HW 3 due Wed Oct 26.
Problem 4 fixed typo
1 New problem.

Chapter 2 is done. So now what?

DEF: A ring is a tuple $(R, +, \times, 0, 1)$
where
- $(R, +, 0)$ is abelian group
- $(R, \times, 1)$ is semigroup
- $\forall a, b, c \in R$
  $a(b+c) = ab + ac$
  $(a+b)c = ac + bc$.

R is commutative if $ab = ba$ $\forall a, b \in R$.
$(R, \times, 1)$ abelian semigroup

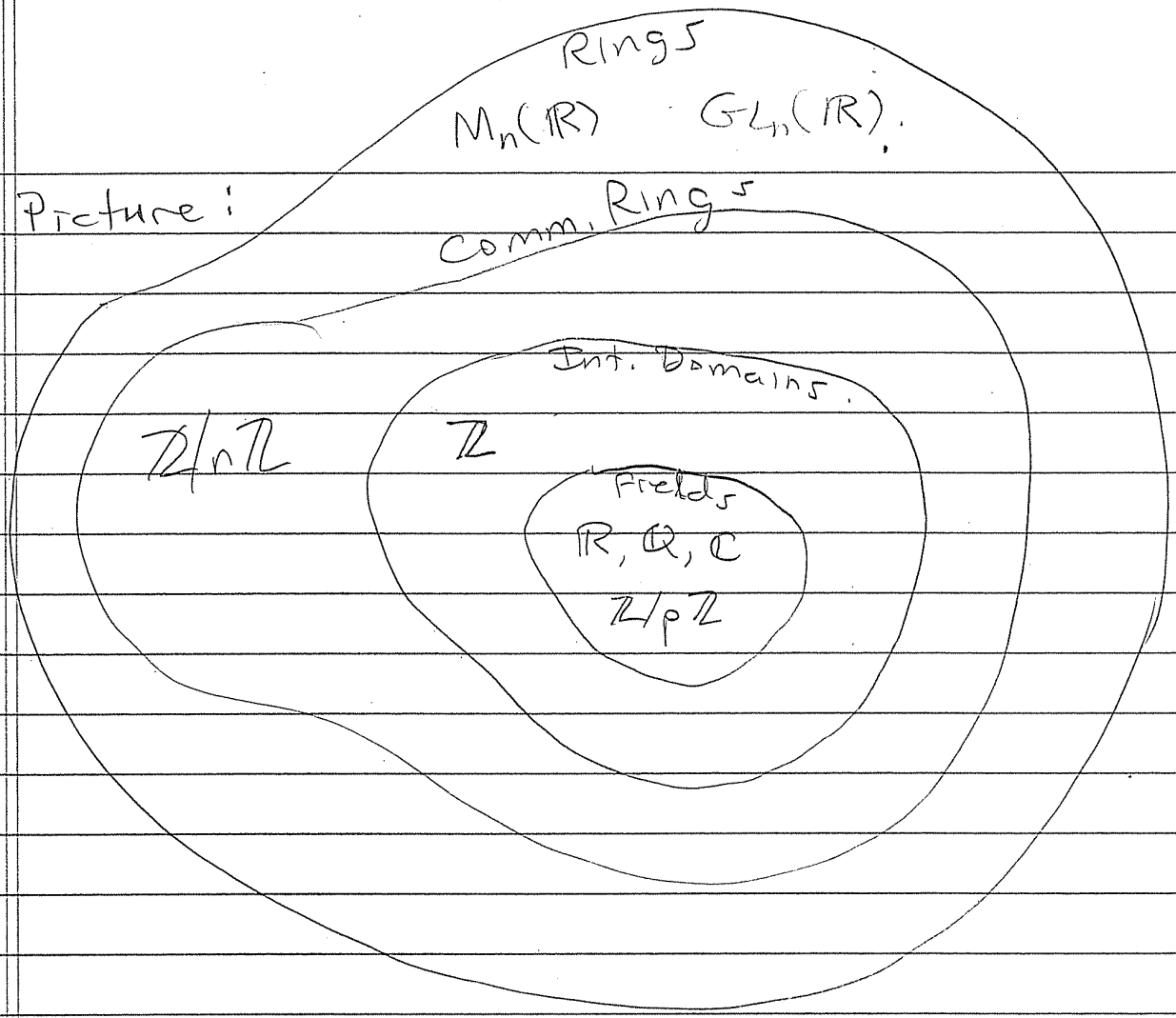
R is an integral domain if it is commutative, and...

