A brief history of rings

Daniel Smolkin

Department of Mathematics
University of Utah

GSAC Colloquium

March 24, 2015

Intro

Commutative algebra is concerned with the study of these abstract things called

- Rings (generalizations of the integers)
- Modules (generalizations of vector spaces)
- Ideals (special kinds of modules)

This talk will explore where these notions came from

Ancient Greece

Let a, b, c be integers. If p is prime and p divides ab, then p divides a or p divides b. This gives unique prime factorization—each integer a can be written in a unique (up to order) way as a product of primes

$$a = p_1 p_2 \cdots p_n$$

Uniqueness means that if $a = q_1 q_2 \cdots q_m$ is another prime factorization, then $m = n$ and each q_j is equal to a unique p_i.

We say that a and b are relatively prime if their greatest common divisor, or gcd, is 1. Equivalently, any prime appearing in the factorization of a does not appear in the factorization of b.
Uniqueness of prime factorization implies:

Theorem

if $ab = c^2$ *and* $\gcd(a, b) = 1$ *then* a *and* b *are both perfect squares.*

Theorem

if $ab = c^2$ *and* $\gcd(a, b) = 1$ *then* a *and* b *are both perfect squares.*

Proof.

- Let $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$, and $c = r_1 \cdots r_l$ be prime factorizations of a, b, and c.

Similarly, if $ab = c^n$ and $\gcd(a, b) = 1$, then a and b are nth powers

Theorem

if $ab = c^2$ *and* $\gcd(a, b) = 1$ *then* a *and* b *are both perfect squares.*

Proof.

- Let $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$, and $c = r_1 \cdots r_l$ be prime factorizations of a, b, and c.
- Then $c^2 = ab = p_1 \cdots p_n q_1 \cdots q_m$ is a prime factorization of c^2

Similarly, if $ab = c^n$ and $\gcd(a, b) = 1$, then a and b are nth powers

Theorem

if $ab = c^2$ *and* $\gcd(a, b) = 1$ *then* a *and* b *are both perfect squares.*

Proof.

- Let $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$, and $c = r_1 \cdots r_l$ be prime factorizations of a, b, and c.
- Then $c^2 = ab = p_1 \cdots p_n q_1 \cdots q_m$ is a prime factorization of c^2
- But $c^2 = (r_1 \cdots r_l)^2 = r_1 r_1 \cdots r_l r_l$ is another prime factorization of c^2. By uniqueness, each r_i either appears in $p_1, \cdots, p_n, q_1, \cdots, q_m$

Similarly, if $ab = c^n$ and $\gcd(a, b) = 1$, then a and b are nth powers

Theorem

if $ab = c^2$ *and* $\gcd(a, b) = 1$ *then* a *and* b *are both perfect squares.*

Proof.

- Let $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$, and $c = r_1 \cdots r_l$ be prime factorizations of a, b, and c.
- Then $c^2 = ab = p_1 \cdots p_n q_1 \cdots q_m$ is a prime factorization of c^2
- But $c^2 = (r_1 \cdots r_l)^2 = r_1 r_1 \cdots r_l r_l$ is another prime factorization of c^2. By uniqueness, each r_i either appears in $p_1, \cdots, p_n, q_1, \cdots, q_m$
- So each r_i appears in $p_1, \cdots, p_n$ or in $q_1, \cdots, q_m$. Since $\gcd(a, b) = 1$, if one copy of r_i appears in $p_1, \cdots, p_n$ then the second one does too.

□

Similarly, if $ab = c^n$ and $\gcd(a, b) = 1$, then a and b are nth powers

Theorem

if $ab = c^2$ *and* $\gcd(a, b) = 1$ *then* a *and* b *are both perfect squares.*

Proof.

- Let $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$, and $c = r_1 \cdots r_l$ be prime factorizations of a, b, and c.
- Then $c^2 = ab = p_1 \cdots p_n q_1 \cdots q_m$ is a prime factorization of c^2
- But $c^2 = (r_1 \cdots r_l)^2 = r_1 r_1 \cdots r_l r_l$ is another prime factorization of c^2. By uniqueness, each r_i either appears in $p_1, \cdots, p_n, q_1, \cdots, q_m$
- So each r_i appears in $p_1, \cdots, p_n$ or in $q_1, \cdots, q_m$. Since $\gcd(a, b) = 1$, if one copy of r_i appears in $p_1, \cdots, p_n$ then the second one does too.
- Thus $a = r_1 r_1 \cdots r_j r_j = (r_1 \cdots r_j)^2$ for some j.

