0.1 正规子群

定义 0.1 (正规子群)

令 $(G,\cdot)$ 是一个群，且 $N\subset G$。我们称 N 是个正规子群, 记作 $N\lhd G$，若

$$N \text{ 是个子群,}$$
$$\forall a\in G, aN=Na.$$

注 注意 $aN=Na \nLeftrightarrow an=na,\forall n\in N$. 虽然 $an=na,\forall n\in N\Rightarrow aN=Na$, 但是 $aN=Na\nRightarrow an=na,\forall n\in N$. 实际上,$aN=Na\Leftrightarrow \exists n,n'\in N\ \text{s.t.}\ an=n'a$.

引理 0.1

设 H 是一个幺半群, 则 $HH=H$。

笔记 因为群也是幺半群，所以这个引理对群也成立。

证明 一方面，对 $\forall h_1,h_2\in H$，根据乘法封闭性 (乘法是 H 上的代数运算)，都有 $h_1h_2\in H$。故 $HH\subset H$。

另一方面，设 $h\in H$，则 $h=he\in HH$，其中 e 是 H 的单位元. 故 $H\subset HH$。因此 $HH=H$。 □

命题 0.1

令 $(G,\cdot)$ 是一个群，且 $N\lhd G$，$a,b\in G$，则

$$(aN)\cdot(bN)=(ab)N.$$

是良定义的.

注 因为陪集代表元的不唯一性可能导致上述乘积运算结果不唯一, 所以上述乘积运算不一定是良定义的, 需要给出证明.

结论 元素与群 (其实只要满足结合律的半群就足够了) 的乘积满足广义结合律. 例如: 设 G 是一个群, 若 $H,K<G$,$a,b\in G$, 则

$$aHbK=(aH)(bK)=a((Hb)K)=a(H(bK))=(a(Hb))K=((aH)b)K.$$
$$abHK=(ab)(HK)=a((bH)K)=a(b(HK))=((ab)H)K.$$
$$\cdots\cdots\cdots\cdots$$

即两个陪集相乘可以看作一个陪集或两个陪集的乘积的陪集等.

证明 证法一: 设 $aN=a'N,bN=b'N$，则由引理**??**可知 $a^{-1}a',b^{-1}b'\in N$，我们只须证明 $abN=a'b'N$，即 $(ab)^{-1}a'b'=b^{-1}a^{-1}a'b'\in N$。首先中间这个部分，即 $a^{-1}a'$，是在 N 中的。接着，利用 N 是个正规子群, 再结合引理**??**, 我们可以得到 $b^{-1}Nb=N$，因此，$b^{-1}a^{-1}a'b'\in b^{-1}Nb'=N$。进一步地，由引理**??**可得 $abN=a'b'N$。这就证明了良定义性。

证法二:事实上，这个乘法可以简单地理解成子集乘法，即 $(aN)(bN)=\{xy:x\in aN,y\in bN\}$。我们只须说明，这从集合意义上，等于 abN。而这几乎是显然的。由于 $Nb=bN$ 及引理**??**, 我们有 $aNbN=abNN=abN$. 这样，既然从集合意义上相等，那么自然就是良定义的（因为我们不必选取单位元）。 □

命题 0.2 (商群)

令 $(G,\cdot)$ 是一个群, 且 $N\lhd G$, 则 $(G/N,\cdot)$ 构成一个群, 称为（G 在 N 上的）商群, 其中的单位元是 $eN=N$, 每个陪集 aN 的逆元是 $a^{-1}N$。

证明 由命题**??**可知商群 $(G/N,\cdot)$ 的乘法是良定义的.

封闭性：对 $\forall aN,bN\in(G/N,\cdot)$, 其中 $a,b\in G$, 根据 G 对乘法的封闭性可得 $ab\in G$, 从而 $(aN)(bN)=abN\in$

$(G/N,\cdot)$.