$\forall a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$.
NO ZERO DIVISORS

R is a field if it is an integral domain and... $(R-0, \times, 1)$ is an (abelian) group.

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

Picture:



Remarks:

- $\mathbb{Z}/n\mathbb{Z}$ not int. domain since $3 \cdot 7 = 0 \bmod 21$ but $3, 7 \neq 0 \bmod 21$.
- $\mathbb{Z}$ is integral domain but, not so easy to prove ...

- Field $\Rightarrow \forall a, b$, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Proof: Suppose $ab = 0$. If $a \neq 0$ then a^{-1} exists. Multiply to get $b = a^{-1}0 = 0$. (HW 3.7).

- for $p \in \mathbb{Z}$ prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/p\mathbb{Z} : \gcd(a,p) = 1\}$$
$$= \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}.$$

Notation: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ($= GF(p)$)

"the field of order p"

~~Galois~~

Summary:

Definition: A field is a tuple $(\mathbb{F}, +, \times, 0, 1)$:

- $(F, +, 0)$ is abelian group.
- $(F - \{0\}, \times, 1)$ is abelian group
- $\forall a, b, c \in \mathbb{F}$, $a(b+c) = ab + ac$

Define: The "characteristic" of $\mathbb{F}$.

Consider $\langle 1 \rangle \leq (\mathbb{F}, +, 0)$. Then

$$\text{char}(\mathbb{F}) = \begin{cases} 0 & \text{if } |\langle 1 \rangle| = \infty \\ |\langle 1 \rangle| & \text{if } |\langle 1 \rangle| < \infty \end{cases}$$

eg $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$

$\text{char}(\mathbb{F}_p) = p$.

Lemma 3.2.10: Given field $\mathbb{F}$, we have $\text{char}(\mathbb{F}) = 0$ OR $\text{char}(\mathbb{F})$ is prime.

[No field of char. 6]

Proof: Consider $(\mathbb{F}, +, \times, 0, 1)$ and define notation $\overline{k} = 1 + 1 + \cdots + 1$, k times. Note: $k \mapsto \overline{k}$ is a ring hom. $\mathbb{Z} \to \mathbb{F}$ (check).
Now suppose $\text{char}(\mathbb{F}) = m \neq 0$.
i.e. $\overline{m} = 1 + 1 + \cdots + 1 = 0 = \overline{0}$.
Suppose $m \in \mathbb{Z}$ is NOT prime. i.e. $\exists\, r, s \in \mathbb{Z}$ $1 < r \leq s < m$ such that $m = rs$, hence then $\overline{r}\,\overline{s} = \overline{rs} = \overline{m} = 0$.
But $1 < r \leq s < m \implies \overline{r} \neq 0$ and $\overline{s} \neq 0$.
Contradiction. Hence m is prime ∎

Q: What good are fields?
A: A field has enough structure to do linear algebra. :)

eg. Solve for $x, y, z \in \mathbb{F}_3$.

$$\begin{cases} 2x + 2y + z = 1 & (1) \\ x + 2y = 2 & (2) \\ 2x + 2y + 2z = 0 & (3) \end{cases}$$

How?

Row Reduction: Note $\frac{1}{2} = 2 \in \mathbb{F}_3$.

$$\begin{array}{ll} ① \leftarrow \frac{1}{2}① & x + y + 2z = 2 \\ ② & x + 2y \quad = 2 \\ ③ \leftarrow \frac{1}{2}③ & x + y + z = 0 \end{array}$$

$$\begin{array}{ll} ① & x + y + 2z = 2 \\ ② \leftarrow ② - ① & y + z = 0 \\ ③ \leftarrow ③ - ① & 2z = 1 \end{array}$$

$$\begin{array}{ll} ① & x + y + 2z = 2 \\ ② & y + z = 0 \\ ③ \leftarrow \frac{1}{2}③ & z = 2 \end{array}$$

$$\begin{array}{ll} ① \leftarrow ① - 2③ & x + y = 1 \\ ② \leftarrow ② - ③ & y = 1 \\ ③ & z = 2 \end{array}$$

$$\begin{array}{ll} ① \leftarrow ① - ② & x = 0 \\ ② & y = 1 \\ ③ & z = 2. \end{array}$$

unique solution :) WHY?

