Math 127, Wed Feb 17

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: 4.2–4.3.
- Reading for next Mon: 5.1 (to be written), 5.2–5.3.
- PS03 due tonight.
- Exam review tonight, 3–4pm, on Zoom (use office hour/problem session link).
- **Exam 1 on Wed Feb 24.**

Definition of ring

today's stuff: on Exam 2, not Exam 1

A **ring** is a set R and binary operations $+$ and $\cdot$ on R s.t.:

+

- ($+$ *associative*) For any $a, b, c \in R$, $(a + b) + c = a + (b + c)$.
- ($+$ *commutative*) For any $a, b \in R$, $a + b = b + a$.
- (*Zero*) There exists some $0 \in R$ such that for all $a \in R$, $0 + a = a = a + 0$.
- (*Negatives*) For every $a \in R$, there exists some $-a \in R$ such that $(-a) + a = 0 = a + (-a)$.

$\cdot$

- ($\cdot$ *associative*) For any $a, b, c \in R$, $(ab)c = a(bc)$.
- ($\cdot$ *commutative*) For any $a, b \in R$, $ab = ba$.
- (*One*) There exists some $1 \in R$ such that for all $a \in R$, $1a = a = a1$.
- (*Distributive*) For any $a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Examples: $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{C}$, $\mathbf{R}$, $R[x]$, $\mathbf{Z}/(m)$ (esp. $\mathbf{F}_p$, p prime).

Domains, inverses, units, fields

Definition

To say that a ring R is a **domain** (or sometimes, an **integral domain**) means that if $a, b \in R$ and $ab = 0$, then either $a = 0$ or $b = 0$.

being a domain = having the Zero Factor Property

Definition

Let R be a ring. For $a \in R$, an **inverse of** a is some $b \in R$ such that $ab = 1$. Since an element can have only one inverse, we use a^{-1} to denote *the* inverse of a. To say that a is a **unit** in R means that a has an inverse in R.

a^{-1} always multiplicative inverse
-a always additive inverse
Also recall: When R=Z, 2 is not a unit.

Definition

A **field** is a ring R in which every nonzero element is a unit and $1 \neq 0$. In other words, to say that a nonzero ring R is a field means that for every $a \neq 0$ in R, there exists some $b \in R$ such that $ab = 1$.

Some helpful facts we saw before, restated

$\deg 0 = -\infty$

Corollary

If R is a domain and $f(x), g(x) \in R[x]$, then

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)),$$

where $-\infty$ plus anything is $-\infty$.

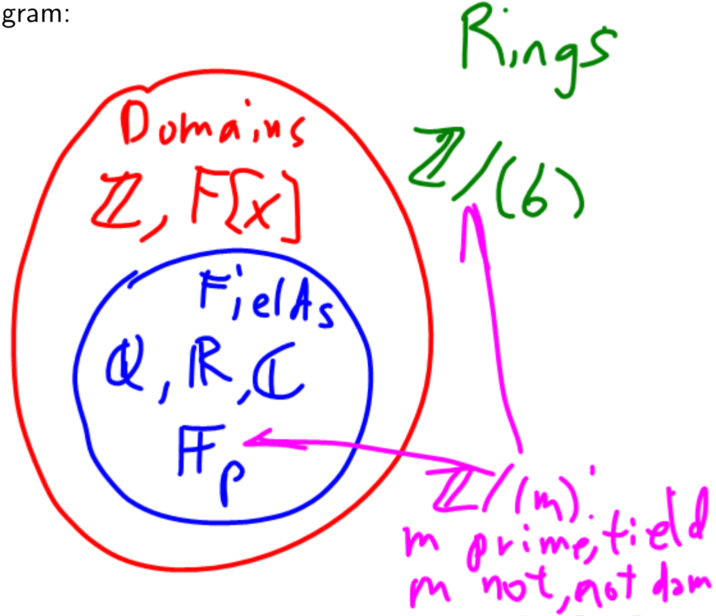
Theorem

If F is a field, then F is a domain.

See PS04 for a proof of field $\Rightarrow$ domain.

Not every ring is a domain; not every domain is a field

Examples/diagram:



Generalizing the Euclidean Algorithm

The abstract version of a body of knowledge is the most interesting special case(s), with unnecessary stuff stripped away.

First we work on stating the problem in a general setting.

Definition

Let R be a domain and $a, b, d \in R$. To say that d **divides** a means that $a = qd$ for some $q \in R$. To say that d is a **common divisor** of a and b means that d divides both a and b.

Definition

Let R be a domain and $a, b \in R$. To say that d is a **greatest common divisor** of a and b means that two things hold:

- d is a common divisor of a and b; and
- If e is a common divisor of a and b, then e divides d.