□

Similarly, if $ab = c^n$ and $\gcd(a, b) = 1$, then a and b are nth powers

Much of mathematics was (and is) about asking such questions about the integers.

Much of mathematics was (and is) about asking such questions about the integers.

In 1770, Euler noticed that it's often useful to use complex numbers to prove things about the integers. For instance, he solved the following conjecture, due to Fermat(1601–1665): 27 is the only perfect cube that's 2 bigger than a perfect sqaure. In other words, the only integer solution to

$$y^3 = x^2 + 2$$

is $(x, y) = (\pm 5, 3)$

- Euler proved this by using $\sqrt{-2}$ to factor $x^2 + 2 = \left(x + \sqrt{-2}\right)\left(x - \sqrt{-2}\right)$. So he worked with numbers of the form $a + b\sqrt{-2}$ where a, b are integers

- Euler proved this by using $\sqrt{-2}$ to factor $x^2 + 2 = \left(x + \sqrt{-2}\right)\left(x - \sqrt{-2}\right)$. So he worked with numbers of the form $a + b\sqrt{-2}$ where a, b are integers
- Similarly, Gabriel Lamé used the number $\zeta_n = e^{2\pi i/n}$ in a proposed solution to Fermat's last thoerem in 1847.

- Euler proved this by using $\sqrt{-2}$ to factor $x^2 + 2 = \left(x + \sqrt{-2}\right)\left(x - \sqrt{-2}\right)$. So he worked with numbers of the form $a + b\sqrt{-2}$ where a, b are integers
- Similarly, Gabriel Lamé used the number $\zeta_n = e^{2\pi i/n}$ in a proposed solution to Fermat's last thoerem in 1847.
- This lead Dedekind to define a *domain of algebraic integers* as any set that's just the integers plus some other stuff in 1871.

- Euler proved this by using $\sqrt{-2}$ to factor $x^2 + 2 = \left(x + \sqrt{-2}\right)\left(x - \sqrt{-2}\right)$. So he worked with numbers of the form $a + b\sqrt{-2}$ where a, b are integers
- Similarly, Gabriel Lamé used the number $\zeta_n = e^{2\pi i/n}$ in a proposed solution to Fermat's last thoerem in 1847.
- This lead Dedekind to define a *domain of algebraic integers* as any set that's just the integers plus some other stuff in 1871.
- Technical aside: let K be a finite field extension of $\mathbb{Q}$. Then Dedekind defined the domain of algebraic integers of K to be the integral closure of $\mathbb{Z}$ in K).

- Euler proved this by using $\sqrt{-2}$ to factor $x^2 + 2 = \left(x + \sqrt{-2}\right)\left(x - \sqrt{-2}\right)$. So he worked with numbers of the form $a + b\sqrt{-2}$ where a, b are integers
- Similarly, Gabriel Lamé used the number $\zeta_n = e^{2\pi i/n}$ in a proposed solution to Fermat's last thoerem in 1847.
- This lead Dedekind to define a *domain of algebraic integers* as any set that's just the integers plus some other stuff in 1871.
- Technical aside: let K be a finite field extension of $\mathbb{Q}$. Then Dedekind defined the domain of algebraic integers of K to be the integral closure of $\mathbb{Z}$ in K).
- Later, Hilbert called these sets *Zahlrings*, or "number rings", in 1892

- Euler proved this by using $\sqrt{-2}$ to factor $x^2 + 2 = \left(x + \sqrt{-2}\right)\left(x - \sqrt{-2}\right)$. So he worked with numbers of the form $a + b\sqrt{-2}$ where a, b are integers
- Similarly, Gabriel Lamé used the number $\zeta_n = e^{2\pi i/n}$ in a proposed solution to Fermat's last thoerem in 1847.
- This lead Dedekind to define a *domain of algebraic integers* as any set that's just the integers plus some other stuff in 1871.
- Technical aside: let K be a finite field extension of $\mathbb{Q}$. Then Dedekind defined the domain of algebraic integers of K to be the integral closure of $\mathbb{Z}$ in K).
- Later, Hilbert called these sets *Zahlrings*, or "number rings", in 1892
- Wikipedia: "ring" is a synonym for "group." Think "drug ring"

Notation: $\mathbb{Z}[\alpha]$ means "take the integers and throw in α." So the set of numbers of the form $a + b\sqrt{-2}$ is denoted $\mathbb{Z}[\sqrt{-2}]$.

