$\boxed{\text{E.g 1}}$ Let $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ Define $\oplus$ and $\otimes$ as

$i \oplus j = i + j \pmod n$ $\quad i \otimes j = i \times j \pmod n$

proposition: $(\mathbb{Z}_n, \oplus, \otimes)$ is a commu. ring

Moreover, if $n = p$ is a prime then $(\mathbb{Z}_p, \oplus, \otimes)$ is a field.

denoted by $\mathbb{F}_p$, $GF(p)$

(By Bezout Thm
$U(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\}$
and $\otimes$ is commu.)

$\boxed{\text{E.g. 2}}$

Let $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subsetneq \mathbb{R}$

claim $\mathbb{Q}(\sqrt{2})$ is a field

Actually "$\mathbb{Q}(\sqrt{2})$" is suitable, since it's the same as our textbook.
"$\mathbb{Q}[\sqrt{2}]$" is not.

$\boxed{\text{E.g. 3}}$ Let $\mathbb{Q}(\sqrt[3]{2}) = \{a + b2^{\frac{1}{3}} + c2^{\frac{2}{3}} \mid a, b, c \in \mathbb{Q}\}$

Claim $\mathbb{Q}(\sqrt[3]{2})$ is a field.

$\boxed{\text{E.g. 4}}$ Let $\mathbb{Q}(\pi) = \left\{ \dfrac{a_0 + a_1\pi + \dots + a_n\pi^n + \dots}{b_0 + b_1\pi + \dots + b_n\pi^n + \dots} \,\middle|\, a_i, b_j \in \mathbb{Q} \right\}$

Claim. $\mathbb{Q}(\pi)$ is a field

Eg 2-3.4 are extensions of $\mathbb{Q}$ 4 is transcendental extension

$\boxed{\text{E.g. 5}}$ Gauss Integer Ring

$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ where $i = \sqrt{-1}$

Claim. $\mathbb{Z}[i]$ is a ring.

$\boxed{\text{E.g. 6}}$ Let F be a field. and let $M_n(F) = \{$invertible matrices of degree n over $F\}$

G //

$(G, \times)$ is a group, called a general linear group over F

$GL_n(F)$

if $F = \mathbb{F}_p$ $\quad GL_n(\mathbb{F}_p) = GL_n(p)$

$(G, \times)$

Let a group.

$(H, \times)$

Def A subset $H \subset G$ is called a subgroup if is a group.

This def is very easy to induce a misunderstanding.

You must write $(G, \times)$, $(H, \times)$ here since it hints that they have the same multiplication.

If "Let G a group. a subset H ... H is a group"

Then it's WRONG!

denoted by $H \leqslant G$

$H \neq \emptyset$ is the precondition.

Lemma $H \subset G$ is a subgp $\Leftrightarrow$ $\forall x, y \in H$ we have

① $xy \in H$, $x^{-1} \in H$

② $xy^{-1} \in H$

not both. one of these is enough since ① $\Leftrightarrow$ ②

Moreover if $|G|$ then $xy \in H$ is enough

This is because $\forall x \in H$, $|x|$ is finite, you can always find $x^{-1} = x^{|x|-1} \in H$ ($xy \in H$ guarantee this)

problem: $|GL_n(p)| = ?$ $\quad |SL_n(p)| = ?$ $\quad$ HW!

$C = \left\{ \begin{bmatrix} a & & \\ & \ddots & \\ & & a \end{bmatrix} \middle| \ 0 \neq a \in F \right\} \subset GL_n(F)$

$(C, \times)$ is a subgp of $GL_n(F)$

$\boxed{\text{problem}}$ $\boxed{\text{HW2}}$

claim: C is the center of $GL_n(F)$ denoted by $Z(GL_n(F))$

$\boxed{\text{Def}}$ A subgrp $H \leq G$ is called the center of G if $hg = gh$ for all $h \in H$ and $g \in G$

$\boxed{\text{Def}}$ Let $Hg = \{hg \mid h \in H\}$ where $g \in G$, similarly $gH = \{gh \mid h \in H\}$ is called right / left coset.

properties:

① For $g_1, g_2 \in G$

if $Hg_1 \cap Hg_2 \neq \emptyset$ then $Hg_1 = Hg_2$

Pf: Let $x \in Hg_1 \cap Hg_2$ (since $Hg_1 \cap Hg_2 \neq \emptyset$)

Then $\exists h_1, h_2$ s.t $h_1 g_1 = h_2 g_2$, i.e $g_1 = h_1^{-1} h_2 g_2$

Thus $Hg_1 = H h_1^{-1} h_2 g_2 = Hg_2$

② if $|H| < \infty$ then $|Hg| = |H|$ since $H \longrightarrow Hg$, $h \longmapsto hg$ is $1 \leftrightarrow 1$ map.

$\boxed{\text{Thm}}$ (Lagrange) if G is a finite group, then the order of a subgrp divides the order $|G|$

i.e for $H \leq G$ we have $|H| \mid |G|$

Usually "$\leq$" means "subgroup"

"$<$" means "proper subgroup"

Pf : Write all right cosets of H in G (distinct cosets)

$Hg_1, \dots, Hg_m$. then $G = \bigsqcup_i Hg_i$

Since $|H| = |Hg|$ $\forall g \in G$ $\Rightarrow$ $|H| \mid |G|$

Let $|G| < \infty$ for $g \in G$, $g, g^2, \dots, g^n \dots$ is finite sequence.

i.e for some m, $g^m \in \{g, g^2, \dots, g^{m-1}\}$

So $g^m = g^j$ for some $1 \le j \le m-1$

$\Rightarrow$ $g^{m-j} = 1$ $\Rightarrow$ $g^{-1} = g^{m-j-1}$ $\quad$ $\langle g \rangle$ forms a subgroup of G $\quad |g| = |\langle g \rangle|$

Thus. In particular. each elts of G, their order dividing $|G|$

i.e. $\forall x \in G$. $|x| \mid |G|$

$\boxed{\text{Thm}}$ (Fermat) Let p a prime and $a \in \{1, \dots p-1\}$

Then $a^{p-1} \equiv 1 \mod p$.

pf: Let $G = (\mathbb{Z}_p \setminus \{p\}, \otimes)$ a grp. of order $p-1$

Then $a \in G$ so $|a| \mid |G|$, i.e $a^{p-1} \equiv 1 \mod p$.

$a^{|G|} = \bar{1}$

$\boxed{\text{HW}}$ $(\mathbb{Z}_n, \oplus, \otimes)$ is a ring

$(\mathbb{Z}_n \setminus \{0\}, \otimes)$ is not necessary a group

Let $U(n) = \{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}$

Then $(U(n), \otimes)$ is a group of order $\varphi(n)$

φ is Eular function. prove this and use this prove following Thm:

$\boxed{\text{Thm}}$ (Eular) Let n be a positive integer. and let a be an integer which is coprime to n.

if $1 \le a < n$ the $a^{\varphi(n)} \equiv 1 \mod n$.

$\boxed{\text{Def}}$ let $H \le G$ Then H is called normal subgroup of G if

$g^{-1}hg \in H \ \forall\, h \in H$ and $\forall\, g \in G$. denoted by $H \triangleleft G$.

$\boxed{\text{HW4}}$ $Z(G) \triangleleft G$