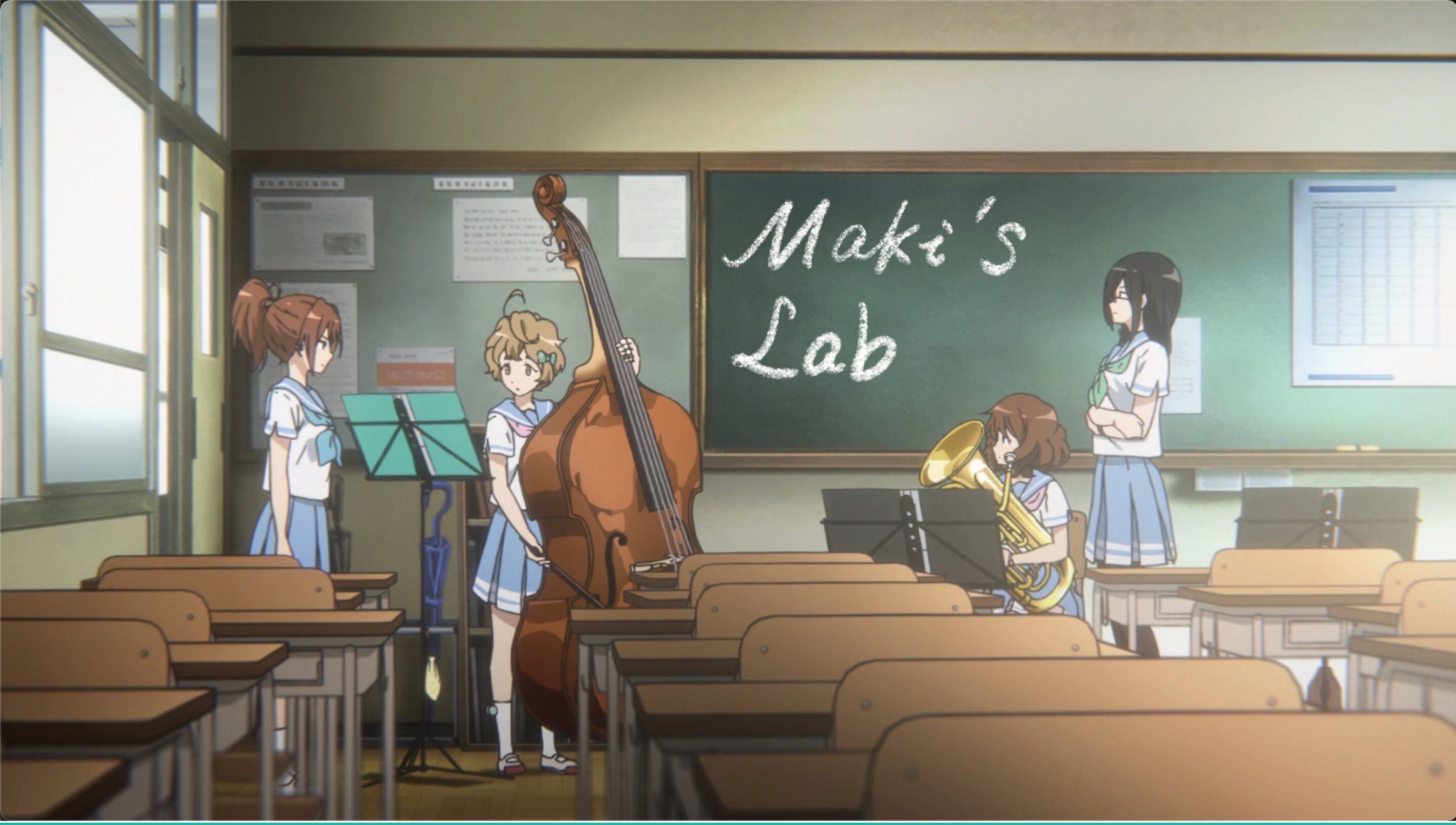
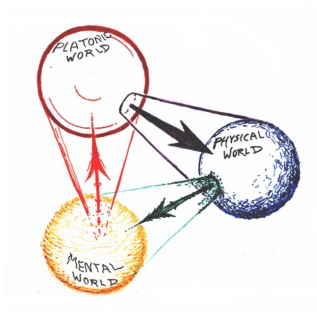


抽象代数 II
MAT2B20

作者：抽象代数委员会
组织：Maki's Lab
时间：August 29, 2022
版本：1.0



”九万里风鹏正举。风休住，蓬舟吹取三山去。”——【宋】李清照

目录

第 1 章 群论 II——Group Theory II

1.1 中心、中心化子与正规化子

我们先给出中心、中心化子和正规化子的定义。

定义 1.1

令 G 是一个群，则 G 的中心，记作 $Z(G)$，定义为

$$Z(G) = \{a \in G : \forall g \in G, ag = ga\}$$

显然，阿贝尔群的中心是整个群。这是因为阿贝尔群中的每个元素都和所有元素交换（利用乘法交换律）。

命题 1.1

令 G 是一个群，则 G 的中心 $Z(G)$ 是 G 的一个正规子群。

证明 首先，显然 $e \in Z(G)$，因为对任意 $g \in G$ 都有 $eg = ge = g$。

令 $g, h \in Z(G)$，则 g 和 h 与任意元素都交换。令 $x \in G$，则 $(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh)$，这就证明了 $gh \in Z(G)$，并且通过对 $gx = xg$ 两边同时左乘和右乘 g^{-1}，我们可以得到 $g^{-1}x = xg^{-1}$。

现在，令 $g \in Z(G)$，$a \in G$，我们只须证明 $aga^{-1} \in Z(G)$，而这是显然的，因为根据 $ag = ga$，我们有 $aga^{-1} = g$。

