ALGEBRA IN ALGEBRAIC GEOMETRY AND NUMBER THEORY: KRONECKER, DEDEKIND, AND WEBER

CALEB JI

1. Historical background

Leopold Kronecker (1823 - 1891) was inspired by the mathematician Ernst Kummer as a high schooler, and did his PhD in 1845 at the University of Berlin in number theory under Dirichlet. Both of these mentors married into the Mendelssohn family. For the next ten years he was a businessman, running his family's farming estate. He returned to mathematics in 1855 and held positions at the Berlin Academy and the University of Göttingen.

Kronecker was an extremely original mathematician, and held some unorthodox views in the philosophy of mathematics, such as finitism. On the other hand, he introduced many ideas which were ahead of his time, such as divisors in algebraic number theory, a general form of algebraic geometry, the Kronecker-Weber theorem, and his Jugendtraum.

Richard Dedekind (1831 - 1916) was a German mathematician who was a colleague of Riemann. Dedekind did his PhD under Gauss at Göttingen, and then studied at Berlin. He taught at what is now the ETH Zürich, then returned to his hometown where he worked as a professor for the rest of his life.

Dedekind is known for the Dedekind cut in analysis. He also worked in logic and supported Cantor, in opposition to Kronecker. His most important contributions are perhaps in algebra, where he introduced ideals and used them to study number fields. Along with Weber, he developed a brilliant algebraic approach to Rieman surfaces.

2. Algebraic background

2.1. **Ideals.** Recall that in a **ring** we have two operations, modeled after addition and multiplication, such that we always have additive inverses but not always multiplicative inverses. While there exist non-commutative rings, such as $\mathrm{GL}(2,\mathbb{C})$, we will only be concerned with commutative rings here, and not bother with the adjective. Examples of rings include $\mathbb{Z}, \mathbb{Z}[\sqrt{2},\sqrt{3}], \mathbb{Z}/8\mathbb{Z}, \mathbb{C}[x,y]$, $\mathbb{C}[x,y,z]/(y^2-x^3)$, and the ring of continuous real-valued functions on a manifold.

A **field** contains all the properties of a ring, but also has multiplicative inverses. Examples include $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \overline{\mathbb{Q}}, \mathbb{C}(x), \mathbb{Q}(x,y), \mathbb{F}_p$, and $\overline{\mathbb{F}_p}$. Often, there is a 'base field' in algebraic geometry or algebraic number theory which underlies what constants you are working with, just like in linear algebra.

A **domain** is halfway between a ring and a field: it is a ring with no zero-divisors; i.e., if $rs = 0$, then $r = 0$ or $s = 0$. All fields are domains, but $\mathbb{Z}$ is an example of a domain that is not a field.

Definition 2.1. *An additive subgroup I of a ring R is an **ideal** if $rx \in I$ for all $r \in R$ and $x \in I$.*

For example, in $\mathbb{Z}$, the ideals are given by $n\mathbb{Z}$: the set of multiples of some integer n. Note that if an ideal contains 1, rhen it must be the entire ring. In general, every element $r \in R$ gives rise to an ideal (r), consisting of all elements that can be written as a product of r and another element

Date: September 27, 2024.

of the ring. The term *ideal* is based off of Kummer's previous idea of an *ideal number*, which refers to the element that generates an ideal.

Thinking algebraically about number theory or geometry leads us to see ideals as primary objects of study. In particular, prime ideals and maximal ideals appear as new ways to think about numbers and points.

Definition 2.2. *A **prime ideal** $\mathfrak{p} \subset R$ is an ideal such that for all $a, b \in \mathbb{R}$, if $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.*

A useful mnemonic to remember for ideals is "to divide is to contain." That is, if $r|s$, then $(s) \subset (r)$ and vice versa. In the example of $R = \mathbb{Z}$, saying that (n) is a prime ideal means that if $n|ab$, then $n|a$ or $n|b$. This is one way to characterize primes. Note, however, that (0) **is** a prime ideal, even though we generally don't include 0 in the list of primes!

Definition 2.3. *A **maximal ideal** $\mathfrak{m} \subset R$ is an ideal, not equal to all of R, such that the only ideal that strictly contains it is all of R.*

For example, in $\mathbb{Z}$ the maximal ideals consist of all the prime ideals **except** for (0).

