LECTURE 8 Oct. 1/2003

§ Finish-up from last time

$G \supset K \rhd H$ normal subgroup of G
(H normal in $G \Rightarrow H$ normal in K)

$G \xrightarrow{f} G/H$ = quotient group
(the cosets of H)

$a \longmapsto aH.$

1) H is normal in K; so have group $K/H \subset G/H$

K/H is a subgroup of G/H!

The cosets cK are stable under multiplication as K is stable under multiplication

2) Conversely, any subgroup of G containing H corresponds to a subgroup of G/H in this manner

$$K = \underbrace{\bigcup aH}_{\text{cosets corresp. to subgroup}} = \underbrace{f^{-1}\begin{pmatrix}\text{subgroup of}\\ G/H\end{pmatrix}}_{\text{in } G.}$$

Example: $G = \mathbb{Z}$ p a prime number
$H = p\mathbb{Z}$

Claim If $\mathbb{Z} \supset K \supset p\mathbb{Z}$ is a subgroup, then either $K = \mathbb{Z}$ or $K = p\mathbb{Z}$

Pf Such a K gives a subgroup of the cyclic quotient group $\mathbb{Z}/p\mathbb{Z}$. So gives either 0 or $\mathbb{Z}/p\mathbb{Z}$.

§ Vector spaces (over reals $\mathbb{R}$, complex #s $\mathbb{C}$)

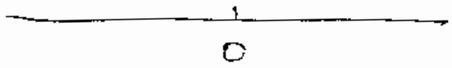
V over $\mathbb{R}$:

1) abelian group:
   operation $+$ $v+w$
   identity 0_V
   inverses $-v$
2) Scalar mult. by $c \in \mathbb{R}$
   $v \mapsto cv$

   s.t.
   - $1 \cdot v = v$
   - $(a \cdot b) \cdot v = a \cdot (b \cdot v)$
   - $a(v_1 + v_2) = a \cdot v_1 + a \cdot v_2$
   - $(a+b) \cdot v = a \cdot v + b \cdot v$.

Ex: ① $V = \{0\}$

② $V = \mathbb{R}$



③ $V = \mathbb{R}^n$ usual addition & scalar multiplication law

$\mathbb{R}^n$ has a richer structure:

$$v \cdot w = \sum a_i \cdot b_i$$
$$\|v\| = \sqrt{\sum a_i^2}$$

§ Vector spaces over a field F

Definition of a field

Set F with two operations + & ×

s.t.: ① Abelian group under +

+, 0 = ident. element,

$-a$ = inverse

② $F^{\times} := F - \{0\}$ forms an abelian group under ×

1 = identity

inverses: $a^{-1} = 1/a$

③ + & × distribute $a(b+c) = ab + ac$

$F' \subset F$ subfield if closed under $+, \times$, inverses, etc.

<u>Ex</u>: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

$\mathbb{Q}$ = rational numbers.

At the very least:
$F \supset \{0, 1\}$ (we always assume $0 \neq 1$)

The simplest field: $\mathbb{Z}/2\mathbb{Z}$

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

More generally, if p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$, with the multiplication inherited from $\mathbb{Z}$, <u>is a field</u>.

<u>Warning</u> $\mathbb{Z}/n\mathbb{Z}$ is not a field if n is composite

To show that $\mathbb{Z}/p\mathbb{Z}$ is a field, we must show that if $a \not\equiv 0 \pmod p$ then there is an integer b s.t.

$$ab \equiv 1 \pmod p$$

$$(b \equiv \text{"}a^{-1}\text{"} \pmod p)$$

<u>Pf</u>: Recall from 30 minutes ago that $p\mathbb{Z} \subset \mathbb{Z}$ is a maximal subgroup. If $a \not\equiv 0 \pmod p$, then $a \notin p\mathbb{Z}$. Hence

$p\mathbb{Z} + a\mathbb{Z} = \mathbb{Z}$ as this is a subgroup of $\mathbb{Z}$ containing $p\mathbb{Z}$.

So since $1 \in \mathbb{Z}$,

$$1 = mp + ba$$

$$1 \equiv ba \pmod p.$$

$\boxtimes$

Note:
$\mathbb{Z}/p\mathbb{Z}$ is not a subfield of $\mathbb{C}$!

$1 \in F \qquad \underbrace{1+\cdots+1}_{n \text{ times}} \in F \quad (n \geq 1)$

In $\mathbb{Z}/p\mathbb{Z}$: $\underbrace{1+\cdots+1}_{p \text{ times}} = 0$

In $\mathbb{Q}$: this is not so.

Question: What are the finite fields (beyond $\mathbb{Z}/p\mathbb{Z}$)? What is the order $|F|$?

Answer: For each prime p and $n \geq 1$, there is a unique field F of order p^n (up to isomorphism).

Def'n A vectorspace over a field F is a set V w/
① V is an abelian group under $+$ (ident: 0_V)
② There is a scalar product $F \times V \to V$, $(c,v) \mapsto c \cdot v$
- $1_F \cdot v = v$ • $(ab)v = a(bv)$
- $(a+b)v = av+bv$ • $a(v+w) = av+aw$.

Examples: of V/F

1. $\{0_V\}$
2. F
3. F^n
4. $F[X] :=$ {all polynomials $p(X)$ with coeffs in F}

$W \subset V$ vector subspace
subgroup under $+$ &
stable under scalar mult. by F

$$V = F^2$$
$$\cup$$
$$W = \{(a_1, a_2) : a_1 = c a_2, \ c \in F\}$$
is a subspace.

$T: V \longrightarrow W$ homomorphism (linear transformat.)

$$T(v + w) = Tv + Tw$$
$$T(c \cdot v) = c \cdot Tv$$

bijective hom = isomorphism

$\ker T = \{v : Tv = 0_W\}$ is a subspace of V

$\operatorname{Im} T = \{Tv : v \in V\}$ is a subspace of W

$W \subset V$ define V/W;

has vectorspace structure

$f : V \to V/W$ is a linear transformation with kernel W.