引理 1.1

令 G 是一个群，则 $Z(G)$ 是个阿贝尔群。

证明 令 $a, b \in Z(G)$，显然 $ab = ba$，所以 $Z(G)$ 是个阿贝尔群。

对于中心，我们有一个重要的命题。在介绍这个命题之前，我们先定义一个群的内自同构群。

定义 1.2

令 G 是一个群，则 G 上的所有内自同构构成一个群，称为内自同构群，记作 $\mathrm{Inn}(G)$。

注 我们回顾一下，G 上的一个内自同构指的是一个自同构 ϕ_g（$g \in G$），定义为 $\phi_g(x) = xgx^{-1}$。

证明 内自同构群上的运算显然是复合运算。我们来证明这样的复合是良定义的。令 $g, h \in G$，我们只须证明 $\phi_{gh} = \phi_g \circ \phi_h$。在抽代 I 的共轭作用处我们已经证过这个结论了。

同样，我们已经证明过 $(\phi_g)^{-1} = \phi_{g^{-1}}$。

因此，显然 $\mathrm{Inn}(G)$ 是个群。

现在，我们引出一个重要的命题。

命题 1.2

令 G 是一个群，则 $G/Z(G) \simeq \mathrm{Inn}(G)$。

证明 老样子，我们用群同构第一定理，我们只须构造出一个从 G 到 $\mathrm{Inn}(G)$，并且核是 $Z(G)$ 的群同态即可。

再次利用共轭作用的知识，我们知道 $g \mapsto \phi_g$ 给出了一个从 G 到 $\mathrm{Inn}(G)$ 的一个同态。现在，我们来求这个群同态的核。

令 $g \in G$。则 $g \in \ker(\phi)$ 当且仅当 $\phi(g) = id_G$，即对任意 $x \in G$，都有 $gxg^{-1} = x$；换言之，对任意 $x \in G$，我们有 $xg = gx$，这就等价于说 $x \in Z(G)$。

利用群同构第一定理，我们就得到了

$$G/Z(G) \simeq \mathrm{Inn}(G)$$

此即得证。

现在，我们来做一道经典的例题。若 G 的自同构群是个循环群，那么 G 是一个阿贝尔群。

我们先给出自同构群的定义。

定义 1.3

令 G 是一个群，则 G 上的自同构群是由所有 G 的自同构所构成的群，记作 $\mathrm{Aut}(G)$。

显然，每一个内自同构都是自同构，所以 $\mathrm{Inn}(G)$ 是 $\mathrm{Aut}(G)$ 的子群。

命题 1.3

令 G 是一个群，若 $\mathrm{Aut}(G)$ 是一个循环群，则 G 是一个阿贝尔群。

证明 假设 $\mathrm{Aut}(G)$ 是一个循环群，那么 $\mathrm{Inn}(G)$ 作为它的一个子群，当然也是一个循环群。利用刚才证明的同构关系，我们知道 $G/Z(G)$ 也是一个循环群。不妨假设 $aZ(G)$ 是这个循环群的一个生成元，因此每一个 $gZ(G)$（$g \in G$）都可以写成 $aZ(G)$ 的一个幂次。

现在，令 $g.h \in G$，我们只须证明 $gh = hg$。

现在，我们假设 $gZ(G) = a^m Z(G)$，$hZ(G) = a^n Z(G)$，换言之，存在 $x, y \in Z(G)$，使得 $g = a^m x$，$h = a^n y$。

注意到 $x, y \in Z(G)$，我们就知道

$$gh = a^m x a^n y = a^m a^n xy = a^{m+n} xy$$
$$hg = a^n y a^m x = a^n a^m yx = a^{m+n} yx = a^{m+n} xy$$

因此 G 是一个阿贝尔群，此即得证。

这个命题有一个简单的推论，但也很有趣，我们用一个引理来说明这个推论。

引理 1.2

令 G 是一个有限群，则 $[G : Z(G)]$ 不能是一个素数。

证明 用反证法，假设 $[G : Z(G)]$ 是一个素数。

注意到 $G/Z(G)$ 同构于 $\mathrm{Inn}(G)$，这就告诉我们 $\mathrm{Inn}(G)$ 是一个素数阶的群，因此必定是一个循环群。

利用刚才的命题，这告诉我们 G 是一个阿贝尔群，而阿贝尔群的中心是所有元素，即 $Z(G) = G$，因此 $[G : Z(G)] = 1$，不是一个素数。

此即得证。

接着，我们来说中心化子和正规化子。对一个群 G 的任意子集，我们都可以定义中心化子和正规化子。

定义 1.4

令 G 是一个群，而 $A \subset G$，则中心化子 $C_G(A)$ 和 $N_G(A)$ 分别被定义为

$$C_G(A) = \{g \in G : \forall x \in A, gx = xg\}$$
$$N_G(A) = \{g \in G : \forall x \in A, gxg^{-1} \in A\}$$

在上面的定义中，“中心” 和 “正规” 都是非常恰当的用词，让我们很容易记忆。一般而言，中心化子是个子群，而正规化子是个子群。特别地，正规子群的中心化子是个正规子群。

命题 1.4

令 G 是一个群，$A \subset G$，则 $C_G(A)$ 是一个子群。

证明 令 $A \subset G$，令 $g, h \in C_G(A)$，即对任意 $a \in A$，我们有 $ga = ag$，$ha = ah$。

第一，对任意 $a \in A$，我们有 $ea = ae$，所以 $e \in C_G(A)$。

第二，对任意 $a \in A$，我们有 $(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh)$，所以 $gh \in C_G(A)$。

第三，对任意 $a \in A$，我们有 $ga = ag$，此即 $g^{-1}a = ag^{-1}$，所以 $g^{-1} \in C_G(A)$。

此即得证。

命题 1.5

令 G 是一个群，$N \lhd G$，则 $C_G(N)$ 是一个正规子群。

证明 令 $g \in C_G(N)$，$x \in G$，我们只须证明 $xgx^{-1} \in C_G(N)$。令 $n \in N$，我们只须证明 $xgx^{-1}n = nxgx^{-1}$，而这是因为

$$xgx^{-1}n = xg\left(x^{-1}nx\right)x^{-1} = xx^{-1}nxgx^{-1} = nxgx^{-1}$$

此即得证。

要证明正规化子是个子群，我们可以先证明一个有趣的引理，这同样是正规化子的一个重要性质。

引理 1.3

令 G 是一个群，而 $g, h \in G$，$A \subset G$，则 $gAg^{-1} = hAh^{-1}$ 当且仅当 $g^{-1}h \in N_G(A)$。

