratic Reciprocity. It says that $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ happens exactly when at least one of p or q is 1 modulo 4, and otherwise $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

6. Diophantine equations

Challenge: find all solutions to

$$y^2 = x^3 - 2$$

in integers x and y. An equation where you are looking for only integer solutions is called *Diophantine*.

An example is

$$5x + 7y = 1.$$

That's a linear equation – easily solved using the Euclidean algorithm. Second-degree equations are more subtle, but mathematicians have methods of solving them. Third-degree equations like $y^2 = x^3 - 2$ require special techniques, often tailored to the situation at hand.

Let's return to $y^2 = x^3 - 2$. We can observe that if x is even, then so is y, and so y^2 is divisible by 4. But then x^3 is divisible by 4 as well, and so $x^3 - 2$ is not divisible by 4, contradiction. So any integer solution to $y^2 = x^3 - 2$ must have x and y odd.

Rewrite the first equation as

$$x^3 = y^2 + 2 = (y - \sqrt{-2})(y + \sqrt{-2}).$$

We are now working in the ring of integers $\mathbf{Z}[\sqrt{-2}]$ in $\mathbf{Q}(\sqrt{-2})$. Facts about this ring:

- The units in this ring are just ± 1.
- The division algorithm holds in this ring.
- Therefore, so does unique factorization.
- If α and β share no nonunit common factor, and $\alpha\beta$ is a perfect cube, then both α and β are perfect cubes.

Proving these facts is a matter of repeating what we have done for $\mathbf{Z}$ and $\mathbf{Z}[i]$.

We now argue that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ share no nonunit common factor. Any such common factor would have to divide the difference $2\sqrt{-2}$. But the only irreducible factor $2\sqrt{-2}$ is $\sqrt{-2}$. This cannot divide $y + \sqrt{-2}$, as then it would have to divide the odd number y. (I invite you to rigorously work out the details.)

By the last bullet point, we must have

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3$$

for some $a, b \in \mathbf{Z}$. Expanding, we get

$$y + \sqrt{-2} = a^3 + 3a^2b\sqrt{-2} - 6ab^2 - 2b^3\sqrt{-2}.$$

Equate like terms:

$$\begin{aligned} y &= a^3 - 6ab^2 \\ 1 &= 3a^2b - 2b^3 = b(3a^2 - 2b^2) \end{aligned}$$

Therefore $b = \pm 1$. Let's first examine $b = 1$. Then $1 = 3a^2 - 2$. Thus $a = \pm 1$. Then $y = -5$ or $y = 5$. I get the solutions $(3, \pm 5)$. The case $b = -1$ leads to contradiction (check this!) and so $(3, \pm 5)$ are the only solutions to $y^2 = x^3 - 2$.

The Diophantine equation $y^2 = x^3 - k$ is called *Mordell's equation*. It is known to have only finitely many solutions for each value of k. However, deciding whether it has solutions for a given k is generally a tricky business, especially if the class group of $\mathbf{Q}(\sqrt{-k})$ has order divisible by 3.