- So that's where rings come from!

- So that's where rings come from!
- The story of *ideals* is more complicated

- So that's where rings come from!
- The story of *ideals* is more complicated
- Let's look at Euler's proof that the only integer solution to $y^3 = x^2 + 2$ is $(x, y) = (\pm 5, 3)$

$$y^3 = x^2 + 2$$

We can factor $x^2 + 2 = \left(x + \sqrt{-2}\right)\left(x - \sqrt{-2}\right)$. Then Euler treats the quantities $x - \sqrt{-2}$ and $x + \sqrt{-2}$ as though they were integers: he asserts they're "relatively prime," and since their product is a cube, they must be cubes themselves. Thus we can say

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

$$y^3 = x^2 + 2$$

We can factor $x^2 + 2 = \left(x + \sqrt{-2}\right)\left(x - \sqrt{-2}\right)$. Then Euler treats the quantities $x - \sqrt{-2}$ and $x + \sqrt{-2}$ as though they were integers: he asserts they're "relatively prime," and since their product is a cube, they must be cubes themselves. Thus we can say

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

Equating real and imaginary parts,

$$x = a^3 - 6ab^2$$
$$\sqrt{-2} = \left(3a^2b - 2b^3\right)\sqrt{-2}$$

Thus $1 = b\left(3a^2 - 2b^2\right)$. Thus $b = \pm 1$ and $3a^2 - 2b^2 = \pm 1$, so $a = \pm 1$. Thus $x = a^3 - 6ab^2 = \pm 5$ and $y = 3$

- The question: Does Euler's approach really work? When does it work?

- The question: Does Euler's approach really work? When does it work?
- First question: yes

- The question: Does Euler's approach really work? When does it work?
- First question: yes
- Second question: it's an open problem! (Sort of) We'll get back to this.

- The question: Does Euler's approach really work? When does it work?
- First question: yes
- Second question: it's an open problem! (Sort of) We'll get back to this.
- Rings where you have unique factorization into primes are called *unique factorization domains*.

- In this case, we're considering the ring $\left\{a + b\sqrt{-2} \mid a, b \text{ integers}\right\}$, aka $\mathbb{Z}[\sqrt{-2}]$.

- In this case, we're considering the ring $\left\{a + b\sqrt{-2} \mid a, b \text{ integers}\right\}$, aka $\mathbb{Z}[\sqrt{-2}]$.
- Let $x \mid y$ denote "x divides y"

- In this case, we're considering the ring $\left\{a + b\sqrt{-2} \mid a, b \text{ integers}\right\}$, aka $\mathbb{Z}[\sqrt{-2}]$.
- Let $x \mid y$ denote "x divides y"
- In analogy with the integers, $a + b\sqrt{-2}$ is a "prime" of $\mathbb{Z}[\sqrt{-2}]$ if it satisfies

$$(a + b\sqrt{-2}) \mid \left(c + d\sqrt{-2}\right)\left(e + f\sqrt{-2}\right) \Rightarrow$$

$$\left(a + b\sqrt{-2}\right) \mid \left(c + d\sqrt{-2}\right) \text{ or } \left(a + b\sqrt{-2}\right) \mid \left(e + f\sqrt{-2}\right)$$

- In this case, we're considering the ring $\left\{a + b\sqrt{-2} \mid a, b \text{ integers}\right\}$, aka $\mathbb{Z}[\sqrt{-2}]$.
- Let $x \mid y$ denote "x divides y"
- In analogy with the integers, $a + b\sqrt{-2}$ is a "prime" of $\mathbb{Z}[\sqrt{-2}]$ if it satisfies

$$(a + b\sqrt{-2}) \mid \left(c + d\sqrt{-2}\right)\left(e + f\sqrt{-2}\right) \Rightarrow$$

$$\left(a + b\sqrt{-2}\right) \mid \left(c + d\sqrt{-2}\right) \text{ or } \left(a + b\sqrt{-2}\right) \mid \left(e + f\sqrt{-2}\right)$$