$$\det\begin{pmatrix} 2 & 2 & 1 \\ 1 & 2 & 0 \\ 2 & 2 & 2 \end{pmatrix} = 2\det\begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} - 2\det\begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix} + 1\det\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

$$= 2(4-0) - 2(2-0) + 1(2-4)$$

$$= 2(4) - 2(2) + 1(-2)$$

$$8 - 4 - 2 = 2 \neq 0$$

Def: A vector space is a pair $(V, \mathbb{F})$ where $\mathbb{F}$

- $(V, +, \vec{0})$ is abelian group
- $(\mathbb{F}, 0, 1)$ is a field

AND $\mathbb{F}$ "acts on" V by scalar multiplication

$\cdot : \mathbb{F} \times V \to V$

$(a, \vec{v}) \mapsto a\vec{v}$ such that

- $1\vec{v} = \vec{v} \quad \forall\ \vec{v} \in V$
- $(ab)\vec{v} = a(b\vec{v}) \quad \forall\ a, b \in \mathbb{F},\ \vec{v} \in V.$
- $(a+b)\vec{v} = a\vec{v} + b\vec{v} \quad \forall\ a, b \in \mathbb{F},\ \vec{v} \in V$

($+$ in $\mathbb{F}$; $+$ in V)

THE Example: Given field $\mathbb{F}$ define vector space

$$\mathbb{F}^n = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} : a_1, a_2, \ldots, a_n \in \mathbb{F} \right\}$$

with $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}$

and $r \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ \vdots \\ ra_n \end{pmatrix}$

///

finite dimensional

FACT: All f.d. v.s. over $\mathbb{F}$ look like $\mathbb{F}^n$ for some n, but we won't prove it.

"vector space" is a rigid concept.

Note: $|\mathbb{F}_p^n| = p^n$
a finite vector space.

We can define finite matrix groups/rings.

ring $M_n(\mathbb{F}_p)$, size p^{n^2}.

group $GL_n(\mathbb{F}_p) := \{A \in M_n(\mathbb{F}_p) : \det A \neq 0\}$.

group $SL_n(\mathbb{F}_p) := \{A \in M_n(\mathbb{F}_p) : \det A = 1\}$.

Q: $|GL_n(\mathbb{F}_p)| = ?$

Claim: $|GL_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1})$.

$$= p^{n^2} \prod_{i=1}^{n} \left(1 - \frac{1}{p^i}\right)$$

Proof: Let $A = (\vec{a}_1, \vec{a}_2 \cdots \vec{a}_n) \in GL_n(\mathbb{F}_p)$.
So columns $\vec{a}_1, \cdots, \vec{a}_n$ are independent.
Choose $\vec{a}_1, \vec{a}_2, \cdots, \vec{a}_n$ in order....

$\vec{a}_1 \neq \vec{0} \Rightarrow p^n - 1$ ways to choose $\vec{a}_1$.

$\vec{a}_2 \notin \text{span}\{\vec{a}_1\} \approx \mathbb{F}_p^1 \leq \mathbb{F}_p^n$

$\Rightarrow p^n - p^1$ ways to choose $\vec{a}_2$.

$\mathbb{F}_p^n - \mathbb{F}_p^1$.

$\vec{a}_3 \notin \text{span}\{\vec{a}_1, \vec{a}_2\} \approx \mathbb{F}_p^2$

$\Rightarrow p^n - p^2$ ways to choose $\vec{a}_3$.

etc. ▨

Q: $|SL_n(\mathbb{F}_p)| = ?$

Note. $\det : GL_n(\mathbb{F}_p) \to \mathbb{F}_p^\times$ is hom.

with $\ker \varphi = SL_n(\mathbb{F}_p)$. Lagrange + 1st Iso. Thm.

$\Rightarrow |GL_n(\mathbb{F}_p)| / |SL_n(\mathbb{F}_p)| = |\mathbb{F}_p^\times| = p - 1$

$\Rightarrow |SL_n(\mathbb{F}_p)| = \frac{1}{p-1} |GL_n(\mathbb{F}_p)|$

///.

Let V, W be vector spaces (both / $\mathbb{F}$).

Define homomorphism of V.S.

$\varphi : V \to W$.

HW 3 due Wed.
Exam 2 Mon.

Wed: Review.
Today: Interlude (Linear Algebra).

Recall: a field is a tuple $(\mathbb{F}, +, \times, 0, 1)$
where
- $(\mathbb{F}, +, 0)$ abelian group
- $(\mathbb{F} - \{0\}, \times, 1)$ abelian group
- $\forall a, b, c \in \mathbb{F}$, $a(b+c) = ab + ac$.

Examples: $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ (p prime).

