Tues Jan 14, 2014

Welcome to MTH 562.
I'm filling in for Bruno De Oliveira

— Last semester you discussed
Artin Chapters 2–7

i.e. Groups & Linear Algebra.

— This semester we will discuss
Artin Chapters 11–16

i.e. Commutative Rings & Modules.

HOWEVER: My presentation will be more elementary / fundamental than Artin's.

My main theme is the analogy between two rings

$\mathbb{Z}$	$K[x]$
The Integers	Polynomials in 1 variable over a field.
(Z is for Zahlen)	(K is for Körper)

This analogy is the foundation of modern number theory and algebraic geometry.

Course Evaluation:

25% Homework
25% Exam 1
25% Exam 2
25% Exam 3
NO FINAL EXAM. (except for the grad prelim)

BEGIN:

(1) Review of $\mathbb{Z}$ (with a view toward ring theory)

What is $\mathbb{Z}$?

Joke Definition:

$$\mathbb{Z} := \{ \cdots < -2 < -1 < 0 < 1 < 2 < \cdots \}$$

It's an abelian group $(\mathbb{Z}, +, 0)$.
In fact it's a cyclic group, generated by the special element $1 \in \mathbb{Z}$.

$$\mathbb{Z} = \langle 1 \rangle$$

What are the subgroups of $\mathbb{Z}$?

[Notation: Given $a \in \mathbb{Z}$ we write

$$(a) \text{ OR } a\mathbb{Z} = \{\ldots, -2a, -a, 0, a, 2a, \ldots\}$$

for the cyclic group generated by a.]

Theorem: Every subgroup of $(\mathbb{Z}, +, 0)$ has the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$.

Proof: Let $H \leq \mathbb{Z}$ be a subgroup.
If $H = \{0\} = 0\mathbb{Z}$ we're done, so suppose that $H \neq \{0\}$ and let a be the smallest positive element of H.

[Why does this a exist?]

We claim that $H = a\mathbb{Z}$.

(1) Since H is a group and $a \in H$ we have $a\mathbb{Z} \subseteq H$

(2) To show that $H \subseteq a\mathbb{Z}$, consider any element $h \in H$.

By the Division Algorithm, there exist $q, r \in \mathbb{Z}$ such that

$$h = qa + r \quad \& \quad 0 \leq r < a.$$

[How can this be proved?]

But then since h and $qa \in H$ we have $r = h - qa \in H$ with
$0 \leq r < a$.

Since a was the smallest nonzero elt. of H we conclude that

$$r = 0 \Rightarrow h = qa \Rightarrow h \in a\mathbb{Z}.$$

Hence $H \subseteq a\mathbb{Z}$. ∎

But $\mathbb{Z}$ has more structure than just $(\mathbb{Z}, +, 0)$.

It is also a multiplicative semigroup $(\mathbb{Z}, \times, 1)$.

and the two operations <u>distribute</u>:

$\forall\, a, b, c \in \mathbb{Z}$ we have

$$a(b+c) = ab + ac.$$

Now here's a fun trick:

Given $a, b \in \mathbb{Z}$ consider the set

$$a\mathbb{Z} + b\mathbb{Z} = \{ax + by : x, y \in \mathbb{Z}\}.$$

Note that is is a subgroup of $(\mathbb{Z}, +, 0)$:

Given $ax_1 + by_1$ and $ax_2 + by_2 \in a\mathbb{Z} + b\mathbb{Z}$ we have

$$(ax_1 + by_1) - (ax_2 + by_2)$$
$$= a(x_1 - x_2) + b(y_1 - y_2) \in a\mathbb{Z} + b\mathbb{Z}$$

Hence by the previous theorem there exists $d \geq 0$ such that

$$\boxed{a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}}.$$

What is this d?

Since $a \in a\mathbb{Z} + b\mathbb{Z}$ we have
$a \in d\mathbb{Z} \implies d \mid a$.

Similarly, $d \mid b$.

So d is a <u>common</u> divisor of a, b.

Claim: d is the <u>greatest</u> common divisor of a, b.

<u>Proof</u>: Suppose e is <u>any</u> common divisor, i.e. $e \mid a$ and $e \mid b$, say $a = ea'$ and $b = eb'$.

Now since $d \in d\mathbb{Z}$ we have
$d \in a\mathbb{Z} + b\mathbb{Z}$.

$\implies \exists\, x, y \in \mathbb{Z}$ such that
$d = ax + by$.

But then

$$\begin{aligned} d &= ax + by \\ &= ea'x + eb'y \\ &= e(a'x + b'y) \implies e \mid d. \end{aligned}$$

Say $d = re$.

Finally we have

$$d \geq |d| = |r||e| \geq |e|$$

since $|r| \geq 1$. //

Similarly, given $a, b \in \mathbb{Z}$ note that

$$a\mathbb{Z} \cap b\mathbb{Z}$$

is a subgroup of $(\mathbb{Z}, +, 0)$ and hence $\exists\, m \geq 0$ such that

$$\boxed{a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}}$$

What is this m?

Claim: m is the least common multiple of a, b.

Proof: Certainly

$m \in m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} \subseteq a\mathbb{Z} \Rightarrow a \mid m$

and similarly, $b \mid m$.

Now consider any common multiple with $a \mid n$ and $b \mid n$.