证明 左乘 g^{-1}，右乘 g，我们就得到了 $A = (gh)A(gh)^{-1}$。等价地，$(gh)A = A(gh)$，或者 $gh \in N_G(A)$。此即得证。

特别地，$gAg^{-1} = A$ 当且仅当 $g \in N_G(A)$。

注 未来我们会看到，这样的条件在西罗定理的证明中是非常重要的。

命题 1.6

令 G 是一个群，则 $N_G(A)$ 是一个子群。

证明 $eA = Ae$，所以 $e \in N_G(A)$。

假设 $gA = Ag, hA = Ah$，所以 $ghA = gAh = Agh$，因此 $gh \in N_G(A)$。

假设 $gA = Ag$，所以 $g^{-1}A = Ag^{-1}$，因此 $g^{-1} \in N_G(A)$。

综上所述，$N_G(A)$ 是一个子群。

我们来做一个小练习。

引理 1.4

令 G 是一个群，而 $H < G$，则 $H \lhd N_G(H)$。

证明 首先，任意的 $h \in H$ 都满足 $hH = Hh$，所以 $H \subset N_G(H)$。由于它们都是 G 的子群，所以 $H < N_G(H)$。

接着，令 $h \in H$，$a \in N_G(H)$，则 $aH = Ha$，所以 $aha^{-1} \in H$，这就证明了 $H \lhd N_G(H)$。

此即得证。

现在，我们定义共轭子群。

定义 1.5

令 G 是一个群，则 G 的两个子群 H, K 是共轭的，当且仅当存在 $g \in G$，使得 $H = gKg^{-1}$。

子群的共轭显然是一个等价关系。

命题 1.7

令 G 是一个群，则子群的共轭是一个等价关系。

证明 令 $H, K, L < G$。

第一，$H = eHe^{-1}$，所以 H 共轭于 H。

第二，假如 $H = gKg^{-1}$，则 $K = g^{-1}Kg$，于是 K 共轭于 H。

第三，假如 $H = gKg^{-1}$，$L = hHh^{-1}$，则 $L = hgK(hg)^{-1}$，于是 H 共轭于 L。

此即得证。

特别地，$gHg^{-1} = H$ 当且仅当 $g \in N_G(H)$，这就是我们刚才叙述的引理。

给出正规化子的定义后，我们可以将刚才的命题 $G/Z(G) \simeq \mathrm{Inn}(G)$ 推广。

命题 1.8

令 G 是一个群，而 $H < G$，则 $N_G(H)/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的一个子群。

证明 根据群同构第一定理，我们只须找到一个从 $N_G(H)$ 到 $\mathrm{Aut}(H)$ 的一个群同态，其核是 $C_G(H)$。

令 $a \in N_G(H)$，我们定义 $f : N_G(H) \to \mathrm{Aut}(H)$ 为 $(f(a))(x) = axa^{-1}$。

这是良定义的，因为对任意 $x \in x$，我们有 $axa^{-1} \in aHa^{-1} = H$。

每一个 $f(a)$ 都是一个同态，因为 $(f(a))(xy) = axya^{-1} = axa^{-1}aya^{-1} = (f(a))(x)(f(a))(y)$。

因此，f 是良定义的。

接下来，我们要找 f 的核。

假设 $f(a) = id$，换言之，对任意 $x \in H$，都有 $axa^{-1} = x$；那么等价地，这就是说 $a \in C_G(H)$，即 a 与 H 的每一个元素都交换。此即得证。

注 这显然是 $G/Z(G)$ 是 $\mathrm{Aut}(G)$ 的一个子群的特例，因为当 $H = G$ 时，我们有 $N_G(G) = G$ 以及 $C_G(G) = Z(G)$。

我们有以下的引理。

引理 1.5

令 $A \subset G$，则 $[G : N_G(A)]$ 等于 A 在 G 中的共轭子群的个数。

证明 令 $S = \{gAg^{-1} : g \in G\}$。不难发现，由 $\phi_g(B) = gBg^{-1}$ 定义的 $\phi_g : S \to S$ 是一个群作用，我们也称为共轭作用。根据轨道稳定化子定理，我们知道 A 的轨道的阶等于 $G/\mathrm{Stab}(A)$ 的阶。

此时，A 的轨道就是所有的 $\{gAg^{-1}\}$，也就是 A 的所有共轭子群。而 $\mathrm{Stab}(A) = \{g \in G : gAg^{-1} = A\} = N_G(A)$。

综上所述，我们就证明了 $[G : N_G(A)]$ 等于 A 在 G 中的共轭子群的个数。此即得证。

引理 1.6

若 G 是一个有限群，$H < G$ 是一个真子群，则 G 不能写成 H 的共轭子群的并。

证明 用反证法，假设 $N_G(H) = m$，$|H| = k$，$|G| = n$，则我们有 $n = mk$。注意到 $gHg^{-1} = H$ 当且仅当 $g \in N_G(H)$，以及 $e \in gHg^{-1} \cap H$。

假设 G 可以写成 H 中共轭子群的并，则 $mk = n \leq m(k-1)+1$，所以 $m \leq 1$，即 $m = 1$，所以 $H = G$，这就导致了一个矛盾。

此即得证。

1.2 类方程与西罗定理

在给出类方程之前，我们先给出一个等价关系。

正如子群的共轭是一个等价关系，元素的共轭也是一个等价关系。

定义 1.6

令 G 是一个群，我们称 $x, y \in G$ 是共轭的当且仅当存在 $g \in G$，使得 $x = gyg^{-1}$。

引理 1.7

群中元素的共轭关系是一个等价关系。

证明 令 $x, y, z \in G$。

首先，$x \sim x$，这是因为 $x = exe^{-1}$。

接着，若 $x = gyg^{-1}$，则 $y = g^{-1}xg$。

最后，若 $x = gyg^{-1}$，$y = hzh^{-1}$，则 $x = ghz(gh)^{-1}$。

此即得证。

定义 1.7

我们称群 G 中共轭关系的等价类为共轭类。

显然，共轭类构成了群 G 的一个分拆。

下面，我们证明一个有趣的引理。

引理 1.8

令 G 是一个群，则 x 的共轭类中只有 x 一个元素当且仅当 $x \in Z(G)$。

证明 假设 x 的共轭类中只有 x 一个元素，那么对任意 $g \in G$，我们有 $gxg^{-1} = x$，换言之，x 与群 G 中所有元素都交换，也就是说 $x \in Z(G)$。