These two properties are the conclusion of the theorem "The Euclidean Algorithm works".

Note: Not obvious what "greatest" means for an unspecified ring

The thing that makes EA work: A size function

Definition

Let R be a domain. A **size function** on R is a function $\sigma : R \to \mathbf{Z} \cup \{-\infty\}$ such that for all nonzero $r \in R$, $\sigma(r) \geq 0$ and $\sigma(r) > \sigma(0)$.

Point: sigma defines the "size" of every element of R.

Definition

A **Euclidean domain** is a domain R with a size function σ that satisfies the following axiom: For $a, d \in R$, $d \neq 0$, there exist $q, r \in R$ such that

size(remainder) < size(divisor)

$$a = qd + r \qquad \text{with } \sigma(r) < \sigma(d).$$

In other words, a Euclidean domain is a domain where some version of the Division Theorem holds.

Examples of Euclidean domains

- The ring $R = \mathbf{Z}$ with the size function $\sigma(r) = |r|$ is a Euclidean domain (use signed division).
- Suppose F a field. The ring $F[x]$ with the size function $\sigma(f(x)) = \deg(f(x))$ is a Euclidean domain (use polynomial division).
- Just to have one new example: Define the **Gaussian integers**

$$\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}.$$

Then if

$$\sigma(a + bi) = (a + bi)(a - bi) = a^2 + b^2,$$

the Gaussian integers $\mathbf{Z}[i]$ are a Euclidean domain.

Not obvious! But it is true; can prove Division Theorem for Gaussian integers just like we prove Signed Division Theorem.

The Euclidean Algorithm

R is a Euclidean domain
Want to find gcd(a,b)
Let r_{-1} = a, r_0 = b

Almost exactly the same!

any c.d. divs d

$$
\begin{aligned}
r_{-1} &= q_1 r_0 + r_1 & (\sigma(r_1) < \sigma(r_0)) \\
r_0 &= q_2 r_1 + r_2 & (\sigma(r_2) < \sigma(r_1)) \\
r_1 &= q_3 r_2 + r_3 & (\sigma(r_3) < \sigma(r_2)) \\
&\vdots \\
r_{N-4} &= q_{N-2} r_{N-3} + r_{N-2} & (\sigma(r_{N-2}) < \sigma(r_{N-3})) \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} & (\sigma(r_{N-1}) < \sigma(r_{N-2})) \\
r_{N-2} &= q_N r_{N-1}
\end{aligned}
$$

$r_{N-1} = d$

d divs a & b

Size of remainders decreases by at least 1 each time, so alg terminates.

The Euclidean Algorithm works

Theorem

Let R be a Euclidean domain, and let a and b be nonzero elements of R.

- *The Euclidean Algorithm terminates after finitely many steps, and the result $r_{N-1} = gcd(a, b)$ is actually a greatest common divisor of a and b.*
- *(Bezout) There exist $x, y \in R$ such that*

$$ax + by = \gcd(a, b).$$

Proof: Pretty much the same!

Something new: Unique factorization

R domain

Definition

$a, b \in R$ are **associates**: $a = ub$ for some unit $u \in R$.

"Irreducible" generalizes idea of an integer being prime.
Ex. 7 irred in Z b/c 7 = (7)(1) = (-7)(-1) only factorizations of 7.

Definition

R be domain. $r \in R$ is **irreducible** means r is not a unit, and if $r = ab$ for $a, b \in R$, then one of a and b must be a unit.

Theorem (Unique factorization in Euclidean domains)

Let R be a Euclidean domain, and let a be a nonzero, non-unit element of R. Then a can be factored as a product of irreducible elements of R in essentially one way. That is, $a = p_1 \cdots p_k$ for some irreducible elements $p_i \in R$; and if

$$a = p_1 \cdots p_k = q_1 \cdots q_r$$

same # irrs.

with all p_i, q_j irreducible, then $k = r$, and we can rearrange the q_j so that for $1 \leq i \leq k$, we have that p_i is an associate of q_i.

Application: Turns out to be very useful (money-making) to be able to figure out irreducible polynomials in F_p[x].

Google "irreducible polynomials over GF(2)"

Unique factorization isn't obvious

The proof of that theorem comes later. For now, important to understand why factorization might not be unique (!?!?!).

Example: $R = \mathbf{Z}[\sqrt{-5}]$.

$$= \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

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

$$\begin{array}{ccc} & 6 & \\ \swarrow & & \searrow \\ 2 & & 3 \end{array} \qquad \begin{array}{ccc} & 6 & \\ \swarrow & & \searrow \\ (1+\sqrt{-5}) & & (1-\sqrt{-5}) \end{array}$$

So in R, you can get factor trees with different endings!