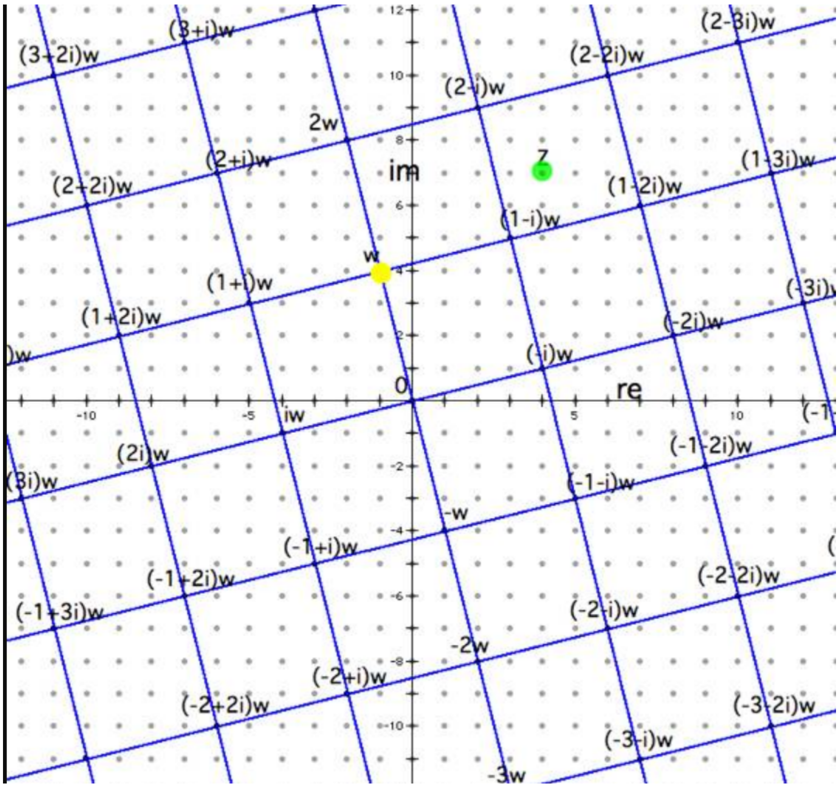

Notes: These are notes live-tex'd from a graduate course in Algebraic Number Theory taught by Paul Pollack at the University of Georgia in Spring 2021. As such, any errors or inaccuracies are almost certainly my own.

Algebraic Number Theory

Lectures by Paul Pollack. University of Georgia, Spring 2021

D. Zack Garza

D. Zack Garza
University of Georgia
dzackgarza@gmail.com

Last updated: 2021-01-17

Table of Contents

Contents

1 | Thursday, January 14

See website for notes on books, intro to class.

- Youtube Playlist: https://www.youtube.com/playlist?list=PLA0xtXqOUji8fjQysx4k8a6h-hOZ7x5ue

- Free copies of textbook: https://www.dropbox.com/sh/rv5j222kn74bjhm/AABZ1qcR1rOnpaBsa5CL3P_Ea?dl=0&lst=

- Course website: ?

Paul's description of the course:

"This course is an introduction to arithmetic"beyond $\mathbb{Z}$", specifically arithmetic in the ring of"integers" in a finite extension of $\mathbb{Q}$. (Among many other things) we'll prove three important theorems about these rings:

- Unique factorization into ideals.
- Finiteness of the group of ideal classes.
- Dirichlet's theorem on the structure of the unit group."

1.1 Motivation

Solving Diophantine equations, i.e. polynomial equations over $\mathbb{Z}$.

Example 1.1.1 ***(?):*** Consider $y^2 = x^3 + x$.

Claim: $(x, y) = (0, 0)$ is the only solution.

To see this, write $y^2 = x(x^2 + 1)$, which are relatively prime, i.e. no $D \in \mathbb{Z}$ divides both of them. Why? If $d \mid x$ and $d \mid x + 1$, then $d \mid (x^2 + 1) + (-x) = 1$. It's also the case that both $x^2 + 1$ and x^2 are squares (up to a unit), so $x^2, x^2 + 1$ are consecutive squares in $\mathbb{Z}$. But the gaps between squares are increasing: $1, 2, 4, 9, \cdots$. The only possibilities would be $x = 0, y = 1$, but in this case you can conclude $y = 0$.

Example 1.1.2 ***(Fermat):*** Consider $y^2 = x^3 - 2$.

Claim: $(3, \pm 5)$ are the only solutions.