反过来，假如 $x \in Z(G)$，那么对于任意 $g \in G$，我们有 $gxg^{-1} = x$，所以 x 的共轭类中只有 x 一个元素。

此即得证。

这个引理妙的地方在于 $Z(G)$ 本身是一个子群（正规子群），所以在有限群的情况下，$Z(G)$ 的阶会整除整个群的阶。

我们同样有另一个引理。

引理 1.9

令 $x \in G$，则存在一个从 x 的共轭类到 $G/C_G(x)$ 的双射。

证明 利用群作用的知识，我们知道共轭作用是一个群作用。利用轨道稳定化子定理，我们知道 $\mathrm{Orb}(x)$ 与 $G/\mathrm{Stab}(x)$ 存在一个一一对应。

显然，$\mathrm{Stab}(x) = \left\{g \in G : gxg^{-1} = x\right\} = C_G(x)$。

此即得证。

特别地，我们就知道 x 的共轭类的大小等于 $[|G|, |C_G(x)|]$。

现在，我们给出类方程。

命题 1.9

令 G 是一个有限群，则

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

其中 x_i 是那些元素超过一个的共轭类的代表元。

证明 利用共轭关系是一个等价关系，我们可以将群分拆为共轭类的无交并。

接着，我们作以下分类，假设 y_j 是那些只有一个元素的共轭类的代表元，那么等价地，我们有 $y_j \in Z(G)$，而 x_i 指的是那些元素超过一个的共轭类的代表元。

我们将所有的 y_j 取并集，就得到了 $Z(G)$。利用刚才的引理，我们同样知道 x_i 的共轭类的大小等于 $[|G|, |C_G(x_i)|]$。

综上所述，我们就证明了

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

这就是众所周知的类方程。

特别地，我们知道，$|Z(G)|$ 整除 $|G|$，并且每一个 $[G : C_G(x_i)]$ 都整除 $|G|$，我们就可以得到很多有意思的结论。

引理 1.10

假设 G 的阶是一个素数 p 的幂次，则 G 的中心是非平凡的。

证明 假设 $|G| = p^n$，其中 p 是一个素数。根据类方程，我们有

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

其中每一个 $[G : C_G(x_i)]$ 都整除 $|G|$，但是又不等于 1，因此必须被 p 整除。又因为 $|G|$ 被 p 整除，所以 $|Z(G)|$ 也被 p 整除，这就证明了 G 的中心是非平凡的。

在讲西罗定理之前，我们先讲柯西定理。

命题 1.10 (柯西定理)

令 G 是一个有限群，且素数 p 整除 $|G|$，则存在一个 $a \in G$，$|a| = p$。

证明 分类讨论，首先假设 G 是一个阿贝尔群。

用数学归纳法。

假设 $|G| = p$，任取 $a \in G - \{e\}$，根据拉格朗日定理，我们知道 $|a|$ 整除 p。又因为 $|a| \neq 1$，我们有 $|a| = p$。

假设对 $|G| < n$，命题都成立。现在假设 $|G| = n$。任取 $a \in G - \{e\}$，令 $N = \langle a \rangle$。因为 G 是个阿贝尔群，所以 N 是 G 的一个正规子群。假设 p 整除 $|N|$，则 $a^{|N|/p}$ 的阶显然是 p。否则，假设 p 不整除 $|N|$。由于 p 整除 $|G|$，p 一定整除 $|G/N|$。因为 $a \neq e$，所以 $|N| > 1$。利用归纳假设，我们知道存在一个 $aN \in G/N$，使得 $|aN| = p$。同时，因为 $a^{|a|} = e$，我们有 $(aN)^{|a|} = a^{|a|}N = eN$。因为 $|a| > 1$，我们有 p 整除 $|a|$。类似地，我们取 $a^{|a|/p}$，这个元素的阶是 p。

这就证明了阿贝尔群的情形。

接下来，假设 G 不是一个阿贝尔群。

根据类方程，我们知道

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

假设 p 整除 G 的阶，则利用前面的引理，我们知道 p 一定整除 $Z(G)$ 的阶。由于 $Z(G)$ 是一个阿贝尔群，所以存在一个 $a \in Z(G) \subset G$，使得 $|a| = p$。

此即得证。

下面，我们讲西罗定理。西罗定理是柯西定理的推广。

我们首先定义 p-子群和西罗 p-子群。

定义 1.8

令 G 是一个有限群，若素数 p 整除 $|G|$，且 $H < G$，则 H 被称为一个 p-子群当且仅当 $|H| = p^n$，其中 $n \geq 1$。

定义 1.9

令 G 是一个有限群，若素数 p 整除 $|G| = n$，且 $|G| = p^a m$，其中 $\gcd(m, p) = 1$，则 $H < G$ 被称为一个西罗 p-子群当且仅当 $|H| = p^a$。

我们记 G 的所有西罗 p-子群构成的集合为 $\mathrm{Syl}_p(G)$，我们将 $\left|\mathrm{Syl}_p(G)\right| = n_p(G)$。

命题 1.11 (西罗第一定理)

令 G 是一个有限群，若素数 p 整除 $|G|$，则 $\mathrm{Syl}_p(G) \neq \emptyset$。

证明 用数学归纳法。

假设 $|G| = 1$，此时命题是一个虚真命题。

假设命题对 $|G| < n$ 都成立。假设 $|G| = n = p^a m$。分类讨论。

假如 p 整除 $|Z(G)|$。利用柯西定理，我们可以找到 $a \in Z(G)$，使得 $|a| = p$。令 $N = \langle a \rangle$，由于 $a \in Z(G)$，显然有 $N \lhd G$。此时，G/N 是一个阶为 $p^{a-1}m$ 的群。根据归纳假设，我们可以找到 G/N 的西罗 p-子群，记作 $H' \subset G/N$，其中 $|H'| = p^{a-1}$。我们只须构造出群 G 的一个阶为 p^a 的子群。