Then $\left.\begin{array}{l} a \mid n \Rightarrow n \in a\mathbb{Z} \\ b \mid n \Rightarrow n \in b\mathbb{Z} \end{array}\right\} \Rightarrow n \in a\mathbb{Z} \cap b\mathbb{Z}$.

$\Rightarrow n \in m\mathbb{Z} \Rightarrow m \mid n$.

and it follows that $|m| \leq |n|$. ///

You may have noticed that we don't really distinguish between

$\pm n$.

Idea : Instead of thinking of elements n of $\mathbb{Z}$, we will think of ideals

$$(n) := n\mathbb{Z}$$

Then

gcd = addition of ideals
lcm = intersection of ideals.

What does it mean to say that $a, b \in \mathbb{Z}$ are coprime (or relatively prime) ?

It means that $\gcd(a,b) = 1$.
In other words

$$a\mathbb{Z} + b\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}$$

" a and b generate $\mathbb{Z}$ "

In this case $\exists\ x, y \in \mathbb{Z}$ such that

$$☆ \quad \boxed{1 = ax + by} \quad ☆$$

This is called "Bézout's Identity" and it is the most useful lemma in elementary number theory

Example: We say that $p \in \mathbb{Z}$ is prime if

$$d \mid p \Longrightarrow d = \pm 1 \text{ or } d = \pm p.$$

The fundamental property of prime numbers is called

"Euclid's Lemma":
Let $a, b, p \in \mathbb{Z}$ with p prime.

If $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof: Suppose that $p \mid ab$ (say $ab = pk$) and $p \nmid a$. We'll show that $p \mid b$.

Well, we have $\gcd(a,p) = 1$ or p and p is impossible ($p \nmid a$), hence $\gcd(a,p) = 1$.

Then Bézout says $\exists\, x, y \in \mathbb{Z}$ such that

$$1 = ax + py.$$

Multiply both sides by b to get

$$\begin{aligned} b &= abx + py \\ &= pkx + py \\ &= p(kx + y) \implies p \mid b. \end{aligned}$$

$\blacksquare$

Easy Peasy.

1/16/14

Current Topic:

Review of $\mathbb{Z}$ with a view toward ring theory.

Given $a, b \in \mathbb{Z}$ we have

$$\boxed{a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}}$$

where $d = \gcd(a,b)$, and

$$\boxed{a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}}$$

where $m = \operatorname{lcm}(a,b)$.

We say that a, b are <u>coprime</u> if $\gcd(a,b) = 1$, i.e., if and only if we have

$$a\mathbb{Z} + b\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}$$

(a and b <u>generate</u> $\mathbb{Z}$).

Note that this happens if and only if

$$1 \in a\mathbb{Z} + b\mathbb{Z}$$

i.e. $\exists\, x, y \in \mathbb{Z}$ such that

$$1 = ax + by$$

This is called Bézout's Identity and it is USEFUL.

Definitions:

We say that $u \in \mathbb{Z}$ is a "unit" if it has a multiplicative inverse. The units of $\mathbb{Z}$ are just ± 1.

Proof: Clearly ± 1 are units because $1 \cdot 1 = 1$ and $(-1)(-1) = 1$. Now let $n \neq \pm 1$, $n \neq 0$, and assume that there exists $x \in \mathbb{Z}$ such that

$$nx = 1.$$

We have $1 = nx + 0$ with $0 \leq 0 < |n|$, thus 0 is the remainder when we divide n by 1. But we also have

$$1 = 0 \cdot n + 1 \quad \text{with} \quad 0 \leq 1 < |n|.$$

Hence 1 is the remainder when 1 is divided by n. But the remainder is UNIQUE [Why?]

Contradiction. //

We write

$$\mathbb{Z}^{\times} = \{+1, -1\},$$

This is the (multiplicative) group of units.

Given nonzero, nonunit $p \in \mathbb{Z}$, we say that p is irreducible if

$$p = ab \implies a \text{ or } b \text{ is a unit}.$$

[Remark: You could also say "prime" but I'm choosing my words carefully.]

Examples: The irreducibles are

$$\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \text{ etc.}$$

Theorem: Every nonzero integer $n \neq 0$ can be written as a product of irreducibles, times a unit. (By convention the product of an empty set of numbers is 1)

Proof by Induction:

True for $n = \pm 1$ because

$$\pm 1 = \pm 1 \text{ (empty product)}.$$

So assume that $n \neq \pm 1$. If n is irreducible we're done, so assume that n is reducible, say

$$n = ab$$

where a, b are nonunits. Since $n \neq 0$ we know that $a, b \neq 0$. Since $b \neq \pm 1$ we have

$$1 < |b|.$$

$$|a| < |a||b| = |n|.$$

By induction on absolute value,

We know that a is a product of irreducibles times a unit

$$a = u_1 \, p_1 p_2 \cdots p_k .$$

Similarly, b is a product of irreducibles times a unit

$$b = u_2 \, q_1 q_2 \cdots q_k .$$

Finally,

$$\begin{aligned} n &= ab \\ &= u_1 p_1 \cdots p_k \, u_2 q_1 \cdots q_l \\ &= (u_1 u_2) \, p_1 p_2 \cdots p_k \, q_1 q_2 \cdots q_l \end{aligned}$$

is a product of irreducibles times a unit.

[Why is $u_1 u_2$ a unit ?]