- (Recall: an integer p is prime if $p \mid ab \Leftrightarrow p \mid a$ or $p \mid b$)

So to make Euler's proof legit, we need to find out what the primes of $\mathbb{Z}\left[\sqrt{-2}\right]$ are and whether each number factorizes into these primes *uniquely*

So to make Euler's proof legit, we need to find out what the primes of $\mathbb{Z}\left[\sqrt{-2}\right]$ are and whether each number factorizes into these primes *uniquely*

It's not obvious! E.g. 5 is not prime in $\mathbb{Z}[\sqrt{-2}]$:

$$5 = \left(1 + \sqrt{-2}\right)\left(1 - \sqrt{-2}\right)$$

and 5 doesn't divide either factor on the right. Can see this by taking absolute values of each side

Fermat's last theorem: there are no integer solutions to $x^n + y^n = z^n$ for $n > 2$

In 1847, Gabriel Lamé gave a (false) proof of Fermat's last theorem using the same approach as Euler. He begins by writing $y^n = z^n - x^n$. Then he factors the right hand side:

$$z^n - x^n = (z - x)(z - \zeta_n x)\left(z - \zeta_n^2 x\right) \cdots \left(z - \zeta_n^{n-1} x\right)$$

where

$$\zeta_n = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$$

So far so good. But then Lamé makes the same assumption as Euler: that each term in the factorization is relatively prime to all of the others, and that this implies each term on the right is an n^{th} power. Not true!

- Kummer (1810–1893) showed three years earlier that this fails for $n = 23$; in fact, it fails for n any prime greater than 19.
- So the question of which rings have unique factorization was very important
- Kummer invented *ideal numbers* to figure this out, and maybe to salvage Lamè's proof.
- The idea—suppose our ring doesn't have unique factorization. Can we introduce new numbers until it does?

"In the theory of rational integers, one can recognise the essential constitution of a number without effecting its decomposition into prime factors, observing only how it behaves as a divisor."–Dedekind

- If there is some b with $a \nmid b$ but $a \mid b^2$, then some prime must appear twice in the factorization of a. Intuition: "a only divides b after you double some of the primes in b's factorization"

"In the theory of rational integers, one can recognise the essential constitution of a number without effecting its decomposition into prime factors, observing only how it behaves as a divisor."–Dedekind

- If there is some b with $a \nmid b$ but $a \mid b^2$, then some prime must appear twice in the factorization of a. Intuition: "a only divides b after you double some of the primes in b's factorization"
- Suppose $a \mid b^2c^2$ only when $a \mid b^2$ or $a \mid c^2$. Then a is either 1, a prime, or the square of a prime. (It's easy to show by constructing counterexamples)

"In the theory of rational integers, one can recognise the essential constitution of a number without effecting its decomposition into prime factors, observing only how it behaves as a divisor."–Dedekind

- If there is some b with $a \nmid b$ but $a \mid b^2$, then some prime must appear twice in the factorization of a. Intuition: "a only divides b after you double some of the primes in b's factorization"
- Suppose $a \mid b^2c^2$ only when $a \mid b^2$ or $a \mid c^2$. Then a is either 1, a prime, or the square of a prime. (It's easy to show by constructing counterexamples)
- So if both of these hold, then $a = p^2$ for some prime p

Ideal numbers

- The number 2 has both of these properties when you're working in $\mathbb{Z}[\sqrt{-5}]$:

Ideal numbers

- The number 2 has both of these properties when you're working in $\mathbb{Z}[\sqrt{-5}]$:
- For instance, 2 does not divide $1+\sqrt{-5}$, but 2 does divide $\left(1+\sqrt{-5}\right)^2 = -4+2\sqrt{-5}$.

Ideal numbers

- The number 2 has both of these properties when you're working in $\mathbb{Z}[\sqrt{-5}]$:
- For instance, 2 does not divide $1+\sqrt{-5}$, but 2 does divide $\left(1+\sqrt{-5}\right)^2 = -4+2\sqrt{-5}$.
- Moreover, let $\omega = a+b\sqrt{-5}$. Then $\omega - \bar{\omega} = 2b\sqrt{-5}$, so $\omega \equiv \bar{\omega} \bmod 2$. I.e., ω is divisible by 2 precisely when $\bar{\omega}$ is divisible by 2.