令 H 是 H' 在典范满同态 $a \mapsto aN$ 的原像。

显然，当我们将典范满同态限制在 H 上时，就到了一个满同态 $f : H \to H'$，定义为 $a \mapsto aN$，它的核是

$$\ker(f) = \{h \in H : h \in N\}$$

即 $\ker(f) = N$。

利用群同构第一定理，我们有

$$\frac{|H|}{|N|} = |H'|$$

换言之，$|H| = p \cdot p^{a-1} = p^a$。这就证明了 p 整除 $|Z(G)|$ 的情形。

接下来，假设 p 不整除 $|Z(G)|$，可是 p 整除 $|G|$。利用类方程，我们有

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

因此，存在一个 i，使得 p 不整除 $[G : C_G(x_i)]$，也就是不整除 $|G|/|C_G(x_i)|$，因此 $|C_G(x_i)|$ 中 p 的幂次等于 a。若 $|C_G(x_i) = G$，则 G 中每个元素都与 x_i 交换，但这是不可能的，因为 $x_i \notin Z(G)$。因此，$|C_G(x_i)| < |G|$。利用归纳假设，我们可以找到一个阶为 p^a 的子群，这个子群同时也是 G 的一个西罗 p-子群。

此即得证。

命题 1.12 (西罗第二定理)

令 G 是一个有限群，若素数 p 整除 $|G|$，则任意两个西罗 p-子群都是共轭的。

证明 令 P 是一个西罗 p-子群。令 $S = \{gPg^{-1} : g \in G\}$，即由所有与 P 共轭的子群所构成的集合。考虑 G 在 S 上的共轭作用，这显然是良定义的。

利用共轭子群的知识，我们知道

$$|S| = [G : N_G(P)]$$

我们已经证明过 P 是 $N_G(P)$ 的正规子群。现在，P 是一个西罗 p-子群，又因为 $|P|$ 整除 $|N_G(P)|$，所以 p 不整除 $|S|$。

现在，令 Q 是任意的西罗 p-子群，我们只须证明 $Q \in S$。

同理，我们知道 Q 在 S 上也有共轭作用。我们将 S 拆成轨道的无交并，因此

$$|S| = \sum_{i=1}^{m} |\operatorname{Orb}(P_i)|$$

其中 P_i 是某个 $g_iPg_i^{-1}$。考虑到 p 不整除 $|S|$，所以 p 至少不整除某一个 $|\operatorname{Orb}(P_i)|$。利用轨道稳定化子定理，我们知道 $|\operatorname{Orb}(P_i)|$ 必须整除 $|Q|$，而 Q 是个西罗 p-子群，所以 $|\operatorname{Orb}(P_i)| = 1$。换言之，对任意 $q \in Q$，我们都有 $qP_iq^{-1} = P_i$。因此 $Q < N_G(P_i)$。

要证明 $Q \in S$，我们只须证明 $Q = P_i$，注意到它们的阶相等，所以只须证明 $Q < P_i$。

注意到 P_i 是 $N_G(P_i)$ 的一个正规子群，而 P_i 同构于 P，所以 p 不整除 $|N_G(P_i)/P_i|$。

考虑限制到 $Q < N_G(P_i)$ 上的典范同态 $f : a \mapsto aP_i$。现在，$Q - \{e\}$ 中元素的阶都能被 p 整除，任取 $a \in Q - \{e\}$，我们有 $(f(a))^{|a|} = 1$，然而 $f(a)$ 在 $N_G(P_i)$ 中，$N_G(P_i)$ 的阶不能被 p 整除，因此 $f(a)$ 的阶一定是 1，所以 $f(a) = e'$。这就告诉我们 f 是一个平凡同态，换言之，$Q \subset P_i$。

由于 Q 和 P_i 的阶相等，这就证明了 $Q < P_i$。此即得证。

为了证明西罗第三定理，我们先讲一个引理。

引理 1.11

令 G 是一个有限群，若素数 p 整除 $|G|$，P 是一个西罗 p-子群，Q 是一个 p-子群，则 $Q \cap P = Q \cap N_G(P)$。♡

证明 我们已经证明过，$P \lhd N_G(P)$，所以显然 $Q \cap P < Q \cap N_G(P)$。我们只须证明 $Q \cap N_G(P) \subset Q \cap P$。

类似地，我们考虑限制在 $Q \cap N_G(P)$ 的典范同态 $f : a \mapsto aP$。我们知道 $Q - \{e\}$ 中的每个元素的阶都能 p 整除，而 $N_G(P)/P$ 的阶不能被 p 整除。同理，我们就可以证明 f 是一个平凡同态。换言之，$Q \cap N_G(P) \subset P$。显然，又因为 $Q \cap N_G(P) \subset Q$，我们有 $Q \cap N_G(P) \subset Q \cap P$。

此即得证。

命题 1.13 (西罗第三定理)

令 G 是一个有限群，若素数 p 整除 $|G|$，则 $n_p \equiv 1 (\bmod 1)$。♠

证明 令 $S = \{P_1, \cdots, P_m\}$ 是由所有的西罗 p-子群所构成的集合，利用西罗第二定理，我们知道它们是两两共轭的。

类似地，考虑 P_1 在 S 的共轭作用。显然，$|\operatorname{Orb}(P_1)| = 1$，因为对任意 $a \in P_1$，我们有 $aP_1 = P_1 = P_1a$。

现在，令 $2 \le i \le m$，我们只须证明 $|\operatorname{Orb}(P_i)|$ 能被 p 整除。利用上面的引理，我们首先求出

$$\operatorname{Stab}(P_i) = \{g \in P_1 : gP_ig^{-1} = P_i\} = P_1 \cap N_G(P_i) = P_1 \cap P_i$$

此外，利用轨道正规化子定理，我们知道 $|\operatorname{Orb}(P_i)| = |P_i|/|P_1 \cap P_i|$。

显然，根据定义，$P_1 \ne P_i$，所以 $P_1 \cap P_i$ 的阶会小于 P_i 的阶。因此 $|\operatorname{Orb}(P_i)|$ 不能等于 1，所以 $|\operatorname{Orb}(P_i)|$ 一定能被 p 整除。

