半群的定义：非空集合G+二元运算"$\circ$"+"$\circ$"满足结合律 → 幺半群：有幺元的群

群的定义：幺半群中每个元都是可逆元

（半群中左右幺元不一定都存在，存在也不一定唯一，甚至可能都不存在 ⇒ 幺半群是特殊的半群（幺元唯一性：$e_1=e_1\circ e_2=e_2$））

↳ 群是一个集合G，且关于G中运算$\circ$满足以下4个条件

① $\forall a,b\in G$，有$a\circ b\in G$，即运算封闭

② $\forall a,b,c\in G$，有$(a\circ b)\circ c=a\circ(b\circ c)$ 结合律

③ $\exists e\in G$, s.t. $\forall a\in G$，有$e\circ a=a\circ e=a$ 幺元

④ $\forall a\in G$, $\exists b\in G$, s.t. $b\circ a=a\circ b=e$ 可逆元

→ 交换半群中，若有左(右)幺元，则其为幺元（逆元同理）

proof：设e_1,e_2为左幺元，$e_1=e_2\circ e_1=e_1\circ e_2=e_2$

可简化为单边条件

such as… ③* $\exists e\in G$, $\forall a\in G$, $e\circ a=a$ 左幺元

④* $\forall a\in G$, $\exists b\in G$, 使$b\circ a=e$ 左逆元

⇒ proof：① 左逆元=右逆元，记$(a^{-1})'$为a^{-1}的左逆元

故$a\cdot a^{-1}=(a^{-1})'\cdot a^{-1}\cdot a\cdot a^{-1}=(a^{-1})'\cdot e\cdot a^{-1}=(a^{-1})'\cdot a^{-1}=e$

② 左幺元=右幺元

利用①结论有$a\cdot e=a\cdot a^{-1}\cdot a=e\cdot a=a$

得证

只是左幺元和右逆元不行，例子如下：

半群$\langle G,\circ\rangle$，$a\circ b=b$，则$\forall a\in G$，任取一个元素e，$e\circ a=a$

则e为左幺元，而$\forall a\in G$，$a\circ e=e$，故e为右逆元

那么这种半群不存在右幺元和左单位元，不是群

命题：若半群G满足：$\forall a,b\in G$，方程$ax=b$，$xa=b$均有解，则G是群

proof：利用群定义的4个条件①②③*④*证明

由于G是半群，①②已满足，因$xa=a$有解，记为e_a

下证e_a是G的左幺元，$\forall c\in G$，$ax=c$有解，记为d

⇒ $ad=c$，$e_ac=e_aad=ad=c$，得证，③*成立

又$\forall a\in G$，$xa=e_a$有解，解即为a的左逆元，④*成立

命题：有限半群G若满足左右消去律，则G是群

proof：设$G=\{a_1,\cdots,a_n\}$，证明$\forall a,b$，$ax=b$，$xa=b$均有解

断言$aa_1,aa_2,\cdots,aa_n$两两不等，否则由消去律知矛盾，由半群

对运算封闭，知$aa_1,\cdots,aa_n$为$a_1\cdots a_n$的一个排列，由$b\in G$，知$\exists a_i$；

$aa_i=b$，则a_i为$ax=b$的解，同理可证$xa=b$有解

规定$a^n=\overbrace{aa\cdots a}^{n个}$，$a^{-n}=(a^{-1})^n$，$a^0=e$，由此对$\forall m,n\in\mathbb{Z}$有$a^ma^n=a^{m+n}$，$(a^m)^n=a^{mn}$

若G是交换群，还有$(ab)^m=a^mb^m$

当G是交换群时，我们有时把运算记为加法，这时的幺元常称为零元，记为0，$a\in G$的逆元常称为负元，记为$-a$

阶

群G中所含元素的个数$|G|$，若$|G|$有限称为有限群，若$|G|$无限称为无限群

群中元素a，若$\forall k\in N$，有$a^k\neq e$，称a的阶为无限，若$\exists k\in N$，使$a^k=e$，则称$\min\{k\in N|a^k=e\}$为a的阶

即$\forall m,n$，若$m\neq n$，则$a^m\neq a^n$

☆ 定理：在有限群中，元素的阶整除群的阶

proof：$\forall a\in G$，G为有限群，考虑由a产生的循环群，先记$|a|=d$，则$\{e,a,a^2,\cdots,a^{d-1}\}$为$G$的一个子群$A$

由$A<G$，Lagrange定理得$|G|=[G:A]|A|=[G:A]d$

⇒ $d\,\big|\,|G|$，得证

Abel群中很好用

命题：设$a,b\in G$，a的阶为m，b的阶为n，$ab=ba$，$(m,n)=1$，则ab的阶为mn

proof：记ab的阶为q，去证$q=mn$（常用套路为证$q|mn$，$mn|q$）

1° 由交换律，故$(ab)^{mn}=(a^m)^n(b^n)^m=e$ ⇒ $q|mn$

2° 又$(ab)^{qm}=(a^m)^q(b^{qm})=b^{qm}$，而$(ab)^{qm}=((ab)^q)^m=e^m=e$，于是$b^{qm}=e$ ⇒ $n|qm$