Example

$$12$$

$$4 \cdot 3 \qquad 2 \cdot 6 \qquad (-3)(-4)$$

$$(-2)(-2) \cdot 3 \qquad 2 \cdot 3 \cdot 2 \qquad (-3)(-1) \cdot 2 \cdot 2$$

DONE DONE DONE

The factorization seems to be unique except for reordering and units. How can we prove this?

Consider $a, b \in \mathbb{Z}$ such that

$$a \mid b \quad \text{and} \quad b \mid a.$$

What does this mean?

We have $a = kb$ and $b = la$, so

$$a = kb = kla.$$
$$a - kla = 0$$
$$(1 - kl)a = 0.$$

Since $a \neq 0$ this implies [Why?] that

$$1 - kl = 0$$
$$1 = kl.$$

In other words, k and l are units and we have either

$$k = l = 1 \quad \text{or} \quad k = l = -1$$
$$(a = b) \qquad\qquad (a = -b)$$

Jargon: If $a, b \in \mathbb{Z}$ differ by a unit (i.e. $a = \pm b$) we say they are <u>associates</u>.

We need one more ingredient to prove unique factorization.

☆ Euclid's Lemma: Let $p \in \mathbb{Z}$ be irreducible. Then for all $a, b \in \mathbb{Z}$ we have

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

Proof: Suppose that $p \mid ab$ (say $ab = pk$) and assume that $p \nmid a$. We will show that $p \mid b$.

Note that $\gcd(a,p) = 1$ or p (± 1 or $\pm p$) and p is impossible ($p \nmid a$). Hence a, p are coprime and by Bézout $\exists\, x, y \in \mathbb{Z}$ such that

$$1 = ax + py$$

Multiply by b to get

$$\begin{aligned} b &= abx + pby \\ &= pkx + pby \\ &= p(kx + by) \end{aligned}$$

Hence $p \mid b$. $\blacksquare$

[Jargon: We just proved that in a PID, every irreducible element is prime.]

Here it is.

☆ Fundamental Theorem of Arithmetic:

Every nonzero $n \in \mathbb{Z}$ can be written UNIQUELY as a product of irreducibles times a unit.

Proof: We already showed existence.

If n is a unit we're done. So suppose that $|n| > 1$ and assume for contradiction that n has two DIFFERENT factorizations into irreducibles

$$(*) \quad u_1 a_1 a_2 \cdots a_k = u_2 b_1 b_2 \cdots b_\ell = n$$

Since $a_1 \mid b_1 b_2 \cdots b_\ell$, Euclid's Lemma says that $a_1 \mid b_i$ for some i. WLOG suppose that $a_1 \mid b_1$.

Since $a_1 \neq$ unit and b_1 is irred, this implies that

$$b_1 = u a_1 \quad \text{for unit } u.$$

Now cancel a_1 from both sides of (*) to get

$$u_1 a_1 a_2 \cdots a_k = (u_2 u) b_2 b_3 \cdots b_\ell = n'.$$

Clearly these two factorizations of n' are still DIFFERENT. But $|n'| < |n|$ so we can assume by induction that n' has a UNIQUE factorization.

Contradiction. $\blacksquare$

So What?
Good Question.

1/21/14

HW 1 due Thur Feb 4
NO CLASS THIS THURS.

Last time we proved that $\mathbb{Z}$ has the property of unique factorization.
More precisely we proved

☆ Fundamental Theorem of Arithmetic:

Every nonzero $n \in \mathbb{Z}$ can be written as a product of irreducibles times a unit. This factorization is unique up to reordering factors and multiplying by units.

Example:

$$\begin{aligned} 12 &= 2 \cdot 2 \cdot 3 \\ &= 2 \cdot 2 \cdot 3 \cdot 1 \\ &= 2 \cdot 2 \cdot 3 \cdot 1 \cdot 1 \\ &= (-2) \cdot 2 \cdot (-3) \\ &= 3(-1)(-1)\, 2 \cdot 2 \end{aligned}$$

etc.

"THE" prime factors of 12 are 2, 2, 3.

Recall the ingredients of the proof:

- Every additive subgroup of $\mathbb{Z}$ is equal to $a\mathbb{Z}$ for some $a \in \mathbb{Z}$ (Proof: Division Algorithm).

- Every $a, b \in \mathbb{Z}$ have a greatest common divisor $d \in \mathbb{Z}$ (i.e. such that $d|a$ and $d|b$ and $\forall e \in \mathbb{Z}$ we have

$$e|a \text{ \& } e|b \Rightarrow e|d.)$$

Moreover this gcd is unique up to multiplication by a unit.

- We say $a, b \in \mathbb{Z}$ are coprime if $\gcd(a,b) = 1$ (or any unit). This happens if and only if

$$\exists\, x, y \in \mathbb{Z} \text{ such that } 1 = ax + by.$$

(Bézout's Identity)

- We say nonzero, nonunit $p \in \mathbb{Z}$ is irreducible if

$$p = ab \Rightarrow a \text{ or } b \text{ is a unit.}$$

<u>Euclid's Lemma says</u>: If $p \in \mathbb{Z}$ is <u>irreducible</u> then p is <u>prime</u>, i.e.

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.$$

- Every $0 \neq n \in \mathbb{Z}$ has a factorization into irreducibles (times a unit) by Well-Ordering. Then Euclid's Lemma (irred $\Rightarrow$ prime) implies that the factorization is unique.

Who Cares?

Good Question.

All of MTH 562 will be an attempt to answer this question.

Right now I'll give 3 tentative answers.

