Algebraic Geomtery vs. Algebraic Number Theory

Notes on talk by Aaron Bertram

Utah: March 2010

Sonya Leibman

Review of the Gaussian Integers.

Definition.

- The *Gaussian Integers* $\mathbb{Z}[i]$ are the complex numbers of the form: $a+bi$ for $a, b \in \mathbb{Z}$
- The *Gaussian Rationals* $\mathbb{Q}[i]$ are the complex numbers of the form: $\alpha+\beta i$ for $\alpha, \beta \in \mathbb{Q}$

Note: $\mathbb{Q}(i)$ is a field, while $\mathbb{Z}[i]$ is not.

Properties.

1. Gaussian Integers have unique factorization.
2. Ordinary primes factor in $\mathbb{Z}[i]$ as follows:

$$2 = (1+i)(1-i) = (-i)(1+i)^2$$
$$5 = (2+i)(2-i)$$
$$13 = (3+2i)(3-2i)$$

   In general,

   (a) if $p \equiv 1 \mod 4$, then $p = a^2 + b^2 = (a+bi)(a-bi)$,
   (b) if $p \equiv 3 \mod 4$, then p remains irreducible in $\mathbb{Z}[i]$,

   and the factors (of the integer primes) are the primes in $\mathbb{Z}[i]$.

3. The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$

Trivial Fact:

Gaussian Integers are roots of monic polynomials with integer coefficients.
If $a+bi \in \mathbb{Z}[i]$, then it is a root of $p(x) = (x-(a+bi))(x-(a-bi)) = x^2 - 2ax + (a^2+b^2)$.

Cool Fact:

Converse!
A Gaussian Rational that is a root of a monic polynomial with integer coefficients is necessarily a Gaussian Integer.

What is Algebraic Number Theory?

Definition.

A *number field* is a finite field extension of the rationals:

$$\mathbb{Q} \subset K;\ [K:\mathbb{Q}] = d < \infty$$

In fact, every number field is $\mathbb{Q}(\alpha)$ for some algebraic number $\alpha \in \mathbb{C}$,
(that is a root of an irreducible plynomial $a_d x^d + a_{d-1}x^{d-1} + ... + a_o$ with rational coefficients),
and $\mathbb{Q}(\alpha)$ is a vector space over $\mathbb{Q}$ with basis $1, \alpha, \alpha^2, ..., \alpha^{d-1}$.

Algebraic Number Theory seeks an understanding of number fields.
Do this by studying:

Definition.

The ring $\mathcal{O}_K \subset K$ of *algebraic integers* consists of the numbers that are roots of monic polynomials with integer coefficients.

Remark:

We may study K by studying its ring of integers.

Sample Questions:

- What is $(\mathcal{O}_K, +)$ as an abelian group? (Easy: $\mathbb{Z}^d$).
- What is the group of units in $\mathcal{O}_K$? (Dirichlet Unit Theorem).
- Does $\mathcal{O}_K$ have unique factorization? And if not, "how far" is it from having unique factorization? (Hard. A central open question!).

Examples:

- $\mathbb{Q}(\sqrt{d})$, *quadratic fields*
- $\mathbb{Q}(e^{\frac{2\pi i}{p}})$
- $K = \mathbb{Q}(\sqrt{5})$.

  We know $\mathcal{O}_K \neq \mathbb{Z}[\sqrt{5}]$, since $\dfrac{-1 \pm \sqrt{5}}{2}$ is a root of $x^2 + x - 1 = 0$,
  but $\dfrac{-1 \pm \sqrt{5}}{2} \notin \mathbb{Z}(\sqrt{5})$. In fact,

$$\mathcal{O}_K = \{\frac{1}{2}(a + b\sqrt{5}); a, b \in \mathbb{Z}\}$$

As a lattice in the $1, \sqrt{5}$-plane, this is spanned by

$$\varphi, \psi = \frac{1}{2}(\pm 1 + \sqrt{5})$$

which are inverses of each other! Notice that

$$..., \psi, 1, \varphi, \varphi^2 = \frac{1}{2}(3 + \sqrt{5}), \varphi^3 = 2 + \sqrt{5}, \varphi^4 = \frac{1}{2}(7 + 3\sqrt{5}), ...$$

are all units, so the group of units is infinite.