Rewrite

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$$
$$\in \mathbb{Z}[\sqrt{-2}] \coloneqq \left\{ a + b\sqrt{-2} \;\middle|\; a, b, \in \mathbb{Z} \right\} \leq \mathbb{C}.$$

This is a subring of $\mathbb{C}$, and thus at least an integral domain. We want to try the same argument: showing the two factors are relatively prime. A little theory will help here:

Definition 1.1.3 ***(Norm Map)***
For $\alpha \in \mathbb{Z}[\sqrt{-2}]$ define $N\alpha = \alpha\overline{\alpha}$.

Lemma 1.1.4 ***(?).***
Let $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$. Then

1. $N(\alpha\beta) = N(\alpha)N(\beta)$
2. $N(\alpha) \in \mathbb{Z}_{\geq 0}$ and $N(\alpha) = 0$ if and only if $\alpha = 0$.
3. $N(\alpha) = 1 \iff \alpha \in R^\times$

Proof (?). 1. Missing, see video (10:13 AM).

2. $N(\alpha) = a^2 + 2b^2 \geq 0$, so this equals zero if and only if $\alpha = \beta = 0$
3. Write $1 = \alpha\overline{\alpha}$ if $N(\alpha) = 1 \in R^\times$. Conversely if $\alpha \in R^\times$ write $\alpha\beta = 1$, then
$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta) \in \mathbb{Z}_{\geq 0},$$
which forces both to be 1.

■

Claim: The two factors $y \pm \sqrt{2}$ are *coprime* in $\mathbb{Z}[\sqrt{-2}]$, i.e. every common divisor is a unit.

Proof (?).
Suppose $\delta \mid y \pm \sqrt{-2}$, then $y + \sqrt{-2} = \delta\beta$ for some $\beta \in \mathbb{Z}[\sqrt{-2}]$. Take norms to obtain $y^2 + 2 = N\delta N\beta$, and in particular

- $N\delta y^2 + 2$
- $\delta \mid (y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2}$ and thus $N\delta \mid N(2\sqrt{-2}) = 8$.

In the original equation $y^2 = x^3 - 2$, if y is even then x is even, and $x^3 - 2 \equiv 0 - 2 \pmod 4 \equiv 2$, and so $y^2 \equiv 2 \pmod 4$. But this can't happen, so y is odd, and we're done: we have $N\delta \mid 8$ which is even or 1, but $N\delta \mid y^2 + 2$ which is odd, so $N\delta = 1$.

■

We can identify the units in this ring:

$$\mathbb{Z}[\sqrt{-2}]^\times = \left\{ a + b\sqrt{-2} \;\middle|\; a^2 + 2b^2 = 1 \right\}$$

which forces $a^2 \leq 1, b^2 \leq 1$ and thus this set is $\{\pm 1\}$.

So we have $x^3 = ab$ which are relatively primes, so a, b should also be cubes. We don't have to worry about units here, since ± 1 are both cubes. So e.g. we can write

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

Comparing coefficients of $\sqrt{-2}$ yields

$$1 = b(3a^2 b - 2b^2) \in \mathbb{Z} \implies b \mid 1,$$

and thus $b \in \mathbb{Z}^\times$, i.e. $b \in \{\pm 1\}$. By cases:

- If $b = 1$, then $1 = 3a^2 - 2 \implies a^2 = 1 \implies a = \pm 1$. So

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

  which forces $y = \pm 5$, the solution we already knew.

- If $b = -1$, then $1 = -(3a^2 - 1)$ which forces $1 = 3a^2 \in \mathbb{Z}$, so there are no solutions.

Example 1.1.5 ***(?):*** Consider $y^2 = x^3 - 26$. Rewrite this as

$$x^3 = y^2 + 26 = (y + \sqrt{-26})(y - \sqrt{-26}),$$

then the same lemma goes through with 2 replaced by 26 everywhere where the RHS factors are still coprime. Setting $y + \sqrt{-26} = (a + b\sqrt{-26})^3$ and comparing coefficients, you'll find $b = 1, a = \pm 3$. This yields $x = 35, y = \pm 207$. But there are more solutions: $(x, y) = (3, \pm 1)$! The issue is that we used unique factorization when showing that ab is a square implies a or b is a square (say by checking prime factorizations and seeing even exponents). In this ring, we can have ab a cube with *neither* a, b a cube, even up to a unit.

Question 1.1.6
When does a ring admit unique factorization? Do you even *need* it?

This will lead to a discussion of things like the **class number**, which measure the failure of unique factorization. In general, the above type of proof will work when the class number is 3!

ToDos

List of Todos

1

Definitions

1 Theorems

1 Exercises

Figures

List of Figures