<u>1</u>. Unique factorization is the most powerful tool in number theory.

Example: The biggest unsolved problem in number theory prior to 1994 was

Conjecture (Fermat's Last "Theorem", 1637):

Given $n \in \mathbb{Z}$, $n \geq 3$, the following equation has NO SOLUTION $x, y, z \in \mathbb{Z}$:

$$x^n + y^n = z^n.$$

Gabriel Lamé gave a "proof" in 1847, but he made a mistake.

Let $\omega_n := e^{2\pi i/n}$ and define the ring of cyclotomic integers

$$\mathbb{Z}[\omega_n] := \{a_0 + a_1\omega_n + a_2\omega_2^2 + \cdots + a_{n-1}\omega_n^{n-1} : a_i \in \mathbb{Z}\}.$$

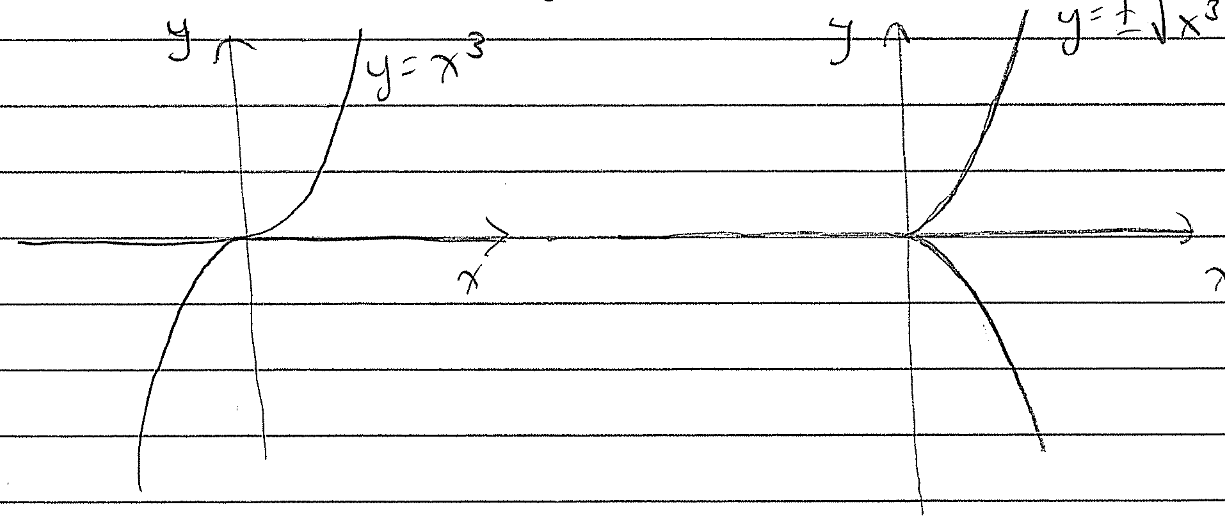
Lamé assumed that $\mathbb{Z}[\omega_n]$ has unique factorization and used this to prove FLT.

But Ernst Kummer had shown in 1844 that $\mathbb{Z}[\omega_{23}]$ does NOT have unique factorization!

FLT was finally proved in 1994-95.

2. Unique factorization is related to "smoothness" in geometry.

Example: Draw the curve $y^2 = x^3$ in the real x,y-plane.



This curve has a singlatrity (a "cusp") at $(x,y) = (0,0)$. We can detect this algebraically as follows.

We can think of every polynomial $f(x,y) \in \mathbb{R}[x,y]$ as a function on the curve

$$f : \text{curve} \longrightarrow \mathbb{R}$$
$$(x,y) \longmapsto f(x,y).$$

However, two different polynomials $f, g \in \mathbb{R}[x,y]$ will define the <u>same</u> function if

$$f(x,y) = g(x,y) + q(x,y)(y^2 - x^3).$$

Because for $a, b \in \mathbb{R}^2$ on the curve (i.e. $b^2 = a^3$) we have

$$f(a,b) = g(a,b) + \cancel{q(a,b)} \cdot 0$$

Formally, the ring of functions : curve $\to \mathbb{R}$ is a quotient ring

$$\mathbb{R}[x,y] / (y^2 - x^3).$$

The fact that this ring does NOT have unique factorization

$$y^2 = x^3 \quad \text{with } y, x \text{ irreducible}$$

implies that the curve has a <u>singularity</u>.

The relationship between smoothness and UFD generalizes.

3. The attempt to recover unique factorization (by Kummer and Dedekind) led to the central definition of ring theory: that of <u>ideal</u>. //

It is time to BEGIN.

<u>Definition</u>: A <u>ring</u> is a structure $(R, +, \times, 0, 1)$ such that

- $(R, +, 0)$ is an abelian group.
  i.e. — $a+b = b+a \quad \forall a, b \in R$.
  — $a+(b+c) = (a+b)+c \quad \forall a, b, c \in R$
  — $\exists 0 \in R, \ a+0 = a \quad \forall a \in R$.
  — $\forall a \in R, \ \exists b \in R, \ a+b = 0$.

- $(R, \times, 1)$ is an abelian semigroup
  i.e — $ab = ba \quad \forall a, b \in R$
  — $a(bc) = (ab)c \quad \forall a, b, c \in R$
  — $\exists 1 \in R, \ a1 = a \quad \forall a \in R$.