现在，对于任意的 $2 \le i \le m$，我们都有 $|\operatorname{Orb}(P_i)|$ 能被 p 整除。因此，$n_p \equiv 1 (\bmod p)$。

此即得证。

我们来看一个西罗定理的一个简单应用。

引理 1.12

令 G 是一个有限群，假设 $|G| = pq$，其中 $p < q$ 是两个素数，则 G 有唯一的 q 阶子群，因此是一个正规子群。♡

证明 利用西罗定理，我们知道 $n_q \equiv 1 (\bmod q)$，以及 $n_q | p$，我们只须证明 $n_q = 1$，因为这样的话，与这个唯一的西罗 q-子群共轭的子群只有它自己，就证明了它是一个正规子群。

注意到 $n_q = 1$ 或 q。假设 $n_q = p$，则 $q | (p-1)$，所以 $q \le p - 1 < p$，可是 $p < q$，这是不可能的。

此即得证。

1.3 群的半直积与小阶群

在讲半直积前，我们先来看直积的一个性质。

引理 1.13

令 G 是一个群，若 H, K 都是 G 的正规子群，并且 $H \cap K = \{e\}$，则 H 中的所有元素都和 K 中的所有元素交换。

证明 令 $h \in H$，$k \in K$，我们只须证明 $hkh^{-1}k^{-1} = e$。

注意到 $hkh^{-1} \in K$，所以 $hkh^{-1}k^{-1} \in K$。同理，因为 $kh^{-1}k^{-1} \in H$，所以 $hkh^{-1}k^{-1} \in H$。因为 $H \cap K = \{e\}$，所以 $hkh^{-1}k^{-1} = e$。

此即得证。

引理 1.14

若 $G = HK$，其中 H, K 都是 G 的正规子群，并且 $H \cap K = \{e\}$，则 $G \simeq H \times K$。

证明 我们只须构造出一个从 $H \times K$ 到 HK 的同构。

令 $(h, k) \in H \times K$，我们定义 $f(h, k) = hk$。

这是一个同态，因为对任意 $(h, k), (h', k') \in H \times K$，我们有 $hkh'k' = hh'kk'$。

由于 $G = HK$，我们知道这是一个满射。

接着，假设 $hk = h'k'$，其中 $h, h' \in H$，$k, k' \in K$，我们只须证明 $h = h', k = k'$。而这是因为 $h'h^{-1} = k'k^{-1}$。等号两边分别在 H 和 K 中，这就告诉我们 $h'h^{-1} = k'k^{-1} = e$，换言之，$h = h', k = k'$。

综上所述，$(h, l) \mapsto hk$ 给出了一个从 $H \times K$ 到 HK 的同构。此即得证。

在实践中，我们常常遇到的情形是 $G = NH$，其中 N 是一个正规子群，H 是一个子群，并且 $N \cap H = \{e\}$。

定义 1.10

令 G 是一个群。假设 $N \lhd G$，$H < G$，$G = NH$，$N \cap H = \{e\}$，则我们称 G 是 N 和 H 的一个半直积，记作 $G = N \rtimes H$。

注 一般来说，半直积是不唯一的。例如 $\mathbb{Z}_3$ 和 $\mathbb{Z}_2$ 的半直积既可以是 $\mathbb{Z}_6$，也可以是对称群 S_3。

我们迫切地想要知道，在得知了满足上面条件的 N, H 以后，如何求出所有可能的半直积。

对此，我们有一个极为巧妙的命题。

命题 1.14

令 G 是一个群。假设 $N \lhd G$，$H < G$，$G = NH$，$N \cap H = \{e\}$，则 N 和 H 的半直积由 H 在 N 的共轭作用唯一确定。

证明 对任意 $h \in H$，由于 N 是一个正规子群，我们知道 ϕ_g 是良定义的（这是因为 $hNh^{-1} = N$）。显然，$\phi : H \to \mathrm{Aut}(N)$ 是一个从 H 到 N 的共轭作用。

现在，对于上述的共轭作用 $\phi : N \to \mathrm{Aut}(N)$，我们在二元群对 (N, H) 上定义一个群的结构（一般而言不是直积的结构）。

对任意 $(n, h), (n', h') \in (N, H)$，我们定义

$$(n, h)(n', h') = (n\phi_h(n), hh')$$

这是一个良定义的映射，因为 $\phi_h(n) \in N$。

这个乘法满足结合律，因为若 $(n,h),(n',h'),(n'',h'')\in(N,H)$，则

$$((n,h)(n',h'))\,(n'',h'')=(n\phi_h(n'),hh')\,(n'',h'')=(n\phi_h(n')\phi_{hh'}(n''),hh'h'')=(n\phi_h(n')\phi_h(n')\phi_h(\phi_{h'}(n'')),hh'h'')$$
$$(n,h)\,((n',h')(n'',h''))=(n,h)\,(n'\phi_{h'}(n''),h'h'')=(n\phi_h\left(n'\phi_{h'}(n'')\right),hh'h'')=(n\phi_h\left(n'\phi_{h'}(n'')\right),hh'h'')$$

这个乘法的单位元是 (e,e)，因为对任意 $(n,h)\in N\times H$，我们有

$$(n,h)(e,e)=(n\phi_h(e),he)=(n,h)$$
$$(e,e)(n,h)=(e\phi_e(n),eh)=(n,h)$$

(n,h) 的乘法逆元是 $\left(\phi_{h^{-1}}\left(n^{-1}\right),h^{-1}\right)$，因为

$$(n,h)\left(\phi_{h^{-1}}\left(n^{-1}\right),h^{-1}\right)=\left(n\phi_h\left(\phi_{h^{-1}}\left(n^{-1}\right)\right),hh^{-1}\right)=\left(nn^{-1},e\right)=(e,e)$$
$$\left(\phi_{h^{-1}}\left(n^{-1}\right),h^{-1}\right)(n,h)=\left(\phi_{h^{-1}}\left(n^{-1}\right)\phi_{h^{-1}}(n),h^{-1}h\right)=(e,e)$$