Ideal numbers

- The number 2 has both of these properties when you're working in $\mathbb{Z}[\sqrt{-5}]$:
- For instance, 2 does not divide $1+\sqrt{-5}$, but 2 does divide $\left(1+\sqrt{-5}\right)^2 = -4+2\sqrt{-5}$.
- Moreover, let $\omega = a+b\sqrt{-5}$. Then $\omega - \bar{\omega} = 2b\sqrt{-5}$, so $\omega \equiv \bar{\omega}$ mod 2. I.e., ω is divisible by 2 precisely when $\bar{\omega}$ is divisible by 2.
- Thus $\omega^2 \equiv |\omega|^2$ modulo 2. So if 2 divides $\omega^2\omega'^2$, then 2 divides their norm $|\omega\omega'|^2 = |\omega|^2|\omega'|^2$

Ideal numbers

- The number 2 has both of these properties when you're working in $\mathbb{Z}[\sqrt{-5}]$:
- For instance, 2 does not divide $1+\sqrt{-5}$, but 2 does divide $\left(1+\sqrt{-5}\right)^2 = -4+2\sqrt{-5}$.
- Moreover, let $\omega = a+b\sqrt{-5}$. Then $\omega - \bar{\omega} = 2b\sqrt{-5}$, so $\omega \equiv \bar{\omega}$ mod 2. I.e., ω is divisible by 2 precisely when $\bar{\omega}$ is divisible by 2.
- Thus $\omega^2 \equiv |\omega|^2$ modulo 2. So if 2 divides $\omega^2\omega'^2$, then 2 divides their norm $|\omega\omega'|^2 = |\omega|^2|\omega'|^2$
- 2 is prime in the integers so that means 2 divides $|\omega|^2$ or $|\omega'|^2$. So 2 divides ω^2 or ω'^2.

- So by analogy with integers, 2 should be p^2 for some prime p.
- But 2 is not a square in $\mathbb{Z}[\sqrt{-5}]$!
- So Kummer says: so what? Just declare that $2 = \alpha^2$. α is just a formal symbol.
- We can define what it means to be "divisible by α": we say

$$\alpha \mid \omega \text{ whenever } 2 \mid \omega^2$$

Similar deductions show that 3 and 7 behave like products of distinct primes.

$$3 = \beta_1 \beta_2$$
$$7 = \gamma_1 \gamma_2$$

Now, the number 6 has two factorizations in $\mathbb{Z}[\sqrt{-5}]\ldots$

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

Similar deductions show that 3 and 7 behave like products of distinct primes.

$$3 = \beta_1\beta_2$$
$$7 = \gamma_1\gamma_2$$

Now, the number 6 has two factorizations in $\mathbb{Z}[\sqrt{-5}]$...

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

But only one in terms of these ideal numbers! One can show $\alpha\beta_1 = 1 + \sqrt{-5}$ and $\alpha\beta_2 = 1 - \sqrt{-5}$, whence

$$\begin{aligned} 6 = 2 \cdot 3 &= \alpha^2\beta_1\beta_2 \\ &= \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) = \alpha\beta_1\alpha\beta_2 \end{aligned}$$

Kummer showed that rings like $\mathbb{Z}[\zeta_n]$ (the context of Lamé's proof) have unique factorization in terms of these ideal numbers. Thus $\mathbb{Z}[\zeta_n]$ is itself a UFD if there are no ideal numbers.

Kummer showed that rings like $\mathbb{Z}[\zeta_n]$ (the context of Lamé's proof) have unique factorization in terms of these ideal numbers. Thus $\mathbb{Z}[\zeta_n]$ is itself a UFD if there are no ideal numbers.

Aside: you could just as easily say $\alpha = \sqrt{2}$, and similarly, $\beta_1 = \sqrt{-2+\sqrt{-5}}$, $\beta_2 = \sqrt{-2-\sqrt{-5}}$ and work in the ring $\mathbb{Z}[\sqrt{-5}, \alpha, \beta_1, \beta_2, \gamma_1, \gamma_2]$. Indeed, this was the approach of Kronecker (1823–1891), who was a constructivist. But this is a departure from the philosophy of studying numbers by their divisibility properties. Further, Dedekind complains that this approach requires thinking about a more complicated ring, and that this choice of ring extension is arbitrary.