- $\times$ distributes over $+$.

i.e. $a(b+c) = ab + ac \quad \forall a, b, c \in R$ //

[☆ WARNING: In 562 we assume all rings are commutative ($ab = ba$). The prototypical noncommutative ring is

$$M_n(R) = \{ n \times n \text{ matrices over a comm. ring } R \}.$$]

We say $u \in R$ is a <u>unit</u> if

$$\exists \, v \in R \text{ such that } uv = 1$$

and in this case we write $v = u^{-1}$. Let

$$R^\times := \{ u \in R : u \text{ is a unit} \}.$$

Note that $(R^\times, \times, 1)$ is a group, called the <u>group of units</u> of R.

We say that R is a <u>field</u> if

$$R^\times = R - \{0\}.$$

(all nonzero elements have an inverse)

///

Examples:

(i) $\mathbb{Z} = \{ \cdots -2, -1, 0, 1, 2, \cdots \}$

(ii) Given $n \in \mathbb{Z}$ we have the ring of integers mod n:

$$\mathbb{Z}/n\mathbb{Z} := \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1} \}.$$

where $\bar{a} = a + n\mathbb{Z}$
$= \{ \cdots, a-2n, a-n, a, a+n, a+2n, \ldots \}$.

and we define

$$\left.\begin{array}{l} \bar{a}\,\bar{b} := \overline{ab} \\ \bar{a} + \bar{b} := \overline{a+b} \end{array}\right\} \text{“modular arithmetic”}$$

(iii) $C^0[0,1] := \{ f : [0,1] \to \mathbb{R},\ f \text{ continuous} \}$.

Given $f, g \in C^0[0,1]$ define $f+g$, fg by

$$\left.\begin{array}{l} (f+g)(x) = f(x) + g(x) \\ (fg)(x) = f(x)g(x) \end{array}\right. \quad \forall x \in [0,1]$$

"pointwise + and ×"

(iv) Let R be a ring, x be an abstract symbol (variable). A polynomial over R is an abstract expression

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

in which all but finitely many coefficients $a_i \in R$ equal 0. Let

$$R[x] := \{ f(x) \text{ polynomial over } R \}$$

with addition and multiplication

$$\sum_k a_k x^k + \sum_k b_k x^k := \sum_k (a_k + b_k) x^k$$

$$\left(\sum_k a_k x^k\right)\left(\sum_l b_l x^l\right) := \sum_m \left(\sum_{k+l=m} a_k b_l\right) x^m$$

Given $f(x) = \sum_k a_k x^k \in R[x]$, let

$$\deg(f) := \max \{ n : a_n \neq 0 \}.$$

Q: $\deg(fg) = \deg(f) + \deg(g)$?

(v) A formal power series over R is

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

in which ∞ many a_i may be nonzero. Let

$$R[[x]] := \{ f(x) \text{ formal power series over } R \}$$

with same $+$ and $\times$ as in $R[x]$.

Note that

$$R[x] \subseteq R[[x]]$$

is a subring.

1/28/14.

HW 1 due Tues Feb 4.
Office Hours: Mon 2-3, Wed 3-4.

Last time I defined "rings". They are intended to generalize

$$\mathbb{Z} \quad \text{and} \quad K[x].$$

Def: A ring is a structure $(R, +, \times, 0, 1)$ such that

- $(R, +, 0)$ is an abelian group
- $(R, \times, 1)$ is an abelian semigroup.
- $a(b+c) = ab + ac \quad \forall a, b, c \in R$. //

Subtraction is not part of the definition, but we can construct it as follows:

By definition we have

$$\forall a \in R, \exists a' \in R \text{ such that } a + a' = 0.$$

Claim: This a' is unique.

Proof: Suppose $\exists\, a', a'' \in R$ such that

$$a + a' = 0 = a + a''.$$

Then we have

$$\begin{aligned} a' &= a' + 0 \\ &= a' + (a + a'') \\ &= (a' + a) + a'' \\ &= 0 + a'' \\ &= a'' \end{aligned}$$

///

Definition: We will call this unique inverse "$-a$". Then we define subtraction

$$a - b := a + (-b).$$

HW 1.3 asks you to prove some basic properties such as

$$a(b - c) = ab - ac$$

etc.

Examples of rings:

(i) Fields $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

(ii) Integers $\mathbb{Z}$

(iii) Polynomials $R[x]$.

Given a ring we define the set

$$R[x] := \left\{ \sum_{k \geq 0}^{\infty} a_k x^k \; ; \; a_k \in R \text{ and } a_k = 0 \text{ for all but finitely many } k \right\}.$$

with addition and multiplication

$$\sum_k a_k x^k + \sum_k b_k x^k := \sum_k (a_k + b_k) x^k$$

$$\left(\sum_k a_k x^k\right)\left(\sum_l b_l x^l\right) := \sum_m \left(\sum_{k+l=m} a_k b_l\right) x^m$$

(iv) "Formal" power series $R[[x]]$
(∞ many coeffs may be nonzero)

Note: $R \subseteq R[x] \subseteq R[[x]]$

(v) Very important example $\mathbb{Z}/n\mathbb{Z}$.

Recall that the subgroups of $(\mathbb{Z}, +, 0)$ are just

$$n\mathbb{Z} \quad \text{for any } n \in \mathbb{Z}.$$

Since $\mathbb{Z}$ is abelian, every subgroup is normal and we can form the quotient group $\mathbb{Z}/n\mathbb{Z}$

Recall: We define a relation on $\mathbb{Z}$ by

$$a \sim_n b \iff a - b \in n\mathbb{Z}$$
$$(\exists k \in \mathbb{Z} \text{ with } a - b = nk).$$

This is an equivalence because.