A vector space is an abelian group $(V, +, \vec{0})$ with a field $\mathbb{F}$ (of scalars) acting on it. i.e.
- $1\vec{v} = \vec{v}$ $\forall\ \vec{v} \in V$.
- $(ab)\vec{v} = a(b\vec{v})$ $\forall\ a, b \in \mathbb{F}$, $\vec{v} \in V$.
- $(a+b)\vec{v} = a\vec{v} + b\vec{v}$ $\forall\ a, b \in \mathbb{F}$, $\vec{v} \in V$
  ($a+b$ in $\mathbb{F}$; $a\vec{v} + b\vec{v}$ in V.)

what is this?

FACT: Given v.s. V over $\mathbb{F}$ with $\dim(V) = n < \infty$
we have

$$V \tilde{\to} \mathbb{F}^n$$

($\tilde{\to}$: as vector spaces; $\mathbb{F}^n$ = n-tuples with usual vector operations)

So $\mathbb{F}^n$ are the only finite dim vector spaces.

What does $\cong$ mean for V.S.?

DEF: Given v.s. U, V over $\mathbb{F}$ we say $\varphi: U \to V$ is a homomorphism if

- $\varphi(\vec{x}+\vec{y}) = \varphi(\vec{x}) + \varphi(\vec{y})$ group hom.
- $\varphi(a\vec{x}) = a\varphi(\vec{x})$ preserves $\mathbb{F}$-action

Term: V.S. hom. = "linear" map.
($\mathbb{F}$-linear)

Term: endomorphism = self-homomorphism
i.e. $\varphi: X \to X$.
(endo. + invertible = auto.).

Let $\mathrm{End}(V) := \{\text{endomorphs. } \varphi: V \to V\}$
(a RING!)

VITAL
Important Fact: ☆ n-dim. v.s. $V / \mathbb{F}$.

$\mathrm{End}(V) \cong \mathrm{Mat}_n(\mathbb{F})$.
($+$, $\circ$ composition) ↑ ring ($+$, $\times$ matrices).

Proof: Choose a basis $\beta = \{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\} \in V$.
Given linear $T: V \to V$ i.e. $T \in End(V)$.,
define a matrix

$$[T]_\beta := \left(T(\vec{e}_1)\ T(\vec{e}_2) \cdots T(\vec{e}_n)\right) \in Mat_n(\mathbb{F})$$

(column vectors)

FUN FIELDS: $\mathbb{F}_p$. $(= \mathbb{Z}/p\mathbb{Z})$. p prime.

FUN GROUPS: $GL_n(\mathbb{F}_p)$

Claim: $\exists$ Bijection

$$GL_n(\mathbb{F}_p) \longleftrightarrow \text{ordered bases for } \mathbb{F}_p^n$$

$$A = (\vec{a}_1\ \vec{a}_2 \cdots \vec{a}_n) \longmapsto \{\vec{a}_1, \ldots, \vec{a}_n\}.$$

(columns)

$\det A \neq 0 \iff$ columns form a basis. ///

Corollary:

$$|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p^2) \cdots (p^n - p^{n-1})$$

↓

Proof: choose $\vec{a}_1 \in \mathbb{F}_p^n - \{\vec{0}\}$ in $p^n - 1$ ways

choose $\vec{a}_2 \in \mathbb{F}_p^n - \text{span}\{\vec{a}_1\}$ in $p^n - p$ ways

choose $\vec{a}_3 \in \mathbb{F}_p^n - \text{span}\{\vec{a}_1, \vec{a}_2\}$ in $p^n - p^2$ ways.

etc

$\blacksquare$

eg. $|GL_2(\mathbb{F}_2)| = (2^2-1)(2^2-2)$

$= 3 \cdot 2 = 6$

$$GL_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

Q: How many (unordered) bases has $\mathbb{F}_p^n$?

A: $\#\text{bases} = \dfrac{\#\text{ordered bases}}{n!} = \dfrac{(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})}{n!}$

Q: Given n random vectors in $\mathbb{F}_p^n$

$P(\text{basis}) = ?$

A: $\text{Prob}(\text{basis}) = \dfrac{\#\text{bases}}{\#\text{n-sets}}$

$$\#\text{n-sets} \subseteq \mathbb{F}_p^n = \binom{|\mathbb{F}_p^n|}{n} = \binom{p^n}{n}$$

$$= \frac{(p^n-0)(p^n-1)\cdots(p^n-(n-1))}{n!}$$

$\blacksquare$

$$\Rightarrow \text{Prob(basis)} = \frac{(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})}{(p^n-0)(p^n-1)\cdots(p^n-(n-1))}.$$