Lemma 2.4. *If $\mathfrak{m}$ is a maximal ideal, it is prime.*

Proof. Otherwise, suppose $ab \in \mathfrak{m}$ and neither a nor b is in $\mathfrak{m}$. Then the ideal $(\mathfrak{m}, a)$ must be all of R. Thus we can write $m + ar = 1$ with $m \in \mathfrak{m}, r \in R$. Multiplying by b yields $b \in \mathfrak{m}$, contradiction. □

This same method of proof can be used to characterize maximal ideals in a different way.

Lemma 2.5. *The ideal $\mathfrak{m} \subset R$ is maximal if and only if $R/\mathfrak{m}$ is a field.*

It is simpler to see the corresponding statement for prime ideals.

Lemma 2.6. *The ideal $\mathfrak{p} \subset R$ is prime if and only if $R/\mathfrak{p}$ is a domain.*

2.2. **Valuations.** The theory of valuations did not formally arise until the work of Hensel (1861 - 1941) on p-adic numbers. However, as we will see, the idea was used by Dedekind and Weber in a creative way to define points of a Riemann surface.

Definition 2.7. *A **discrete valuation ring** (dvr) is a principal ideal domain with precisely one maximal ideal.*

A principal ideal domain (PID) is a domain where every ideal can be generated by a single element. A ring with only one maximal ideal is called a *local ring*.

Example 2.8. Let p be a prime and consider the ring consisting of the fractions

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} | p \nmid b\}.$$

Then (p) (the reduced fractions with p dividing the numerator) is the only maximal ideal of $\mathbb{Z}_{(p)}$. Indeed, for any other prime q, we have that (q) contains 1, and thus is the entire ring. This shows that $\mathbb{Z}_{(p)}$ is a dvr.

In fact, we can factor every element of $r \in \mathbb{Z}_{(p)}$ as $r = p^k u$, where u is a unit (multiplicatively invertible, so no factors of p in the numerator or denominator). Then the *valuation* of r is said to be k. This explains the name *dvr*; every element of the ring has a valuation, a nonnegative integer representing how many times p divides r.

Example 2.9. Consider the ring

$$\mathbb{C}[x]_{(x-1)} \coloneqq \{\frac{p(x)}{q(x)} | (x-1) \nmid q(x)\}.$$

This is a discrete valuation ring because $(x-1)$ is the sole maximal ideal. Again, we can write every element in the form $(x-1)^k \frac{p(x)}{q(x)}$, where $k \geq 0$ and the other factor is invertible.

In both of these cases, the construction is an example of **localization**. Given a prime ideal $\mathfrak{p} \subset R$, one constructs the localization $R_{\mathfrak{p}}$ by essentially considering all fractions with denominators not in $\mathfrak{p}$. The general construction is a bit more complicated than that, but that gives the right idea in the cases we looked at. This perspective is a glimpse of the similarity between algebraic numebr theory and algebraic curves, which we will discuss more later.

3. Algebraic varieties

Kronecker began thinking about algebraic varieties in general terms, beginning part of the basic setup which is used today. Recall that we described a variety as a geometric space given by the solutions to polynomial equations. Let us be more precise.

Fix a ground field K. An important case is when $K = \mathbb{C}$. We call K^n **affine n-space**. Associated to it is its ring of polynomial functions $K[x_1, \ldots, x_n]$.

Definition 3.1. *An **affine variety** is given by the solutions to some polynomial equations in affine space. That is, given polynomials $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$, we look at the simultaneous solutions to $f_1 = \ldots = f_k = 0$ in K^n, and declare those to be the points of the variety.*

A first thing to notice is that if X is an affine variety cut out by $f_1, \ldots, f_k$, then it is also in the solution set to $f_1 + f_2$. In fact, it also satisfies any polynomial in the ideal generated by the f_i. This ideal is simply denoted $(f_1, \ldots, f_k)$.

Another thing to note is that if K is not algebraically closed, then there can be some perfectly normal polynomials which don't have roots. For example, $x^2 + 1$ does not have any roots in $\mathbb{R}[x]$. Still we would not like to declare it completely void as a variety, as when the scalars are extended to $\mathbb{C}$ it does have roots. If we declared it completely empty, as a variety would be the same as the variety defined by $x^2 + 2$. Thus instead of understanding a variety by its solution set, it is better to understand it through its ring of functions. That is, given polynomials $f_1, \ldots, f_k$, we consider the quotient ring $K[x_1, \ldots, x_n]/(f_1, \ldots, f_k)$. There still remains the question of why the same variety, thought of as a set of points, can have different rings of functions attached to it. In the future we will first see progress towards understanding this through Hilbert's Nullstellensatz; then we will see Grothendieck's scheme theory resolve all these issues in a completely satisfactory way and go much further besides.