Ideal numbers worked well from Kronecker, but they're far from ideal:

- What is an ideal number? There's no actual definition
- Dedekind: "The greatest circumspection is required to avoid being led to premature conclusions. In particular, the notion of product of arbitrary factors, actual or ideal, cannot be exactly defind without going into minute detail."

Further, this only solves the problem of unique factorization in Lamé's case of cyclotomic integers.
Dedekind's insight: instead of talking about ideal numbers, just talk about all the actual numbers that are divisible by them!

- Recall that $\omega = a + b\sqrt{-5}$ is said to be divisible by α if and only if $2 \mid \omega^2$.

- Recall that $\omega = a + b\sqrt{-5}$ is said to be divisible by α if and only if $2 \mid \omega^2$.
- Further, $\omega^2 \equiv |\omega|^2 \bmod 2$, and $|\omega|^2 = a^2 + 5b^2$ is even if and only if $a \equiv b \bmod 2$.

- Recall that $\omega = a + b\sqrt{-5}$ is said to be divisible by α if and only if $2 \mid \omega^2$.
- Further, $\omega^2 \equiv |\omega|^2 \bmod 2$, and $|\omega|^2 = a^2 + 5b^2$ is even if and only if $a \equiv b \bmod 2$.
- So $\alpha \mid \omega$ if and only if $a = b + 2z$ for some integer z.

- Recall that $\omega = a + b\sqrt{-5}$ is said to be divisible by α if and only if $2 \mid \omega^2$.
- Further, $\omega^2 \equiv |\omega|^2 \bmod 2$, and $|\omega|^2 = a^2 + 5b^2$ is even if and only if $a \equiv b \bmod 2$.
- So $\alpha \mid \omega$ if and only if $a = b + 2z$ for some integer z.
- Thus the set of numbers divisible by α is $\left\{b + 2z + b\sqrt{-5} \mid b, z \in \mathbb{Z}\right\} = \left\{2z + \left(1 + \sqrt{-5}\right) b \mid z, b \in \mathbb{Z}\right\}$

- Recall that $\omega = a + b\sqrt{-5}$ is said to be divisible by α if and only if $2 \mid \omega^2$.
- Further, $\omega^2 \equiv |\omega|^2 \bmod 2$, and $|\omega|^2 = a^2 + 5b^2$ is even if and only if $a \equiv b \bmod 2$.
- So $\alpha \mid \omega$ if and only if $a = b + 2z$ for some integer z.
- Thus the set of numbers divisible by α is $\left\{b + 2z + b\sqrt{-5} \mid b, z \in \mathbb{Z}\right\} = \left\{2z + \left(1 + \sqrt{-5}\right) b \mid z, b \in \mathbb{Z}\right\}$
- So this is all linear combinations of 2 and $1 + \sqrt{-5}$ with integer coefficients. Dedekind denotes this set by $\left[2, 1 + \sqrt{-5}\right]$

- This set has the following properties:

- This set has the following properties:
  - $r \in \mathbb{Z}\left[\sqrt{-5}\right], x \in \left[2, 1+\sqrt{-5}\right] \Rightarrow rx \in \left[2, 1+\sqrt{-5}\right]$

- This set has the following properties:
  - $r \in \mathbb{Z}\left[\sqrt{-5}\right], x \in \left[2, 1+\sqrt{-5}\right] \Rightarrow rx \in \left[2, 1+\sqrt{-5}\right]$
  - $x, y \in [2, 1+\sqrt{-5}] \Rightarrow x+y \in [2, 1+\sqrt{-5}]$

- This set has the following properties:
  - $r \in \mathbb{Z}\left[\sqrt{-5}\right], x \in \left[2, 1+\sqrt{-5}\right] \Rightarrow rx \in \left[2, 1+\sqrt{-5}\right]$
  - $x, y \in [2, 1+\sqrt{-5}] \Rightarrow x+y \in [2, 1+\sqrt{-5}]$
- Then Dedekind does something unprecedented—he defines an ideal as any subset of a ring that satisfies these properties!