这样，我们就证明了 (N,H) 是一个群。

现在，我们只须证明 $G\sim(N,H)$。

类似地，对于任意 $n\in N$，$h\in H$，由于 $G=NH$，我们定义 $f(nh)=(n,h)$。

我们先证明 f 是个良定义的映射。假设 $nh=n'h'$，则显然 $n=n',h=h'$。

f 是一个同态，因为 f 将 G 中的乘法映到了 (N,H) 中的乘法。

f 是一个满同态，因为 (N,H) 从集合的角度来看就是 $N\times H$。

f 是一个单同态，因为如果 $(n,h)=(n',h')$，则从集合或元素的角度来看，我们有 $n=n',h=h'$。

此即得证。

1.4 群的阿贝尔化

我们先定义交换子。

定义 1.11

令 G 是一个群，则 a,b 的交换子指的是 $[a,b]=aba^{-1}b^{-1}$。♣

显然，a,b 交换当且仅当 $[a,b]=e$。

在阿贝尔群中，任意两个元素都交换，所以任意两个元素的交换子都是 e，

我们来定义一个群的换位子群。

定义 1.12

令 G 是一个群，则 G 的换位子群，记作 $[G,G]$，指的是由 $\{[a,b]:a,b\in G\}$ 生成的正规子群。♣

根据定义，G 的换位子群是包含了交换子的最小的正规子群。

现在，我们定义群的阿贝尔化。

定义 1.13

令 G 是一个群，则群 G 的阿贝尔化，记作 G^{ab}，指的是 $G^{\mathrm{ab}}=G/[G,G]$。♣

注 我们可以将 G 阿贝尔化的过程，就是将所有 $ab=ba$ 的关系加到了 G 中的过程。

注 我们记 $x\mapsto x[G,G]$ 的典范满同态为 π。

命题 1.15

令 G 是一个群，则群 G 的阿贝尔化是一个阿贝尔群。

证明 令 $a[G,G], b[G,G] \in G/[G,G]$，我们只须证明 $ab[G,G] = ba[G,G]$，而这是因为

$$(ab)(ba)^{-1} = aba^{-1}b^{-1} = [a,b] \in [G,G]$$

此即得证。

一个群的阿贝尔化满足一个重要的性质。

命题 1.16

令 G 是一个群，而 A 是一个阿贝尔群，则对于任意的群同态 $f : G \to A$，都能找到唯一的群同态 $\overline{f}$: $G^{\mathrm{ab}} \to A$，使得 $f = \overline{f} \circ \pi$。

证明 先证存在性。令 $f : G \to A$ 是一个群同态。我们只须定义 $\overline{f} : G^{\mathrm{ab}} \to A$。假设 $a \in G$，我们定义

$$\overline{f}(a[G,G]) = f(a)$$

我们先证明 $\overline{f}$ 是良定义的。假设 $a[G,G] = b[G,G]$，我们有 $a^{-1}b \in [G,G]$，我们只须证明 $f\left(a^{-1}b\right) = e'$。根据 $[G,G]$ 的定义，它是由所有交换子所生成的正规子群。任取 $[x,y] = xyx^{-1}y^{-1}$，我们有 $f([x,y]) = f\left(xyx^{-1}y^{-1}\right) = f(x)f(y)f(x)^{-1}f(y)^{-1}$。因为 A 是一个阿贝尔群，所以 $f([x,y]) = e$。因此，$[G,G]$ 中的每个元素在 f 下的像都是 e'，于是 $f\left(a^{-1}b\right) = e'$，这就证明了 $\overline{f}$ 是良定义的。

我们再证明 $\overline{f}$ 是一个群同态。令 $a, b \in G$，我们只须证明 $\overline{f}(ab[G,G]) = \overline{f}(a[G,G])\overline{b[G,G]}$，而这是显然的，因为利用 f 的同态性，我们有

$$f(ab) = f(a)f(b)$$

我们还要证明 $f = \overline{f} \circ \pi$。但是根据 $\overline{f}$，这是显然的（因为我们就是这样定义 $\overline{f}$ 的）。

再证唯一性。假设 $g : G^{\mathbf{ab}} \to A$，使得 $f = g \circ \pi$，则对任意 $a \in G$，都有 $f(a) = g(a[G,G])$，而这就证明了 $g = \overline{f}$。

综上所述，我们就证明了这个命题。在范畴论中，我们可以用伴随函子来论述这个命题。

现在，我们快速介绍交换子的三个性质。

引理 1.15

令 $f : G \to G'$ 是一个群同态，$a, b \in G$，则

1. $f([a,b]) = [f(a), f(b)]$。
2. $[a,b]^{-1} = [b,a]$。
3. 令 $g \cdot a$ 表示共轭作用 $g \cdot a = gag^{-1}$，则 $g \cdot [a,b] = [g \cdot a, g \cdot b]$。

证明

1. 第一点在刚才的证明中已经出现了，我们不再赘述。
2. 通过直接的计算可得 $[a,b]^{-1} = \left(aba^{-1}b^{-1}\right)^{-1} = bab^{-1}a^{-1} = [b,a]$。
3. 通过直接的计算可得

$$g \cdot [a,b] = gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = [g \cdot a][g \cdot b][g \cdot a]^{-1}[g \cdot b]^{-1} = [g \cdot a, g \cdot b]$$

此即得证。

换位子群还有一个重要的性质：$[G,G]$ 是 G 中最小的使得商群 G/N 是个阿贝尔群的正规子群 N。我们用下面的命题来描述这个性质。

命题 1.17

令 G 是一个群，而 $N \lhd G$，则 G/N 是个阿贝尔群当且仅当 $[G,G] \subset N$。

证明 先证充分性。假设 $N \lhd G$，使得 G/N 是个阿贝尔群。要证明 $[G,G] \subset N$，利用 $[G,G]$ 的定义，我们只须证明 G 的所有交换子都在 N 中。令 $a,b \in g$，我们只须证明 $[a,b] = aba^{-1}b^{-1} \in N$。

注意到 G/N 是个阿贝尔群，所以 $abN = baN$，因此 $(ab)(ba)^{-1} = aba^{-1}b^{-1} \in N$。换言之，$[a,b] = aba^{-1}b^{-1} \in N$。这就证明了 $[G,G] \subset N$。