4. Algebraic number theory

The basic objects of study in algebraic number theory are number fields and their rings of integers. The most basic example of a number field is $\mathbb{Q}$, the field of rational numbers. Its rings of integers is $\mathbb{Z}$, the integers. We wish to study variants of these fields/rings that have the same discrete feel to them, to which number theory applies.

Definition 4.1. *An algebraic number is a root of a polynomial with integer coefficients. These form a field which is denoted $\overline{\mathbb{Q}}$.*

Definition 4.2. *An algebraic integer is a root of a monic polynomial (i.e. leading coefficient 1) with integer coefficients. These form a ring which is denoted $\overline{\mathbb{Z}}$.*

The fact that $\overline{\mathbb{Z}}$ is a ring is not obvious, and is an important fact at the basis of the theory.

Definition 4.3. *A **number field** is a finite extension of $\mathbb{Q}$.*

These are natural to consider – after all, $\mathbb{Q}$ is a finite extension of $\mathbb{Q}$ of degree 1, and the finite condition ensures that we are studying something with similar behavior. Since a number field is a finite extension of $\mathbb{Q}$, any element of one must be algebraic over $\mathbb{Q}$, and thus be in $\overline{\mathbb{Q}}$. Examples of number fields include $\mathbb{Q}[\sqrt{2}], \mathbb{Q}[i], \mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Definition 4.4. *The **ring of integers** of a number field K, denoted $\mathcal{O}_K$, is the subset of algebraic integers in K.*

The ring of integers $\mathcal{O}_K$ forms a ring because they are realized as the intersection of the ring of algebraic integers and K. To do basic number theory with them, we can ask about how primes and factorization works in $\mathcal{O}_K$. For some rings of integers, we can mimic what is done for the rational integers without really changing our point of view. To explain this, let us recall how we approach the fundamental theorem of arithmetic. The main issue is showing that prime: $p|ab \Rightarrow p|a$ or $p|b$ is equivalent to irreducible: p is not divisible by any whole number between 1 and p (which is usually taken to be the definition of a prime in elementary number theory!).

- Euclidean algorithm gives you the gcd of two integers.
- Use the Euclidean algorithm to prove Bezout's lemma: if $(a, b) = 1$, then we can write $ax + by = 1$ (everything is an integer).
- Irreducibles are prime.

From this we conclude the fundamental theorem of arithmetic.

Theorem 4.5 (fundamental theorem of arithmetic)**.** *Every positive integer can be uniquely represented as a product of primes, up to re-ordering.*

We can do the same thing for the rings of integers of some number fields like $\mathbb{Q}[i]$, taking advantage of the fact that the norm allows us to construct a version of the Euclidean algorithm. Even if we don't have Euclidean function, unique factorization still holds. But there are some fields for which this doesn't work; eg. in $\mathbb{Q}[\sqrt{-5}]$ the ring of integers is $\mathbb{Z}[\sqrt{-5}]$ and we have the two factorizations $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

What works instead is prime factorization of ideals.

Theorem 4.6. *Every ideal in the ring of integers of a number field can be uniquely factorized into a product of prime ideals up to re-ordering.*

In our example above, we have $(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$. We can factorize the other elements in similar ways to get the "prime factorization"

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

In this example, we see that there are ideals in $\mathbb{Z}[\sqrt{-5}]$ that are not principal (generated by a single element). It turns out that this occurs if and only if unique factorization holds *in a ring of integers*.

Rings of integers aren't the only rings that satisfy these nice properties. In honor of Dedekind, we have the following definition.

Definition 4.7. *A **Dedekind domain** is a domain with the three properties:*
(i) Noetherian,
(ii) Integrally closed,
(iii) All non-zero prime ideals are maximal.

Another example of a Dedekind domain are the DVRs from earlier. Indeed, a DVR is essentially a local Dedekind domain. As in algebraic geometry, if you take a Dedekind domain/smooth curve and you localize at a prime ideal, you get a DVR.

An important aspect of rings of integers of number fields is the finiteness of the ideal class group. One can make the ideals into a group by multiplication if we add in fractional ideals. These are essentially ideals where we allow for denominators, e.g. all multiples of 8 divided by 3 form a fractional ideal in $\mathbb{Z}$. Principal fractional ideals are defined similarly; the example above is principal with generator $\frac{8}{3}$.