- $a \sim_n a \quad \forall a \in \mathbb{Z}$
- $a \sim_n b \Rightarrow b \sim_n a \quad \forall a, b \in \mathbb{Z}$
- $a \sim_n b \ \& \ b \sim_n c \Rightarrow a \sim_n c \quad \forall a, b, c \in \mathbb{Z}$.

Check!

Thus $\mathbb{Z}$ is partitioned into equivalence classes of the form

$$a + n\mathbb{Z} := \{a + nk : k \in \mathbb{Z}\}.$$

"the coset of $n\mathbb{Z}$ generated by a".

Note that

$$a \sim_n b \iff a + n\mathbb{Z} = b + n\mathbb{Z}.$$

Proof: Suppose $a + n\mathbb{Z} = b + n\mathbb{Z}$. Since $a \in a + n\mathbb{Z}$ we have $a \in b + \mathbb{Z}$, i.e. $\exists\, k \in \mathbb{Z}$ such that $a = b + nk$. Hence $a \sim_n b$.

Conversely, suppose $a \sim_n b$ (say $a = b + nk$ for some $k \in \mathbb{Z}$). Then we have

$$a + n\mathbb{Z} \subseteq b + n\mathbb{Z}$$

because
$$\begin{aligned} a + n\ell &= (b + nk) + n\ell \\ &= b + n(k+\ell) \in b + n\mathbb{Z} \end{aligned}$$

and $b + n\mathbb{Z} \subseteq a + n\mathbb{Z}$ because

$$b + nl = (a - nk) + nl$$
$$= a + n(l-k) \in a + n\mathbb{Z}.$$

Hence $a + n\mathbb{Z} = b + n\mathbb{Z}$. ///

Let $\mathbb{Z}/n\mathbb{Z}$:= the set of cosets.
We define addition of cosets by

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) := (a+b) + n\mathbb{Z}.$$

Does that make any sense? We must be careful. Suppose we have

$$a + n\mathbb{Z} = a' + n\mathbb{Z} \quad \& \quad b + n\mathbb{Z} = b' + n\mathbb{Z}.$$

Does it follow that

$$(a+b) + n\mathbb{Z} = (a'+b') + n\mathbb{Z} \quad ?$$

Check: By assumption we have

$$a = a' + nk \quad \& \quad b = b' + nl$$

for some $k, l \in \mathbb{Z}$. It follows that

$$a+b = (a'+nk)+(b'+nl)$$
$$= (a'+b') + n(k+l).$$

$$\Longrightarrow \quad (a+b)-(a'+b') = n(k+l) \in n\mathbb{Z}.$$

$$\Longrightarrow \quad (a+b)+n\mathbb{Z} = (a'+b')+n\mathbb{Z} \quad \checkmark.$$

Thus addition of cosets is well-defined.

It is now easy to show that $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group with identity element

$$0+n\mathbb{Z} = n\mathbb{Z}.$$

But $\mathbb{Z}$ is a ring. Is $\mathbb{Z}/n\mathbb{Z}$ also a ring?

We need to define multiplication of cosets.
HOW?

There seems to be an obvious choice:

$$(a+n\mathbb{Z})(b+n\mathbb{Z}) := (ab)+n\mathbb{Z}.$$

Worry: Is this well-defined?

Check: suppose $a + n\mathbb{Z} = a' + n\mathbb{Z}$ & $b + n\mathbb{Z} = b' + n\mathbb{Z}$, say $a = a' + nk$ and $b = b' + nl$. Then

$$\begin{aligned} ab &= (a'+nk)(b'+nl) \\ &= a'b' + a'nl + nkb' + nknl \\ &= a'b' + n(a'l + b'k + nkl). \end{aligned}$$

$\Rightarrow \quad ab - a'b' = n(\text{something}) \in n\mathbb{Z}$

$\Rightarrow \quad (ab) + n\mathbb{Z} = (a'b') + n\mathbb{Z}.$ ✓

Great! We have succeeded in constructing a ring

$(\mathbb{Z}/n\mathbb{Z}, +, \times, 0, 1)$, where

$0_{\mathbb{Z}/n\mathbb{Z}} = 0 + n\mathbb{Z}$ & $1_{\mathbb{Z}/n\mathbb{Z}} = 1 + n\mathbb{Z}$.
$= n\mathbb{Z}$

For simplicity we will usually write

$\overline{a}$ instead of $a + n\mathbb{Z}$

even though this will confuse beginners. ☹

Thus, for example we have

$$\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

and we say things like.

$$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}.$$

$$\bar{5} \cdot \bar{5} = \overline{25} = \bar{1}$$

Q: What is the group of units

$$(\mathbb{Z}/6\mathbb{Z})^{\times} = ?$$

$\bar{2}$ has <u>no</u> inverse. If it did then we would have

$$\bar{2} \cdot \bar{3} = \bar{0} \Rightarrow \bar{2}^{-1} \cdot \bar{2} \cdot \bar{3} = \bar{2}^{-1} \cdot 0$$
$$\Rightarrow \bar{3} = \bar{0} \qquad \times.$$

Similarly, $\bar{3}$ has no inverse.

