§2.9 Modular arithmetic

Q: What time of day will it be 50 hours from now?
What day of week 50 days from now?
Last digit of 7539×10746 ?

+	even	odd
even	?	?
odd	?	?

×	even	odd
even	?	?
odd	?	?

Recall $G = \mathbb{Z}^+$ has all subgroups $H < \mathbb{Z}^+$ of form $H = n\mathbb{Z}$
$= \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$
for some n.

The (left or right) cosets of $H = n\mathbb{Z}$ inside $G = \mathbb{Z}^+$
are of form $a + n\mathbb{Z} := \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\} =: \overline{a}$ need to know the modulus n!
which are equiv. classes for $a \equiv b \bmod n$ if $a-b$ divisible by n, or $a = b + nk$ with $k \in \mathbb{Z}$,
and there are only n of them: $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\} =: \mathbb{Z}/n\mathbb{Z}$ integers modulo n

$\overline{0} = n\mathbb{Z}$, $\overline{1} = 1 + n\mathbb{Z}$, $\overline{2} = 2 + n\mathbb{Z}$, $\overline{n-1} = n-1+n\mathbb{Z} = -1+n\mathbb{Z}$

EXAMPLE: $n=10$ $\quad 10\mathbb{Z} = \{\ldots, -20, -10, 0, 10, 20, \ldots\}$

$\overline{3} = 3 + 10\mathbb{Z} = \{\ldots, -17, -7, 3, 13, 23, \ldots\} = \overline{-7} = \overline{823}$

$\mathbb{Z}/10\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{9}\}$

PROPOSITION: One can add, multiply in $\mathbb{Z}/n\mathbb{Z}$ using any representatives:
(LEMMA 2.9.6)

if $a \equiv a' \bmod n$, $b \equiv b' \bmod n$ then $\overline{a \cdot b} := \overline{a' \cdot b'}$, $\overline{a+b} := \overline{a'+b'}$ make sense because
$a \cdot b \equiv a' \cdot b' \bmod n$
$a + b \equiv a' + b' \bmod n$

proof: If $a = a' + k_1 n$, $b = b' + k_2 n$ then $a+b = a'+b' + \overbrace{(k_1+k_2)}^{\in \mathbb{Z}} n$

$a \cdot b = (a' + k_1 n)(b' + k_2 n) = a'b' + k_1 n b' + k_2 n a' + k_1 k_2 n^2$
$= a'b' + \underbrace{(k_1 b' + k_2 a' + k_1 k_2 n)}_{\in \mathbb{Z}} n$ ∎

10/8/18 >
EXAMPLE: $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$
even, odd

EXAMPLE: $\{Su, M, Tu, W, Th, F, Sa\}$
$\leftrightarrow \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} = \mathbb{Z}/7\mathbb{Z}$

50 days from F is Sa since $\overline{50} + \bar{5} = \bar{1} + \bar{5} = \bar{6}$ in $\mathbb{Z}/7\mathbb{Z}$

Note that reduction modulo n
$$\mathbb{Z}^{+} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^{+}$$
$$a \longmapsto \bar{a}$$

gives a group homomorphism, having $n\mathbb{Z}$ as its kernel.

This generalizes to ...

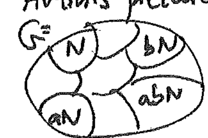
§ 2.12 Quotient groups

PROP-DEF'N: Whenever $N \triangleleft G$ is a normal subgroup, one can make the collection $G/N := \{\text{left cosets } aN : a \in G\}$ into a group, called the quotient group (of G by N), by doing the most naive thing: for cosets aN and bN,

define $aN \cdot bN := abN$

as the composition $G/N \times G/N \longrightarrow G/N$

Artin's picture:



works since
$aNbN = abNN = abN$

proof: What needs to be checked are

- well-definition: does it depend on choices, i.e. if $aN = a'N$, $bN = b'N$, will $abN = a'b'N$?

No, since $a = a'n_1$, $b = b'n_2$ for some $n_1, n_2 \in N$

one has $ab = a'n_1b'n_2 = a'b'n_3n_2 \Rightarrow abN = a'b'N$

since $Nb' = b'N$ as $N \triangleleft G$

- G/N has an identity: $1 \cdot N = N$ itself

$1N \cdot aN = aN \cdot 1N = aN$

- G/N has inverses: $(aN)^{-1} = a^{-1}N$ since $aN \cdot a^{-1}N = a \cdot a^{-1}N = 1N = N$

- G/N has associative multiplication: $\underbrace{(aN\, bN)\cdot cN}_{=abcN} = aN\,(bN\, cN)$

Starting with a normal subgroup $N \triangleleft G$,

one obtains the <u>canonical</u> <u>quotient</u> <u>homomorphism</u>

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ g & \longmapsto & gN \end{array}$$

(Why a <u>homomorphism</u>? $\pi(g_1 g_2) = g_1 g_2 N = g_1 N \cdot g_2 N = \pi(g_1)\pi(g_2)$)

π is surjective ($\operatorname{im}\pi = G/N$)

and $\ker(\pi) = N$ ($\pi(g) = 1_{G/N} = 1 \cdot N = N$ means $gN = N$ i.e. $g \in N$)