Definition 4.8. *The **ideal class group** of $\mathcal{O}_K$ is given by the quotient of the group of fractional ideals by the subgroup of principal fractional ideals.*

In some sense, the ideal class group measures how far a ring of integers is from being a PID. One of the most important theorems of classical algebraic number theory is that the ideal class group of $\mathcal{O}_K$ is finite. This is usually proven using Minkowski's geometry of numbers. Later, we will see that this ideal class group is isomorphic to the Picard group of the scheme corresponding to $\mathcal{O}_K$.

5. Riemann surfaces as function fields

In 1882, Dedekind and Weber published the remarkable *Theorie der algebraischen Fünctionen einer Veränderlichen*, which gave a purely algebraic approach to Riemann surfaces. They used *places*, another name for valuations. The prime ideals in number theory give valuations. Indeed, given a prime ideal $\mathfrak{p}$, the corresponding valuation of an ideal is just the number of times $\mathfrak{p}$ divides it.

We can do something similar in algebraic geometry. The simplest example is the case of $\mathbb{C}(x)$, the field of rational functions. Every points $z \in \mathbb{C}$ gives rise to a valuation on $\mathbb{C}(x)$, given by the number of tiems $x - z$ divides the element. This parallel is an example of the number field - function field dictionary which continues to be a major theme in algebraic geometry.

Let us return to compact Riemann surfaces for a minute. Given such an X, last time we discussed the existence of meromorphic functions on X. For $X = \mathbb{P}^1$, the meromorphic functions are just given by the rational functions $\mathbb{C}(x)$. In general, we denote the field of meromorphic functions of X by $K(X)$. The field $K(X)$ is known as the function field of X. The key fact is that a meromorphic function defines a map $X \to \mathbb{P}^1$ which realizes $K(X)$ as a finite extension of $\mathbb{C}(x)$. In other words, $K(X)$ has **transcendence degree** 1 over $\mathbb{C}$. Function fields can be defined for higher-dimensional varieties too, and their transcendence degree over the ground field is one way to define their dimension.

Example 5.1. Consider an elliptic curve over $\mathbb{C}$. If we define it algebraically as the solutions to $y^2 = x^3 + ax + b$ (with some smoothness condition and projectivity), then its function field is given by $\mathbb{C}(x, y)/(y^2 - x^3 - ax - b)$.

On the other hand, if we define the elliptic curve by a lattice as $\mathbb{C}/\Lambda$, then the function field is given in terms of the Weierstrass $\wp$-function, which as we saw last time gives x (and its derivative gives y) in the algebraic equation.

To construct a Riemann surface, Dedekind-Weber turn this upside-down by beginning with a finite extension of $K/\mathbb{C}(x)$. The crux of their approach is to define the points of the points of X as discrete valuations on K.

Let us consider how this gives the picture of a Riemann surface branched over the Riemann sphere. The valuations on $\mathbb{C}(x)$ are given by one for each complex number z and the point at ∞, which sends P to $-\deg P$. For simplicity, let's just look at the finite places for now. A valuation on K induces one on $\mathbb{C}(x)$. Thus as a point of X, it maps down to a point on $\mathbb{P}^1$. How many valuations on K give the same valuation on $\mathbb{C}(x)$? It turns out there are a finite number, less than the degree $[K(X) : \mathbb{C}(x)]$. The reason these are constrained is because a valuation must satisfy $\nu(fg) = \nu(f)\nu(g)$. The intuition is that the functions in K are algebraic over $\mathbb{C}(x)$, so for instance $\nu(x^{1/n})$ must be an nth root of $\nu(x)$.

This has an important parallel in algebraic number theory. Indeed, if we have a number field K with ring of integers $\mathcal{O}_K$, a prime ideal (p) in $\mathbb{Z}$ factors as a product of no more than $[K : \mathbb{Q}]$ prime ideals in $\mathcal{O}_K$. Indeed, the analogy goes further because taking the elements $f \in K$ such that all $\nu(f) \geq 0$ gives a Dedekind domain, the analogue of the ring of integers. In the 1870s Dedekind had developed the theory of divisibility in Dedekind domains, which he could now apply to Riemann surfaces.

The Dedekind-Weber work goes much further, and among other things proves an algebraic version of the Riemann-Roch theorem. We will return to this in a more detailed study of the Riemann-Roch theorem and its generalizations at a future date.

Annotated bibliography

The Dedekind-Weber can be read in the original German at https://eudml.org/doc/148492. An English translation with useful commentary by John Stillwell can be found at https://bookstore.ams.org/view?ProductCode=HMATH/39. There are many good sources for algebraic number theory, including James Milne's notes here: https://www.jmilne.org/math/CourseNotes/ant.html.