6.

Def: The index of a subgroup $H \leq G$ is $[G:H] = |G/H|$.

Prop: All cosets of H have the same size. 1

Consequently, $|G| = |H|\,[G:H]$. 2

Pf: $aH \to bH$, $g \mapsto ba^{-1}g$ } bijection

$ba^{-1}g' \leftarrow\!\shortmid\ g'$ 1 ✓

2: Both sides are ∞ unless $[G:H] = r < \infty$, in which case

$|G| = |a_1H| \dot\cup \cdots \dot\cup |a_rH| = r|H|$. □

Cor [Lagrange's Thm]: $H \leq G$ and G finite $\Rightarrow |H| \mid |G|$. now you've really seen some group theory

Cor: $a \in G \Rightarrow |a| \mid |G|$.

Pf: $|a| = |\langle a \rangle| \leq G$. □

Cor: $|G| = p$ prime $\Rightarrow G \cong C_p$ is cyclic of order p.

Pf: Pick $g \in G$ with $g \neq e$. Then $|g| = 1$ or p.

$g \neq e \Rightarrow |g| = p \Rightarrow G = \langle g \rangle$. □

Prop: $\varphi: G \to G'$ homomorphism $\Rightarrow$

$|G| = |\ker\varphi| \cdot |\operatorname{im}\varphi|$.

$\Rightarrow |\ker\varphi| \mid |G|$, $|\operatorname{im}\varphi| \mid |G|$, $|\operatorname{im}\varphi| \mid |G'|$

Pf: $|\operatorname{im}\varphi| \leftrightarrow |\{\text{nonempty fibers of } \varphi\}| = [G:H] = |G/H|$ for $H = \ker\varphi$. □

Modular arithmetic

Def: For $a, b, n \in \mathbb{Z}$, $a \equiv b \pmod n$ if $a - b \in n\mathbb{Z}$

"a is congruent to b modulo n"

$a + n\mathbb{Z} = b + n\mathbb{Z}$ G/H

$\bar a = \bar b$ in $\mathbb{Z}/n\mathbb{Z}$

Lemma: $[\mathbb{Z}:n\mathbb{Z}] = n = |\mathbb{Z}/n\mathbb{Z}|$

Pf: Division with remainder: $m = qn + r$ with $0 \leq r \leq n-1$.

Q. $\mathbb{Z}$ has $+, \times$; what about $\mathbb{Z}/n\mathbb{Z}$?

Prop: $a, b, n \in \mathbb{Z} \Rightarrow \overline{a+b} = \bar a + \bar b$

and $\bar a \bar b = \overline{ab}$ are well defined in $\mathbb{Z}/n\mathbb{Z}$.

□

E.g. $n = 2$ $\quad \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$
evens odds

familiar rules:

even + even = even	even · even = even
odd + odd = even	odd · odd = odd
even + odd = odd	even · odd = even

E.g. $n = 10$: last digit of $2179 + 836 = ?$ $\quad \bar{9} + \bar{6} = \overline{15} = \bar{5}$

$2179 \times 836 = ?$ $\quad \bar{9} \times \bar{6} = \overline{54} = \bar{4}$

E.g. "clock arithmetic"

E.g. weekdays: What day of the week will September 14, 2024 be?

Thu $\equiv 5 \pmod 7$ $\qquad 365 \equiv ?\ 1 \pmod 7$ $\qquad 7 \mid 350 \Rightarrow 15 \equiv 1 \pmod 7$

Thu + 365 $\equiv$ 5 + 1 $\equiv$ 6 $\equiv$ Fri Is that right? No! Why? Leap year!
(6) (2) (7) (Sat)

Pf: Need $\left.\begin{matrix} a - a' \in n\mathbb{Z} \\ b - b' \in n\mathbb{Z} \end{matrix}\right\} \Rightarrow \overline{a+b} = \overline{a'+b'}$. But $(a+b) - (a'+b') = (a-a') - (b-b') \in n\mathbb{Z}$. ✓

$\Downarrow$

$\overline{ab} = \overline{a'b'}$. But $ab - a'b' = ab - ab' + ab' - a'b'$

$= a(b-b') + (a-a')b' \in n\mathbb{Z}$. ✓ $\square$

($a \in n\mathbb{Z}$, $b \in n\mathbb{Z}$)

Note: $\mathbb{Z}$ has + associative commutative with inverses, × associative (commutative) distributive over + } ring

$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ring homomorphism

Ch 7

Q. $\mathbb{Z}/n\mathbb{Z}^* = ?$ When is $\bar{m}$ invertible? $\Leftrightarrow am \equiv 1 \pmod n$ for some $a \in \mathbb{Z}$

A.

$\Leftrightarrow am \in 1 + n\mathbb{Z}$ "

$\Leftrightarrow am = 1 - bn$ " and $b \in \mathbb{Z}$

$\Leftrightarrow am + bn = 1$ " "

$\Leftrightarrow \gcd(m, n) = 1$.

E.g. music theory = ? clock arithmetic!

$\mathbb{Z}/12\mathbb{Z} = \{C, C^\#, D, D^\#, \ldots, B^\flat, B\}$ $\quad \# = +1$, $\flat = -1$, so $A^\# = B^\flat$ on notes

octave $\equiv$ unison, octave + 3rd $\equiv$ 3rd : $\equiv$ means "sounds like"

circle of fifths: $\mathbb{Z}/12\mathbb{Z} = \langle 7 \rangle$ since $\gcd(7, 12) = 1$.

on key signatures: up one fifth = +7 = #, down one fifth = −7 = ♭ cf.

2♭ ♭ # 2#
…, $B^\flat$, F, C, G, D, …

$\square$