结合律：令 $a,b,c\in G$，则利用乘法的定义，$(aNbN)cN=(abN)(cN)=((ab)c)N$。利用 G 对乘法的结合律，得到这是等于 $(a(bc))N$ 的。类似地，这最终等于 $aN(bNcN)$。

单位元：令 $a\in G$，则 $aNeN=(ae)N=aN$，类似地 $eNaN=aN$。

逆元：令 $a\in G$，则 $aNa^{-1}N=(aa^{-1})N=eN$，类似地 $a^{-1}NaN=eN$。

综上，若 $N\lhd G$，则 G/N 在这个自然的乘法下构成群，称为一个商群。 □

引理 0.2 (正规子群的等价条件)

令 $(G,\cdot)$ 是一个群，且 $N<G$，则下列命题等价

(1) N 是 G 的正规子群，即 $\forall a\in G, aN=Na$.

(2) $\forall a\in G, aNa^{-1}=N$.

(3) $\forall a\in G, aNa^{-1}\subset N$.

(4) $\forall a\in G,\forall n\in N, ana^{-1}\in N$.

♡

证明 显然 (3) 和 (4) 等价.

(1) ⇔ (2): 一方面，设 N 是 G 的正规子群. 则由引理**??**可得 $\forall a\in G, aNa^{-1}=N$.

另一方面，设 (2) 成立. 则由引理**??**可得 $\forall a\in G, aN=Na$.

(1) ⇔ (3): 一方面，设 N 是 G 的正规子群。令 $a\in G$，则 $aN=Na$。同时右乘 a^{-1} 并取一半的包含关系，我们得到了 $aNa^{-1}\subset N$。

另一方面，设 (3) 成立。令 $a\in G$，则由 $aNa^{-1}\subset N$ 及引理**??**得到 $aN\subset Na$，由 $a^{-1}N(a^{-1})^{-1}\subset N$ 及引理**??**得到得到 $Na\subset aN$。因此，$aN=Na$。 □

例题 0.1 证明: $SL(n,\mathbb{R})\lhd GL(n,\mathbb{R})$.

证明 显然 $SL(n,\mathbb{R})<GL(n,\mathbb{R})$。任取 $A\in GL(n,\mathbb{R})$，$N\in SL(n,\mathbb{R})$，都有

$$\det(ANA^{-1})=\frac{\det(A)\det(N)}{\det(A)}=\det(N)=1.$$

从而 $ANA^{-1}\in SL(n,\mathbb{R})$。故 $SL(n,\mathbb{R})\lhd GL(n,\mathbb{R})$。 □

命题 0.3 (正规子群的任意交还是正规子群)

设 $(N_i)_{i\in I}$ 是一族 G 的正规子群，则它们的交集仍然是 G 的正规子群，即

$$\bigcap_{i\in I}N_i\lhd G.$$

♠

证明 首先，由子群的任意交仍是子群可知 $\bigcap_{i\in I}N_i<G$. 因此我们只需证明正规性。利用正规子群的等价条件 (3) 可知, 对 $\forall a\in G,\forall n\in\bigcap_{i\in I}N_i$, 我们只须证明 $ana^{-1}\in\bigcap_{i\in I}N_i$ 即可. 任取 $i\in I$，则 $n\in N_i$。由于 $N_i\lhd G$，我们有 $ana^{-1}\in N_i$。因此，由 i 的任意性可知 $ana^{-1}\in\bigcap_{i\in I}N_i$。这就证明了 $\bigcap_{i\in I}N_i\lhd G$。 □

命题 0.4

令 $(G,\cdot)$ 是一个群，则

$$\{e\}\lhd G,$$
$$G\lhd G.$$

♠

证明 平凡群：怎么乘都是单位元，所以对乘法封闭；包含单位元；唯一的元素的逆元还是单位元；在这个群中，a 的左右陪集都是 $a\{e\}=\{e\}a=\{a\}$。因此，$\{e\}\lhd G$。

整个群：子群是显然的；在整个群 G 中，每个元素的左右陪集都是全集，即 $aG=Ga=G$，这是因为 $a\in G$。因此，$G\lhd G$(推论**??**). □

推论 0.1

(1) 若 G 是一个群，e 是其单位元，则 $G/\{e\}$ 同构于 G，即 $G/\{e\} \simeq G$。
(2) 若 G 是一个群，则 G/G 是平凡群，即 $G/G = \{e\}$。