$\bar{4}$ has no inverse because

$$\bar{4} \cdot \bar{3} = \bar{2} \cdot \bar{2} \cdot \bar{3} = \bar{2} \cdot \bar{0} = \bar{0}.$$

Hence we have $(\mathbb{Z}/6\mathbb{Z})^{\times} = \{\bar{1}, \bar{5}\}$
with group table

$\times$	$\bar{1}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{1}$

Theorem: For general $n \geq 2$ we have

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\bar{a} : \gcd(a,n) = 1\}$$

Do you know how to prove this?

"$\exists\, \bar{a}^{-1} \iff \gcd(a,n) = 1$."

Proof Sketch:

"$\Rightarrow$" Sp. $\gcd(a,n) \neq 1$ so we have $a = dk$ & $n = dl$ with $\bar{l} \neq \bar{0}$.

If $\bar{a}^{-1}$ exists then

$$\bar{a} = \bar{d}\,\bar{k}$$
$$\bar{a}^{-1}\bar{a} = \bar{a}^{-1}\bar{d}\,\bar{k}$$
$$\bar{1} = \bar{d}(\bar{a}^{-1}\bar{k})$$
$$\Rightarrow \bar{d}^{-1} = \bar{a}^{-1}\bar{k} \quad \text{(exists)}.$$

But then

$$\bar{d}\,\bar{l} = \bar{n} = \bar{0}$$
$$\bar{d}^{-1}\bar{d}\,\bar{l} = \bar{d}^{-1}\bar{0}$$
$$\bar{l} = \bar{0}$$

Contradiction ///

"$\Leftarrow$" Sp. $\gcd(a,n) = 1$. Then Bézout says $\exists\, x, y \in \mathbb{Z}$ with

$$1 = ax + ny$$
$$\bar{1} = \bar{a}\,\bar{x} + \bar{n}\,\bar{y}$$
$$\bar{1} = \bar{a}\,\bar{x} + \cancel{\bar{0}\,\bar{y}}$$
$$\bar{1} = \bar{a}\,\bar{x}$$
$$\bar{a}^{-1} = \bar{x} \quad \text{(exists)}.$$

///

<u>Corollary</u>: We have.

$\mathbb{Z}/n\mathbb{Z}$ is a <u>field</u> $\Longleftrightarrow$ n is prime.

[We will see later $\exists$ unique field of size p^k for all prime p and positive integers k.]

1/30/14

HW 1 due next Tues.

Recall: Last time we constructed the quotient ring $\mathbb{Z}/n\mathbb{Z}$ and we showed that the group of units is

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1 \}.$$

Example:

$$(\mathbb{Z}/12\mathbb{Z})^\times = \{ \bar{1}, \bar{5}, \bar{7}, \bar{11} \}.$$

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

What group is this?

$\cancel{\mathbb{Z}/4\mathbb{Z}}$ OR $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Every element has order 2.

How could we predict the structure of the group $(\mathbb{Z}/n\mathbb{Z})^\times$?

Given two rings R, S we define the <u>direct product</u>

$$R \times S := \{(r,s) : r \in R,\ s \in S\}.$$

This is a ring with componentwise $+$ and $\times$. Note that

$$0_{R\times S} = (0_R, 0_S), \quad 1_{R\times S} = (1_R, 1_S).$$

Now we can state the

☆ Chinese Remainder Theorem (Sun Tzu, 3rd-5th c.)

Given $m, n \in \mathbb{Z}$ with $\gcd(m,n) = 1$ we have

$$\mathbb{Z}/mn\mathbb{Z} \underset{\substack{\uparrow \\ \text{ring isomorphism.}}}{\approx} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

<u>Proof</u>: For all $a, b \in \mathbb{Z}$ we will write

$$[a]_b := a + b\mathbb{Z}.$$

We need to define a bijection

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

that preserves the ring structure. I claim that

$$\varphi([a]_{mn}) := ([a]_m, [a]_n)$$

is such a function.

1. Well-Defined? If $[a]_{mn} = [b]_{mn}$ then we have $a-b \in mn\mathbb{Z}$. But since $mn\mathbb{Z} \subseteq m\mathbb{Z}$ and $mn\mathbb{Z} \subseteq n\mathbb{Z}$ this implies $a-b \in m\mathbb{Z}$ and $a-b \in n\mathbb{Z}$. Hence $[a]_m = [b]_m$ and $[a]_n = [b]_n$, i.e.

$$([a]_m, [a]_n) = ([b]_m, [b]_n). \quad ///$$

2. Preserve ring structure? Given $a, b \in \mathbb{Z}$ we have

$$\begin{aligned}
\varphi([a]_{mn} + [b]_{mn}) &= \varphi([a+b]_{mn}) \\
&= ([a+b]_m, [a+b]_n) \\
&= ([a]_m + [b]_m, [a]_n + [b]_n) \\
&= ([a]_m, [a]_n) + ([b]_m, [b]_n) \\
&= \varphi([a]_{mn}) + \varphi([b]_{mn}).
\end{aligned}$$

The proof for X is similar. ///

3. Injective? Suppose that $\varphi([a]_{mn}) = \varphi([b]_{mn})$ i.e. $([a]_m, [a]_n) = ([b]_m, [b]_n)$. Then we have $[a]_m = [b]_m$, i.e. $m \mid (a-b)$, and $[a]_n = [b]_n$, i.e. $n \mid (a-b)$.
Since m, n are coprime we have

$$m \mid (a-b) \ \& \ n \mid (a-b) \implies mn \mid (a-b).$$

[Do you know how to prove this?]

