§ Finish-up from Last time

Let $G 	riangleright H$ ( $H$ is a normal subgroup of $G$ ) and $f$ be a homomorphism such that

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

$$a \mapsto aH.$$ 

Let $K$ be a subgroup of $G$, which can be written as $G 	riangleright K 	riangleright H$ ( $H$ is necessarily a normal subgroup of $K$ because if $H$ is normal in $G$ i.e. $aH = Ha$ for all $a \in G$ then we have $aH = Ha$ for all $a \in K \subseteq G$).

1) $H$ is normal in $K$, so we have a group $K/H \subset G/H$ so $K/H$ is a subgroup of $G/H$.

In other words, the cosets $\subset K$ are stable under multiplication as $K$ is a subgroup and stable under multiplication.

2) Conversely any subgroup of $G$ containing $H$ corresponds to a subgroup of $G/H$ in this manner. This is very powerful!
Example \( G = \mathbb{Z} \) (group under addition) and \( p \) is 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 \( K = p\mathbb{Z} \).

(We call this situation \( H = p\mathbb{Z} \) is a maximal subgroup of \( G \)).

Proof. Such \( K \) gives a subgroup of the cyclic quotient group \( \mathbb{Z} / p\mathbb{Z} \). Order of subgroup must be a divisor of \( p \). So gives either O (order 1) or \( \mathbb{Z} / p\mathbb{Z} \) (order \( p \)).

§ Vector spaces (over reals \( \mathbb{R} \) or complex numbers \( \mathbb{C} \))

\( V \) over \( \mathbb{R} \):

1) abelian group:

operation + \( v + w \)

identity \( O_v \)

inverse \( -v \)

2) Scalar multiplication by \( c \in \mathbb{R} : v \mapsto cv \)

such that \( 1 \cdot v = v \), \((a \cdot b) v = a(bv) \), \( a(v_1 + v_2) = av_1 + av_2 \), \((a+b)v = av + bv \)

Example:

1. \( V = \{0\} \) stupid one element vector space
2. \( V = \mathbb{R} \)
3. \( V = \mathbb{R}^n \) usual addition an scalar multiplication law

\( \mathbb{R}^n \) has a richer structure: for \( v = (v_1, v_2, \ldots, v_n) \) and \( w = (w_1, w_2, \ldots, w_n) \) we can

define \( v \cdot w = \sum_{i=1}^{n} v_i w_i \) inner product \( \|v\| = \sqrt{\sum_{i=1}^{n} v_i^2} \) norm
§ Vector spaces over a field \( F \)

Definition of a field

Set \( F \) with two operations \(+\) and \(\times\) such that

1. Abelian group under \(+\)
   
   \[ 0 = \text{identity element}, \]
   \[ -a = \text{inverse} \]

2. \( F^* = F \setminus \{0\} \) forms an abelian group under \(\times\)
   
   \[ 1 = \text{identity} \]
   \[ a^{-1} = 1/a = \text{inverse} \text{ (every non-zero elements have inverse, which is critical) } \]

3. \(+\) and \(\times\) distribute \( a \times (b + c) = a \times b + a \times c \)

\( \mathbb{Z} \) is not a field.

We call \( F' \subset F \) a subfield if it is closed under \(+\), \(\times\), inverses, etc.

Example: \( \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \) are fields and subfields (where \( \mathbb{Q} \) = rational numbers)

At the very least, 2 element field: \( F \supset \{0,1\} \) (we always assume \( 0 \neq 1 \))

The simplest field: \( \mathbb{Z}/2\mathbb{Z} \)

<table>
<thead>
<tr>
<th>(+)</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(\times)</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

More generally, if \( p \) is a prime number, then \( \mathbb{Z}/p\mathbb{Z} \) is a field, with the multiplication inherited from \( \mathbb{Z} \),

To show that \( \mathbb{Z}/p\mathbb{Z} \) is a field, we must show that if \( a \neq 0 \pmod{p} \),
then there is an integer \( b \) such that \( ab \equiv 1 \pmod{p} \). \( b = a^{-1} \pmod{p} \).

Proof: Recall, from 30 minutes ago, that \( p\mathbb{Z} \) is a maximal subgroup of \( \mathbb{Z} \). If \( a \neq 0 \pmod{p} \), then \( a \notin p\mathbb{Z} \). Hence \( p\mathbb{Z} + a\mathbb{Z} \) being a subgroup of \( \mathbb{Z} \)
containing \( p\mathbb{Z} \) implies \( p\mathbb{Z} + a\mathbb{Z} = \mathbb{Z} \). So since \( 1 \in \mathbb{Z} \), \( 1 \equiv mp + ba \pmod{p} \) or \( 1 \equiv ba \pmod{p} \). Euclidean algorithm could also give another proof. (Warning: \( \mathbb{Z}/n\mathbb{Z} \) is not a field if \( n \) is composite.)

Note
\( \mathbb{Z}/p\mathbb{Z} \) is not a subfield of \( \mathbb{C} \!\!\!\!\!/
\)

\( 1 \in F \), then \( 1 + \cdots + 1 \in F \) (\( n \geq 1 \))

In \( \mathbb{Z}/p\mathbb{Z} \): \( 1 + \cdots + 1 = 0 \), while in \( \mathbb{C} \) this is not so.

Galois questioned: What are the finite fields (beyond \( \mathbb{Z}/p\mathbb{Z} \))?

What is the order \(|F|\) ?

Galois proved: For each prime \( p \) and \( n \geq 1 \), there is a unique field \( F \) of order \( p^n \) (up to isomorphism). We'll see this later.

Definition A vector space over a field \( F \) is a set \( V \) with

1. \( V \) is an abelian group under + (identity \( 0_v \))

2. There is a scalar product \( F \times V \rightarrow V \), \( (c,v) \rightarrow cv \)

\( 1 \cdot v = v \quad (ab) \cdot v = a \cdot (b \cdot v) \), \( (a + b)v = av + bv \), \( a \cdot (r + w) = a \cdot r + a \cdot w \)

Examples of \( V/F \)

1. \( \{0_v\} \)
2. \( F \)
3. \( F^n \)
4. \( F[X] = \{ \text{all polynomials } p(X) \text{ with coefficients in } F \} \)
\( T:V \rightarrow W \) homomorphism (linear transformation)

\( T(v+w)=Tv + Tw \) group homomorphism

\( T(cv) = cT(v) \)

(bijective homomorphism = isomorphism)

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

\( \text{Im}T = \{ Tv : v \in V \} \) is a subspace of \( W \).

For \( W \subset V \) we can define the quotient \( V/W \) has a vector space structure.

\( f:V \rightarrow V/W \) is a linear transformation with kernel \( W \).