由$(m,n)=1$知$n|q$，同理有$m|q$，故由$(m,n)=1$知$mn|q$

综上所述，$q=mn$

思考1. 若只知道a,b的阶有限，能否推出ab的阶有限？

不能，不存在a,b的阶关连到ab的阶之一般公式

→ 思考2. 若无$(m,n)=1$条件，则ab的阶是？

由右题知$q|mn$，$n|qm$，$m|qn$，且至少知$q|[m,n]$

（易知$|a|=|a^{-1}|=m$，而$a\cdot a^{-1}=e$，$|e|=1$）

子群：H是群G的一个非空子集，若H对于G的运算也构成群，则称H为G一个子群，记作$H<G$

$H=\{e\}$和$H=G$都是G的子群，它们称为G的平凡子群，G的其他子群称为非平凡子群

设H是群G的非空子集，则下面条件是等价的

① $H<G$

② $a,b\in H$ ⇒ $ab\in H$，$a^{-1}\in H$

③ $a,b\in H$ ⇒ $ab^{-1}\in H$

常用

☆ 也可以改写成$a^{-1}b\in H$

⇒ 可用来证明：若$H_1<G$，$H_2<G$，则$H_1\cap H_2<G$

用同样方法可证明群G任意多个（可以是无穷多个）子群的交仍是子群

proof：①⇒②：因H是群，对运算封闭，故$ab\in H$，$a^{-1}\in H$也显然

②⇒③：据②知$b^{-1}\in H$，而$ab^{-1}\in H$

③⇒①：利用群定义的4个条件来验证H也是一个群。

$a,a\in H$ ⇒ $aa^{-1}=e\in H$ 从而H中有幺元，又$\forall b\in H$，$e,b\in H$ ⇒ $eb^{-1}=b^{-1}\in H$

说明H中任一元素有逆元，又$a,b\in H$，$b^{-1}\in H$ ⇒ $a(b^{-1})^{-1}=ab\in H$，从而运算封闭

又$H\subseteq G$，而G是群，故运算满足结合律，综上，$H<G$

命题：H为群G的非空有限子集，则$H<G$ ⇔ H对G中运算封闭

（利用运算封闭 ⇒ 有限半群，又由左右消去律 ⇒ 有限群 得证）

子群延伸概念：左陪集（右陪集） ⟶ $H<G$，$a\in H$，则$aH=\{ah|h\in H\}$为左陪集

（右陪集定义类似）

↳ $H<G$，等价关系：aRb ⇔ $a^{-1}b\in H$

陪集分解

⇒ a所在的等价类$\bar{a}=aH$，故H的全体左陪集的集合$\{aH\}$是G的一个分类

左商集（左陪集空间）：

关于等价关系aRb ⇔ $a^{-1}b\in H$

的商集合G/R称为G对H的左商集

也称为G对H的左陪集空间，记G/H

proof：①R是等价关系：1° $\forall a\in G$，$a^{-1}a=e\in H$ 故aRa　2° 若aRb即$a^{-1}b\in H$，因H是群，故$(a^{-1}b)^{-1}\in H$ ⇒ bRa　3° 又若aRb，bRc，$a^{-1}b\in H$，$b^{-1}c\in H$ ⇒ $a^{-1}b\cdot(b^{-1}c)=a^{-1}c\in H$ ⇒ aRc

② $\forall a\in G$，$\bar{a}=aH$：$\forall b\in\bar{a}$，有aRb，故$a^{-1}b\in H$，记$h=a^{-1}b\in H$ ⇒ $b=ah\in aH$ 故$\bar{a}\subseteq aH$

又$\forall b\in aH$，即$\exists h\in H$，$b=ah$，故$a^{-1}b=h\in H$ ⇒ $b\in\bar{a}$ 故$aH\subseteq\bar{a}$ 于是$\bar{a}=aH$

推论：(1) $a\in aH$　(2) $a\in H$ ⇔ $aH=H$　(3) $b\in aH$ ⇔ $aH=bH$　(4) $aH=bH$ ⇔ $a^{-1}b\in H$

(5) 若$aH\cap bH\neq\emptyset$，则$aH=bH$　proof：设$c\in aH\cap bH$ ⇒ $c\in aH$，$c\in bH$，于是由(3)知$aH=bH=cH$

补充：由G的左陪集分解$G=aH\cup bH\cup cH\cdots$ 可立得G的一个右陪集分解$G=Ha^{-1}\cup Hb^{-1}\cup Hc^{-1}$