证明

(1) 令

$$f : G \to G/\{e\}, a \mapsto a\{e\} = \{a\}.$$

显然 f 是双射。对 $\forall a, b \in G$，我们都有

$$f(ab) = \{ab\} = ab\{e\} = (a\{e\})(b\{e\}) = \{a\}\{b\} = f(a)f(b).$$

因此 f 也是同态映射。于是 f 是同构映射。故 $G/\{e\} \simeq G$。

(2) 由命题**??**及命题**??**可知 G/G 是一个群。注意到 $\forall a \in G$，都有 $aG = G$。因此 $G/G = G$。于是 $|G/G| = 1$。故 $G/G = \{e\}$。

□

命题 0.5

令 $(G, \cdot)$ 是个阿贝尔群，则子群就是正规子群，正规子群也就是子群，即

$$H < G \iff H \lhd G$$

证明 $\Leftarrow$: 由于正规子群都是子群, 故显然成立.

$\Rightarrow$: 根据阿贝尔群满足交换律可知 $aH = \{ah : h \in H\} = \{ha : h \in H\} = Ha$。 □

定理 0.1 (群同构第一定理)

设 $f : G \to G'$ 是一个群同态，则 $\ker(f) \lhd G$，且 G 在 $\ker(f)$ 上的商群同构于 $\mathrm{im}(f)$，即

$$G/\ker(f) \cong \mathrm{im}(f).$$

特别地，若 f 是满同态，则

$$G/\ker(f) \cong G'.$$

若 f 是单同态，则

$$G/\{e\} \cong G \cong \mathrm{im}(f).$$

若 G 是有限群，则

$$\frac{|G|}{|\ker(f)|} = |\mathrm{im}(f)|, \text{也即} |G| = |\ker(f)||\mathrm{im}(f)|.$$

注 要注意，同态的像 $(\mathrm{im}(f))$ 未必是 G' 的正规子群，往往只是普通的子群。

证明 根据命题**??**和 Lagrange 定理, 这三条推论都是显然的，唯一要说明的是 $G/\{e\}$ 为什么同构于 G, 这由推论**??**(1) 可直接得到. 这就意味着我们只须证明原命题即可.

首先要说明每个同态的核都是定义域的正规子群。我们只须证明，若 $a \in G, n \in \ker(f)$，则 $ana^{-1} \in \ker(f)$。注意到

$$f(ana^{-1}) = f(a)e'f(a)^{-1} = e'.$$

因此 $ana^{-1} \in \ker(f)$。这就证明了 $\ker(f) \lhd G$。

接下来，我们要找到一个从商群 $G/\ker(f)$ 到像集 $\mathrm{im}(f)$ 的同构映射。我们称这个映射叫 $\tilde{f} : G/\ker(f) \to \mathrm{im}(f)$，对于 $a \in G$，定义为

$$\tilde{f}(a\ker(f)) = f(a).$$

为了方便起见，在不会引起歧义的情况下，我们令 $N = \ker(f)$，也即

$$\tilde{f}(aN) = f(a).$$

考虑到陪集代表元的不唯一性，我们要证明良定义性。假设 $aN = a'N$，或 $a^{-1}a' \in N$，只须证明 $f(a) = f(a')$，而这是因为

$$f(a') = f(aa^{-1}a') = f(a)f(a^{-1}a') = f(a)f(eN) = f(a)e' = f(a).$$

其中 e 是 G 的单位元,e' 是 G' 的单位元. 这就证明了良定义性。

接下来，我们要证明 $\tilde{f}$ 既是同态，也是双射（单射 + 满射）。

同态：令 $a, b \in G$，则 $\tilde{f}(aN) = f(a)$，$\tilde{f}(bN) = f(b)$，而由 $N = \ker f \lhd G$ 及 f 是一个群同态可得

$$\tilde{f}((aN)(bN)) = \tilde{f}(abN) = f(ab) = f(a)f(b) = \tilde{f}(aN)\tilde{f}(bN).$$

这就证明了 $\tilde{f}$ 是一个同态。

单射：只须证明 $\ker(\tilde{f}) = \{N\}$。设 $\tilde{f}(aN) = e'$，则根据定义，$f(a) = e'$，故 $a \in \ker(f) = N$，所以 $aN = N$，这就证明了 $\tilde{f}$ 是一个单射。