- This set has the following properties:
  - $r \in \mathbb{Z}\left[\sqrt{-5}\right], x \in \left[2, 1+\sqrt{-5}\right] \Rightarrow rx \in \left[2, 1+\sqrt{-5}\right]$
  - $x, y \in [2, 1+\sqrt{-5}] \Rightarrow x+y \in [2, 1+\sqrt{-5}]$
- Then Dedekind does something unprecedented—he defines an ideal as any subset of a ring that satisfies these properties!
- Aside: he also defined a *module* to be any subset of a ring satisfying the second property

These sorts of axiomatic definitions are standard in mathematics now, but no one made them since the Greeks until Dedekind

- So we get from ideal numbers to ideals by taking the set of all numbers divisible by the ideal number. Can do this for regular numbers as well: the set of all numbers divisible by 2 is $\{2z \mid z \in \mathbb{Z}[\sqrt{-5}]\}$
- Note that if $\alpha \mid \beta$ then the ideal corresponding to α will contain the ideal corresponding to β. So we say that I divides J if $I \mid J$. So Dedekind defines a *prime ideal* to be an ideal that's not contained in any other ideal, except $\mathbb{Z}[\sqrt{-5}]$ itself.
- Finally, the product of the ideals corresponding to α and β should the the ideal corresponding to the product $\alpha\beta$. So we define the product of two ideals: $IJ = \{\sum_{finite} a_i b_i \mid a_i \in I, b_i \in J\}$.

Dedekind then proved the following:

Theorem

Each ideal I can be uniquely written as a product of prime ideals,

$$I = P_1 \dots P_n$$

This theorem holds true everywhere that Dedekind called a ring. We now call these rings *Dedekind domains*

- We can use this result to determine whether a given domain has Unique Factorization
- Namely, if every ideal has just one generator, then unique factorization holds! Every factorization of a number gives a factorization of the ideal it generates. The converse holds too, in this case.
- This leads to the theory of class numbers

Class numbers

The set of ideals of any ring forms a monoid: it's closed under multiplication. If your ring R is a dedekind domain (think $\mathbb{Z}\left[\sqrt{D}\right]$), then you can define the multiplicative inverse of an ideal I to be

$$I^{-1} = \{r \in \text{frac } R \mid rI \subseteq R\}$$

This gives an abelian group G under multiplication. The principal ideals and their inverses form a subgroup P. Then the *ideal class group of* R is defined to be G/P. The size of $|G/P|$ is called the *class number* of R. So we've shown that if R is a Dedekind domain, then R is a UFD if and only if its class number is 1.

Big open problem: when is the class number of $\mathbb{Z}[\sqrt{d}]$ equal to 1? Are there infinitely many d where this is true?

If $d < 0$, then the class number is one only in the following cases:

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

Modern definition of a ring

- Meanwhile, algebraic geometers were doing very similar work, only they were thinking about polynomials
- Adolf Fraenkel gave an axiomatic definition of a ring in 1914 that included both cases
- Emmy Noether noticed this definition was not quite right, and published the modern definition in 1921

The modern definition of a ring

A ring is a set A with two functions $p : A \times A \to A$ and $t : A \times A \to A$ satisfying:

1. p(a,b) = p(b,a)
2. there is some element $0 \in A$ satisfying p(0,a) = a for all $a \in A$
3. For each $a \in A$ there is some element $-a \in A$ satisying p(a,-a) = 0
4. p(a, p(b,c)) = p(p(a,b), c) for all a, b, c
5. t(a,t(b,c)) = t(t(a,b), c)
6. There is some element 1 in A satisfying t(a,1) = t(1, a) = a for all $a \in A$.
7. t(a, p(b,c)) = p(t(a,b), t(a, c))
8. t(p(a,b), c) = p(t(a,c), t(b,c))

At the same time Noether invented the *theory* of rings defined this way. She figured out the hypotheses you need for prime factorization of ideals (Dedekind). Namely:

- Ascending chain condition
- Normality
- Every prime ideal is maximal

And found a weaker form of prime factorization (algebraic geometers) when you just have the first hypothesis.

Happy birthday Emmy Noether!

References

- `http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Ring_theory.html`
- Dedekind, Richard. *The Theory of Algebraic Integers*. Translated by John Stillwell. 1996
- Edwards, Harold M. *Fermat's last theorem: a genetic intro. to alg. number theory*. 1977
- Kleiner, Israel. *A History of Abstract Algebra*. 2007