（Lagrange定理）设G是有限群，$H<G$，则有：$|G|=[G:H]|H|$（子群的阶是$|G|$的因子）

proof：首先，H的任一左陪集aH中的元素$=|H|$，因为

$\varphi: h\mapsto ah$，$\forall h\in H$是H到aH的双射

其次，由于$\{aH\}$是G的分类，这些左陪集个数为$[G:H]$

⇒ $|G|=[G:H]|H|$

$[G:H]$称为H在G中的指数

即G/H商集合中元素的个数

推论：设G是有限群，$K<G$，$H<K$，则有$[G:H]=[G:K][K:H]$

从左、右陪集的定义知道，一般地，没有$aH=Ha$，$\forall a\in G$，但如果群G的某个子群H有这个性质，将会连带很多好性质，则具有这种性质的子群称为：

正规子群：设G是群，$H<G$，如果有$ghg^{-1}\in H$，$\forall g\in G$，$\forall h\in H$，则称H为G的一个正规子群，记为$H\lhd G$

1. 平凡子群均是正规子群

2. Abel群的任意子群都是正规子群

正规子群的几个充要条件

① $H\lhd G$

② $gH=Hg$，$\forall g\in G$

☆ ③ $g_1H\circ g_2H=g_1g_2H$，$\forall g_1,g_2\in G$

（这里$g_1H\circ g_2H=\{g_1h_1g_2h_2|h_1,h_2\in H\}$）

proof：①⇒②：因$H\lhd G$，$\forall g\in G$，$\forall h\in H$，有$gh=ghg^{-1}g\in Hg$，$hg=gg^{-1}hg\in gH$（利用ghg^{-1}，$g^{-1}hg\in H$），故$gH=Hg$

★ ②⇒③：$\forall g_1,g_2\in G$，考虑$g_1H\circ g_2H$中的任一元素，$g_1h_1g_2h_2$，$h_1,h_2\in H$，由②知$h_1g_2\in Hg_2=g_2H$，故$\exists h_3\in H$，使$h_1g_2=g_2h_3$ ⇒ $g_1h_1g_2h_2=g_1g_2h_3h_2\in g_1g_2H$

从而$g_1H\cdot g_2H\subseteq g_1g_2H$，又考虑$g_1g_2H$任一元$g_1g_2h=g_1eg_2h\in g_1H\circ g_2H$，故$g_1g_2H\subseteq g_1H\circ g_2H$ 故$g_1H\circ g_2H=g_1g_2H$

③⇒①：$\forall g\in G$，$\forall h\in H$，$ghg^{-1}=ghg^{-1}e\in gH\circ g^{-1}H=gg^{-1}H=H$，则$H\lhd G$

命题：设G是群，$H<G$，R是由G中aRb ⇔ $a^{-1}b\in H$定义的关系，则R是G中同余关系 ⇔ $H\lhd G$

此时，商集合G/R对同余关系R导出的运算也构成一个群，称为G对H的商群，记为G/H

proof："⇐" 设a_1Rb_1，a_2Rb_2，要证$a_1a_2Rb_1b_2$ ⇒ 即证$(a_1a_2)^{-1}(b_1b_2)\in H$，因$(a_1a_2)^{-1}(b_1b_2)=a_2^{-1}(a_1^{-1}b_1)a_2(a_2^{-1}b_2)$

由$a_1^{-1}b_1\in H$，$a_2^{-1}b_2\in H$，及$H\lhd G$知$a_2^{-1}(a_1^{-1}b_1)a_2\in H$ 故知上式成立

"⇒" 现设R是G中的同余关系，去证$H\lhd G$，$\forall g\in G$，$\forall h\in H$，因$g^{-1}(gh)\in H$知$gRgh$，又有$g^{-1}Rg^{-1}$

由同余关系知$gg^{-1}Rghg^{-1}$ ⇒ $eRghg^{-1}$ 即$e^{-1}ghg^{-1}=ghg^{-1}\in H$，故$H\lhd G$

补充 同余关系：由于在运算"$\circ$"下仍然保持，故可以产生一种与"$\circ$"有关的运算"$\bar{\circ}$"，$\bar{a}\,\bar{\circ}\,\bar{b}=\overline{a\circ b}$

即等价类的运算不仅归结为代表元的运算，且不依赖于代表元的选择，这当且仅当该等价关系是同余关系时是正确的（proof：a_1Ra_2，b_1Rb_2 ⇒ $\bar{a}_1=\bar{a}_2$，$\bar{b}_1=\bar{b}_2$，$\bar{a}_1\bar{\circ}\bar{b}_1=\overline{a_1\circ b_1}=\overline{a_2\circ b_2}$，由同余关系易知其成立）

则商集合中的运算可就是$aH\cdot bH=(a\cdot b)H$，$\forall a,b\in G$ 即$\forall aH,bH\in G/R$

这一运算满足结合律（$\forall aH,bH,cH\in G/R$有$(aH\cdot bH)\cdot cH=abH\cdot cH=abcH=aH\cdot(bcH)=aH(bH\cdot cH)$）

这一运算有左幺元eH（$\forall aH\in G/R$，有$eH\cdot aH=(ea)H=aH$）

G/R中任一元aH有左逆元（$\forall aH\in G/R$，$a^{-1}H\cdot aH=(a^{-1}a)H=eH$）

所以商集合G/R对于同余关系R导出的运算也构成一个群，称为G对H的商群，记为G/H