满射：令 $a' \in \operatorname{im}(f)$，取 $a \in G$ 使得 $a' = f(a)$。因此，$\tilde{f}(aN) = f(a) = a'$，这就证明了 $\tilde{f}$ 是一个满射。

综上所述，$\tilde{f}$ 是一个从商群 $G/\ker(f)$ 到像集 $\operatorname{im}(f)$ 的同构。作为结论，

$$G/\ker(f) \cong \operatorname{im}(f).$$

这就完成了整个命题的证明。 □

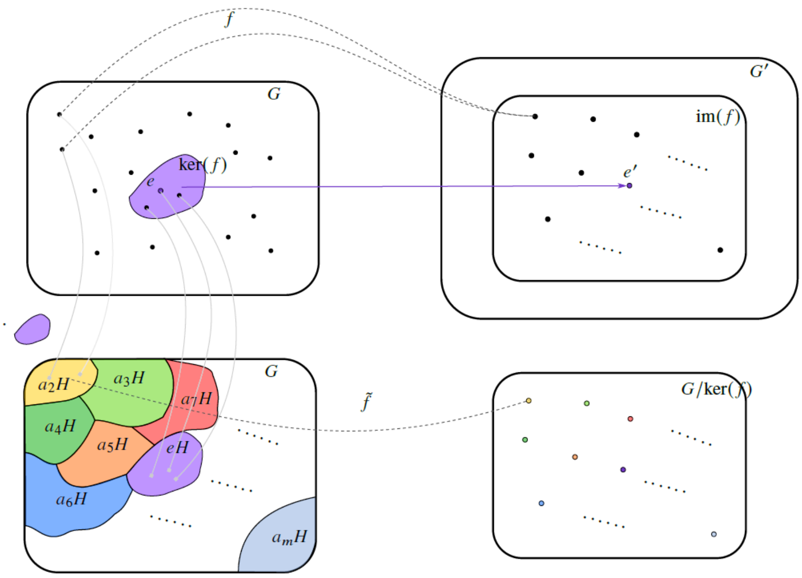

图 1: 群同构第一定理示意图

例题 0.2 证明:$GL(n,\mathbb{R})/SL(n,\mathbb{R}) \cong \mathbb{R}^{\times}$.

证明 由命题??可知

$$\det : GL(n,\mathbb{R}) \to \mathbb{R}^{\times}.$$

是个满同态，且 $\ker(\det) = SL(n,\mathbb{R})$, 故由群同构第一定理，我们有

$$SL(n,\mathbb{R}) \lhd GL(n,\mathbb{R}) \text{且} GL(n,\mathbb{R})/SL(n,\mathbb{R}) \cong \mathbb{R}^{\times}.$$

□

推论 0.2

设 G 是有限群,$f : G \to G'$ 是一个群同态, 则

$$|\mathrm{im}\, f| \,\Big|\, \gcd(|G|, |G'|).$$

证明 由群同构第一定理可知,$|\mathrm{im}\, f| \,\Big|\, G$. 由 Lagrange 定理可知,$|\mathrm{im}\, f| \,\Big|\, G'$. 故

$$|\mathrm{im}\, f| \,\Big|\, \gcd(|G|, |G'|).$$

□

例题 0.3 设 $f : C_{12} \to C_{35}$ 是一个群同态, 求证:f 是平凡同态, 即对 $\forall x \in C_{12}$, 都有 $f(x) = e$, 也即 $\mathrm{im}\, f = \{e\}$., 其中 e 是 C_{35} 的单位元.

证明 由推论??可知,$|\mathrm{im}\, f| \,\Big|\, \gcd(12, 35) = 1$. 又因为 $\mathrm{im}\, f < G'$, 所以 $\mathrm{im}\, f = \{e\}$. □

引理 0.3

设 $(G, \cdot)$ 是一个群，且 $N \lhd G$，$H < G$。则 $HN < G$.