This is a feature of all the *quadratic fields* $\mathbb{Q}(\sqrt{d})$ when d is a squarefree positive integer, and it generates the infinite set of integer solutions to *Pell's equation*: $x^2 - dy^2 = 1$

- $K = \mathbb{Q}(\sqrt{-5})$

  The ring of integers is $\mathbb{Z}[\sqrt{-5}]$.

  However, this does not have unique factorization, since, for example:
  $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, so there are two different ways of factoring 6 into irreducible algebraic integers.

  Although 2 is irreducible, it is not prime, since 2 divides $(1 + \sqrt{-5})^2 = -4 + 2\sqrt{-5}$, but 2 does not divide $1 + \sqrt{-5}$. Instead, the ideal $(2, 1 + \sqrt{-5})$ is prime (but not principal), and $(2) = (2, 1 + \sqrt{-5})^2$ as ideals.

What is Birational Complex Algebraic Geometry?

Instead of a number field, we study fields of finite *transcendence degree* over $\mathbb{C}$, or, what is the same thing, fields K that are a finite extension of a field of rational *functions*:

$$\mathbb{C}(t_1, ..., t_n) \subset K; [K : \mathbb{C}(t_1, ..., t_n)] \leq \infty$$

The analogue of the ring of integers is:

There are inclusions $\mathbb{C}[t_1, ...t_n] \subset \mathbb{C}(t_1, ..., t_n) \subset K$, which gives $\mathcal{O}_K \subset K$ as the roots of monic polynomials with coefficients in $\mathbb{C}[t_1, ...t_n]$. However, the inclusion $\mathbb{C}(t_1, ..., t_n) \subset K$ is not canonical, so $\mathcal{O}_K$ depends on the choice of $t_1, ...t_n$.

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \cup & & \cup \\ \mathbb{C}[t_1, ...t_n] & \subset & \mathbb{C}(t_1, ...t_n) \end{array}$$

Geometry is used to study $\mathcal{O}_K$.

Hilbert's Theorem:

The maximal ideals in $\mathbb{C}[x_1, ...x_n]$ are of the form $((x_1 - a_1), ..., (x_n - a_n))$.

Wonderful Propery of Algebraic Geometry:

$Spec(\mathcal{O}_K) = \{\text{maximal ideals in } \mathcal{O}_K\}$ has a natural"projective" compactification.

Example: n=1

Let $K = (\mathbb{C}(t))(\alpha)$, where α is a root of $x^2 - \prod_{i=1}^{d}(t - a_i)$.

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \cup & & \cup \\ \mathbb{C}[t] & \subset & \mathbb{C}(t) \end{array}$$

$$\begin{array}{ccc} C & \supseteq & Spec(\mathcal{O}_K) \\ \downarrow d & & \downarrow \\ S^2 = \mathbb{CP}^1 & \supset & \mathbb{C} = Spec(\mathbb{C}[t]), \end{array}$$

where C is a Riemann surface.

The Riemann surface does not depend on the choice of t!

C being a genus 0 surface, i.e. a Riemann Sphere, corresponds to $\mathcal{O}_K$ being a UFD.

C is a Riemann sphere $\Leftrightarrow K \simeq \mathbb{C}(s) \Leftrightarrow d = 1, 2$ where α is a root of $x^2 - \prod_{i=1}^{d}(t - a_i)$.

If $n > 1$, $Spec(\mathcal{O}_K)$ might not be a manifold.

Theorem(Hironaka):

Given K, there are choices of $t_1, ..., t_n$ s.t. X (the compactification of $Spec(\mathcal{O}_K)$) is a smooth, compact, complex manifold.

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \cup & & \cup \\ \mathbb{C}[t_1, ..., t_n] & \subset & \mathbb{C}(t_1, ...t_n) \end{array}$$

$$\begin{array}{ccc} X & \supseteq & Spec(\mathcal{O}_K) \\ \downarrow d & & \downarrow \\ \mathbb{CP}^n & \supset & \mathbb{C} = Spec(\mathbb{C}[t_1, ...t_n]) \end{array}$$

There are infinitely many possible isomorphism types!