<u>Thus normal subgroups always arise as kernels of homomorphisms!</u>

EX<u>AMPLES</u>: ①

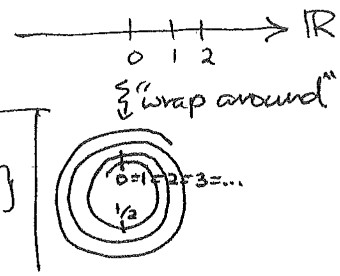
$$\overset{G}{\overset{\shortparallel}{\mathbb{Z}}} \xrightarrow{\pi} \overset{G}{\overset{\shortparallel}{\mathbb{Z}}} / \overset{N}{\overbrace{n\mathbb{Z}}} \quad \text{has } \ker(\pi) = n\mathbb{Z}$$

$$a \longmapsto \bar{a}$$

②

$$\overset{G}{\overset{\shortparallel}{\mathbb{R}^+}} \xrightarrow{\pi} \overset{G}{\overset{\shortparallel}{\mathbb{R}^+}} / \overset{N}{\overset{\shortparallel}{\mathbb{Z}^+}} \quad \text{has } \ker(\pi) = \mathbb{Z}$$

$$x \longmapsto x + \mathbb{Z}^+$$



③

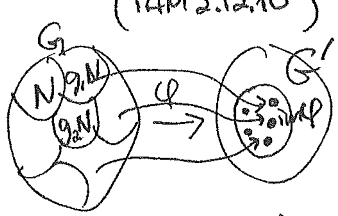
$$\overset{G}{\overset{\shortparallel}{S_n}} \to \overset{G}{\overset{\shortparallel}{S_n}} / \overset{N}{\overset{\shortparallel}{A_n}} \cong \mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\}$$

$$S_n/A_n = \{\underset{A_n}{\text{even perms}}, \underset{pA_n}{\text{odd perms}}\}$$

Sometimes identifying structure of G/N is trickier and this can help:

<u>Noether's 1st Isomorphism Thm:</u> Given a group homomorphism $G \xrightarrow{\varphi} G'$
(THM 2.12.10)
with kernel $\ker\varphi =: N \triangleleft G$, the map

$$\begin{array}{ccc} G/N & \xrightarrow{\bar{\varphi}} & \operatorname{im}\varphi \\ gN & \longmapsto & \varphi(g) \end{array}$$



is a (well-defined) (group) <u>isomorphism</u>.

<u>proof:</u> We've already seen $\varphi(g_1) = \varphi(g_2) \iff g_1 N = g_2 N$, so $\bar{\varphi}$ is a <u>bijection</u>,

and it's also a homomorphism: $\bar{\varphi}(g_1 N \cdot g_2 N) = \bar{\varphi}(g_1 g_2 N) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ ∎

EXAMPLE: Recall Klein-four $V_4 = \{e, (12)(34), (13)(24), (14)(23)\} < S_4$ which has index $[S_4 : V_4] = \frac{24}{4} = 6$.

Not hard to check $V_4 \trianglelefteq S_4$ directly, but let's show this and identify the quotient group S_4/V_4 as isomorphic to S_3 by exhibiting a (surjective) homomorphism $S_4 \xrightarrow{\varphi} S_3$ with $\ker\varphi = V_4$:

$$S_4 \xrightarrow{\varphi} S_3 = S_{\{A,B,C\}} \quad \text{where}$$

$$p \longmapsto \varphi(p) = \text{the permutation } \begin{pmatrix} A & B & C \\ p(A) & p(B) & p(C) \end{pmatrix}$$

$A := \{\{1,2\},\{3,4\}\}$ $\circlearrowleft (12)$, $(12)(34)$

$A \xleftrightarrow{(23)} B$

$B := \{\{1,3\},\{2,4\}\}$ $\circlearrowleft (12)(34)$

$B \xleftrightarrow{(12)} C$

$C := \{\{1,4\},\{2,3\}\}$ $\circlearrowleft (23)$, $(12)(34)$

$$e, (12)(34), (13)(24), (14)(23) \longmapsto \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} = e$$

$$(12) \longmapsto \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} = (BC)$$

$$(23) \longmapsto \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = (AB)$$

$$\vdots$$

having these two in $\operatorname{im}\varphi$ already shows $\operatorname{im}\varphi = S_3$, since $\langle (AB), (BC) \rangle = S_{\{A,B,C\}}$

Since $\ker\varphi = V_4$ and $\operatorname{im}\varphi = S_3$, $S_4/V_4 \cong S_3$, which was not obvious.

10/12/18 >

More modular arithmetic (not in Artin Ch. 2)

Recall $\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{(n-1)}\}$ where $\bar{a} := a + n\mathbb{Z}$ had both $+$ and $\times$ operations, so we get two (abelian) groups

- $(\mathbb{Z}/n\mathbb{Z})^+$, which is just a cyclic group of size n, since we have an isomorphism

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow G = \langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$$

$$\bar{a} \longmapsto g^a$$

$$\underset{=\overline{a+b}}{\bar{a} + \bar{b}} \longmapsto g^{a+b} = g^a \cdot g^b$$

- $(\mathbb{Z}/n\mathbb{Z})^\times := \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \bar{a} \text{ has a multiplicative inverse } \bar{b} \text{ with } \bar{a}\bar{b} = \bar{1}\}$

a little more interesting...