Hence $[a]_{mn} = [b]_{mn}$, as desired. ///

4. Surjective? This is the hardest part.

Since m, n are coprime, Bézout says $\exists\, x, y \in \mathbb{Z}$ such that

$$1 = mx + ny.$$

I claim that $\forall a, b \in \mathbb{Z}$ we have

$$\varphi([bmx + any]_{mn}) = ([a]_m, [b]_n)$$

and hence φ is surjective.

Indeed, note that

$$
\begin{aligned}
[bmx + any]_m &= [\cancel{bmx}]_m^{\,0} + [any]_m \\
&= [any]_m \\
&= [a(1 - mx)]_m \\
&= [a]_m - [\cancel{amx}]_m \\
&= [a]_m
\end{aligned}
$$

The proof that

$$[bmx + any]_n = [b]_n$$

is similar. $\blacksquare$

<u>Application</u>: If $\gcd(m,n) = 1$ then for all $a, b \in \mathbb{Z}$ the simultaneous congruences

$$
\begin{aligned}
x &\equiv a \pmod{m} \\
x &\equiv b \pmod{n}
\end{aligned}
$$

have a unique solution mod mn.

Example: Solve

$$x \equiv 2 \pmod 9$$
$$x \equiv 3 \pmod 7.$$

First solve $1 = 9r + 7s$.

r	s	$9r+7s$
1	0	9
0	1	7
1	-1	2
-3	4	1

$$\Longrightarrow \quad 1 = (-3)\cdot 9 + 4 \cdot 7$$

Therefore the solution is

$$\begin{aligned} x &\equiv 3(-3)\cdot 9 + 2\cdot 4\cdot 7 && \pmod{63} \\ &\equiv -81 + 56 && \pmod{63} \\ &\equiv -25 && \pmod{63} \\ &\equiv 38 && \pmod{63}. \end{aligned}$$

//

Corollary of CRT: Given $\gcd(m,n)=1$ we have

$$(\mathbb{Z}/mn\mathbb{Z})^\times \approx (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

$\uparrow$ group isomorphism.

Proof: Given rings R, S, it is a general fact that

$$(R\times S)^\times = R^\times \times S^\times.$$

[Prove it!] //

Example: Since $12 = 3\cdot 4$ with $\gcd(3,4)=1$ we have

$$(\mathbb{Z}/12\mathbb{Z})^\times \approx (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/4\mathbb{Z})^\times$$

$$\approx \{[1]_3, [2]_3\} \times \{[1]_4, [3]_4\}$$

$$\approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Notation: Let

$$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times$$

Euler's "totient" function.

Is there a formula for computing $\varphi(n)$?

If $\gcd(m,n)=1$ we have

$$\#(\mathbb{Z}/mn\mathbb{Z})^\times = \#(\mathbb{Z}/m\mathbb{Z})^\times \times \#(\mathbb{Z}/n\mathbb{Z})^\times$$
$$\varphi(mn) = \varphi(m)\varphi(n).$$

So if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ then

$$\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}).$$

So what is $\varphi(p^e)$ for p prime?

Among the numbers $\{1, 2, 3, \ldots, p^e\}$, the only numbers not coprime to p^e are the multiples of p:

$$\underbrace{p, 2p, 3p, \ldots, p^e (= p^{e-1}p)}$$

There are p^{e-1} such multiples. Hence

$$\varphi(p^e) = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right).$$

Theorem: We have.

$$\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

Proof: Suppose $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then we have

$$\varphi(n) = \varphi(p_1^{e_1})\, \varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k})$$

$$= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) p_2^{e_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{e_k}\left(1 - \frac{1}{p_k}\right)$$

$$= p_1^{e_1} \cdots p_k^{e_k} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

///

Who Cares? The NSA.

Recall Lagrange's Theorem:

If G is a group then $\forall g \in G$ we have

$$g^{\# G} = 1.$$

Corollary (Euler's Theorem, 1741):
For all $\gcd(a,n) = 1$ we have

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof: Since $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ we have

$$[a]_n^{\#(\mathbb{Z}/n\mathbb{Z})^\times} = [1]_n \quad //$$

Application: Compute the last two digits of 23^{202}.

We want $23^{202} \pmod{100}$. Note that

$$\begin{aligned}\varphi(100) &= 100\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{5}\right)\\ &= 100(1/2)(4/5)\\ &= 40.\end{aligned}$$

Hence $a^{40} \equiv 1 \pmod{100}$ $\forall \gcd(a,100) = 1$.
Since $\gcd(23, 100) = 1$ we get

$$\begin{aligned}23^{202} &\equiv 23^{5\cdot 40+2}\\ &\equiv (23^{40})^5\, 23^2\\ &\equiv 1\cdot 23^2\\ &\equiv 529\\ &\equiv 29 \pmod{100} \quad //\end{aligned}$$

Given two primes p, q then Euler's Theorem tells us that

$$a^{\varphi(pq)} \equiv 1 \pmod{pq}.$$

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

for all $\gcd(a, pq) = 1$. In fact, we have

$$a\,a^{(p-1)(q-1)} \equiv a \pmod{pq}$$

for <u>all</u> integers $a \in \mathbb{Z}$.

This result is the foundation of all modern cryptography

(the "RSA" cryptosystem).