证明 设 e 是 G 的单位元，则由 $N \lhd G$，$H < G$ 可知，$e \in N \cap H$。从而 $e = ee \in HN$。

对 $\forall h_1 n_1, h_2 n_2 \in HN$，其中 $h_1, h_2 \in H$，$n_1, n_2 \in N$。由 $N \lhd G$，$H < G$ 可得

$$h_1 n_1 (h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 n_1 h_2^{-1} n_2^{-1} = h_1 h_2^{-1} n_1 n_2^{-1} \in HN.$$

故 $HN < G$. □

定理 0.2 (群同构第二定理)

设 $(G, \cdot)$ 是一个群，且 $N \lhd G$，$H < G$。则 $H \cap N \lhd H$，$N \lhd HN$，且

$$H/(H \cap N) \cong HN/N.$$

这和之前两个子群乘积的阶的公式是类似的。

注 由引理??可知 $HN < G$. 故此时 $N \lhd HN$ 是有意义的.

证明 第一，要证明 $H \cap N \lhd H$。令 $h \in H$，而 $x \in H \cap N$，则 $hxh^{-1} \in H$，而且因为 $N \lhd G$，$hxh^{-1} \in N$，因此 $hxh^{-1} \in H \cap N$。

第二，要证明 $N \lhd HN$。令 $hn \in HN$，而 $n' \in N$。则由引理??(2) 可得 $hnn'(hn)^{-1} = h(nn'n^{-1})h^{-1} \in hNh^{-1} = N$。

第三，要证明 $H/(H \cap N) \cong HN/N$。令 $f : H \to HN/N$，定义为

$$f(h) = hN.$$

这显然是良定义的 (若 $h = h' \in H$, 则 $h^{-1}h' = e \in N$, 从而 $f(h) = hN = h'N = f(h')$). 又由 $N \lhd G$ 及引理??可知, 对 $\forall h_1, h_2 \in H$, 都有

$$f(h_1 h_2) = h_1 h_2 N = h_1 h_2 N N = h_1 N h_2 N = f(h_1) f(h_2).$$

故 f 是同态的. 根据 $HN/N = \{hnN : h \in H, n \in N\} = \{hN : h \in H\}$ 可知,f 还是个满同态。

接下来，根据引理??可知,f 的核是 $\ker(f) = \{h \in H : hN = eN\} = \{h \in H : h \in N\} = H \cap N$。因此，根据群同构第一定理,

$$H/(H \cap N) \cong HN/N.$$

这就证明了群同构第二定理。 □

引理 0.4

设 $(G, \cdot)$ 是一个群，且 $N < G$，$M \lhd G$，$M < N$, 则 $M \lhd N$.

证明 令 $n \in N \subset G$，$m \in M$，则由 $M \lhd G$ 可知,$nmn^{-1} \in M$。因此由引理??可知 $M \lhd N$. □

定理 0.3 (群同构第三定理)

设 $(G,\cdot)$ 是一个群，且 $N \lhd G$，$M \lhd G$，$M < N$。则 $N/M \lhd G/M$，且

$$(G/M)/(N/M) \cong G/N.$$

♡

证明 首先显然有 $N/M \subset G/M$。由引理**??**可知 $M \lhd N$. 因此 N/M 是个商群。因为这两个都是群，所以对单位元、乘法和逆元都有封闭性. 因此就有 $N/M < G/M$。接下来我们可以先证明正规性，这也几乎是显然的。令 $nM \in N/M(n \in N)$，$gM \in G/M(g \in G)$，则由 $M \lhd N, N \lhd G$ 可得

$$(gM)(nM)(gM)^{-1} = (gng^{-1})M \in \{nM : n \in N\} = N/M.$$

因此 $N/M \lhd G/M$.

那么，我们要定义 $f : G/M \to G/N$，定义为

$$f(gM) = gN.$$

要证明良定义性。假设 $gM = g'M$，则 $g^{-1}g' \in M$，故 $g^{-1}g' \in N$，所以 $gN = g'N$。

同态是显然的：对 $\forall gM, g'M \in G/M$, 都有

$$f(gMg'M) = f(gg'M) = gg'N = gNg'N = f(gM)g(g'M).$$

满同态几乎也是显然的。任取 $gN \in G/N(g \in G)$，则 $f(gM) = gN$。

最后，注意到

$$\ker(f) = \{gM : f(gM) = gN = eN\} = \{gM : g \in N\} = N/M.$$

于是根据群同构第一定理，这就告诉我们

$$(G/M)/(N/M) \cong G/N.$$

综上所述，我们就证明了群同构第三定理。 □