But $$\frac{(p^n-p^i)}{(p^n-i)} = \frac{1-1/p^{n-i}}{1-i/p^n} \longrightarrow 1$$ as $p \to \infty$.

$$\Rightarrow \text{Prob(basis)} \longrightarrow 1 \quad \text{as } p \to \infty \qquad ///$$

DEF: Given v.s. V over $\mathbb{F}$, say $W \subseteq V$ is a subspace if W is a subgroup and closed under $\mathbb{F}$-scaling

i.e. $\alpha W \subseteq W \quad \forall\, \alpha \in \mathbb{F}$.
$\alpha \vec{w} \in W \quad \forall\, \alpha \in \mathbb{F}, \vec{w} \in W$.

Subspaces form a lattice $\mathcal{L}(V)$ with

$U \wedge W = U \cap W$ subspace intersection

$U \vee W =$ "$U + W$" subspace sum.
$= \text{span}\{U, W\}$

If $U \cap W = \{0\}$ we say $U + W = U \oplus W$ (direct sum)

compare $HK = H \times K$.

Given linear map $\varphi : U \to V$ there is a "1st Isomorphism Theorem"

$U/\ker\varphi \cong \operatorname{im}\varphi$ as spaces.

$U/\ker\varphi$: quotient space

Cor: $\dim(U/\ker\varphi) = \dim(\operatorname{im}\varphi)$.

$\dim(U) - \dim(\ker\varphi) = \dim(\operatorname{im}\varphi)$.

$\dim(U) = \dim(\ker\varphi) + \dim(\operatorname{im}\varphi)$.

Rank-Nullity Theorem!

Let $Gr(k, \mathbb{F}_p^n) = \{k\text{-dim subspaces of } \mathbb{F}_p^n\}$

Q: $|Gr(k, \mathbb{F}_p^n)| = ?$

We will count the set

$S = \{(W, B) : \text{subspace } W \subseteq V,\ \dim W = k,\ B \text{ ordered basis for } W\}$

in two ways.

Way 1: Choose $\mathcal{B}$ first. i.e. choose k ordered lin. ind. vectors.

$(p^n-1)(p^n-p)\cdots(p^n-p^{k-1})$ ways. ✓

Then W is determined by $W = \text{span}(\mathcal{B})$.

$\Rightarrow \boxed{|S| = (p^n-1)\cdots(p^n-p^{k-1})}$.

Way 2: Choose W first in $|Gr(k, \mathbb{F}_p^n)|$ ways.
Then choose basis $\mathcal{B}$ for W in

$(p^k-1)(p^k-p)\cdots(p^k-p^{k-1})$ ways.

$\Rightarrow \boxed{|S| = |Gr(k, \mathbb{F}_p^n)|\,(p^k-1)\cdots(p^k-p^{k-1})}$.

Finally.

$$|Gr(k, \mathbb{F}_p^n)| = \frac{(p^n-1)(p^n-p)\cdots(p^n-p^{k-1})}{(p^k-1)(p^k-p)\cdots(p^k-p^{k-1})}$$

$$= \prod_{i=0}^{k-1} \frac{p^n-p^i}{p^k-p^i} \qquad ///$$

Note:

$$\lim_{p\to 1} \frac{p^n-p^i}{p^k-p^i} = \frac{n-i}{k-i}$$

Proof: $\frac{0}{0}$ form $\rightsquigarrow$ use L'Hôpital.

$$\lim_{p\to 1} \frac{p^n - p^i}{p^k - p^i} \overset{p\neq 1}{=} \lim_{p\to 1} \frac{p^{n-i} - 1}{p^{k-i} - 1} = \lim_{p\to 1} \frac{(n-i)p^{n-i-1}}{(k-i)p^{k-i-1}}$$

divide by p^i ; diff

□

Cor As $p \to 1$

$$|Gr(k, \mathbb{F}_p^n)| \to \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1} = \binom{n}{k}$$

This motivates a notation

$$|Gr(k, \mathbb{F}_p^n)| = \begin{bmatrix} n \\ k \end{bmatrix}_p = p\text{-binomial coefficient}$$

or "Gaussian binomial coefficient"

Weird Idea:

a "set" = a "vector space" over $\mathbb{F}_1$ ← the field with 1 element.

?

But $\mathbb{F}_1$ doesn't exist (does it?)

$\mathbb{Z}/1\mathbb{Z} \cong \{0\}$ NOT a field