再证必要性。若 $[G,G] \subset N$，注意到 $[G,G]$ 和 N 都是 G 的正规子群，因此根据群同构第三定理，我们知道

$$(G/[G,G])/(N/[G,G]) \simeq G/N$$

由于 $G/[G,G]$ 是个阿贝尔群，而阿贝尔群的每一个商群都是阿贝尔群，所以 G/N 也是一个阿贝尔群。

此即得证。

1.5 可解群

这一节的内容主要参考了 Serge Lang 的 GTM 211。

我们先定义子群列、正规列、阿贝尔列与循环列。

在有的书中，例如子群列和降子群列是分开定义的，为了方便，我们在语境合适的情况下忽略它们的区别。

定义 1.14

一个子群列指的是形如

$$G = G_0 > G_1 > \cdots > G_m$$

的子群的序列，满足显然的子群关系。

定义 1.15

一个正规列指的是形如

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_m$$

的子群的序列，其中相邻两项满足正规子群的关系。

注 注意，一般来说，若 $M \lhd N$，$N \lhd G$，我们是不能得到 $M \lhd G$ 的。也就是说，这里的正规子群的关系不具有传递性。

定义 1.16

一个正规列指的是形如

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_m$$

的子群的序列，其中相邻两项满足正规子群的关系。

定义 1.17

一个阿贝尔列指的是形如

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_m$$

的子群的序列，其中任意两项的商群 G_i/G_{i-1} 都是阿贝尔群。

定义 1.18

一个阿贝尔列指的是形如

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_m$$

的子群的序列，其中任意两项的商群 G_i/G_{i-1} 都是循环群。

由于循环群一定是阿贝尔群，所以我们很容易发现，每一个循环列都是阿贝尔列，每一个阿贝尔列都是正规列，每一个正规列都是子群列。也就是说，我们上面介绍的条件是越来越强的。

命题 1.18

假设 $f : G \to G'$ 是一个群同态，则子群列的原像依然是一个子群列。

证明 利用显然的数学归纳法，我们只须证明，若 $H' < G'$，则 $f^{-1}(H') < G$。

一方面，因为 $e' \in H'$，以及 $f(e) = e'$，所以 $e \in f^{-1}(H')$。

现在，假设 $x, y \in f^{-1}(H')$，我们只须证明 $xy^{-1} \in f^{-1}(H')$，而这是因为

$$f\left(xy^{-1}\right) = f(x)f(y)^{-1} \in H'$$

最后一个等号是因为 H' 是一个子群。

这样，我们就证明了 $f^{-1}(H') < G = f^{-1}(G')$。

此即得证。

我们还可以证明一个有趣的性质。

命题 1.19

假设 $f : G \to G'$ 是一个群同态，且

$$G' = G'_0 \rhd G'_1 \rhd \cdots \rhd G'_m$$

是 G' 的一个正规列，则对任意 $1 \le i \le m$，存在一个从 $f^{-1}(G_{i-1})/f^{-1}(G_i)$ 到 G'_{i-1}/G'_i 的嵌入（单同态）。

证明 为了方便，令 $G_i = f^{-1}(G_i)$。

我们先证明正规列的原像依然是一个正规列。利用显然的数学归纳法，我们只须证明若 $N' \lhd G'$，则 $f^{-1}(N') \lhd G$。

利用上一个命题，我们已经知道 $f^{-1}(N') < G$，因此我们只须证明正规性。令 $g \in G$，$a \in f^{-1}(N')$，因此 $f(a) \in N'$。我们只须证明 $gag^{-1} \in f^{-1}(N')$，而这是因为

$$f\left(gag^{-1}\right) = f(g)f(a)f(g)^{-1} \in N'$$

最后一个属于关系是根据 N' 的正规性。

令 $1 \le i \le m$。现在，我们当然定义 $\overline{f_i} : G_{i-1}/G_i \to G'_{i-1}/G'_i$ 为

$$\overline{f_i}(aG_i) = f(a)G'_i$$

$\overline{f_i}$ 是良定义的，因为 $f(G_i) = G'_i$。

$\overline{f_i}$ 是个群同态，因为本质上 f 是一个群同态。

我们只须证明 $\overline{f_i}$ 是一个单射。假设 $\overline{f_i}(aG_i) = G'_i$，则根据定义，我们有 $f(a)G'_i = G'_i$，换言之，$f(a) \in G'_i$，也即 $a \in G_i = f^{-1}(G'_i)$（这是根据 G_i 的定义）。

此即得证。

下面，我们定义子群列的改良和单群。

定义 1.19

子群列的改良，指的是在子群列中插入一些子群，接着满足显然的子群关系。

注 显然，对任意一个群 G，我们都有 $G \triangleright \{e\}$。单群指的是无法改良这个子群列的群 G。

定义 1.20

令 G 是一个群，则 G 是一个单群当且仅当正规子群列

$$G \triangleright \{e\}$$

没有非平凡的改良。

在伽罗瓦理论中，我们有一个极为重要的概念，称为可解群。我们在这里也一并引入。

定义 1.21

令 G 是一个群，G 被称为一个可解群当且仅当存在一个从 G 到 $\{e\}$ 的阿贝尔列

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{e\}$$

注 可解群的定义中的重点有两个，一是这个子群列是从 G 一直到 $\{e\}$ 的，另一个是这个子群列是阿贝尔列，换言之任意相邻子群间有正规子群关系，并且对应的商群都是阿贝尔群。

阿贝尔列和循环列有什么关系呢？显然，循环列都是阿贝尔列。事实上，在有限群中，每一个阿贝尔列都有一个循环列的改良。这就是我们要证明的下一个命题。

命题 1.20

令 G 是一个有限群。假设 G 有一个阿贝尔列，那么这个阿贝尔列有一个循环列的改良。

证明 我们只须证明，若 G 是个有限阿贝尔群，则存在一个从 G 到 $\{e\}$ 的循环列。

用数学归纳法。假设 $|G| = 1$，则是显然的。

假设对 $|G| < n$ 都成立，令 $|G| = n$。任取 $x \in G - \{e\}$。令 $N = \langle x \rangle$。因为 G 是一个阿贝尔群，所以 $N \triangleleft G$。显然 G/N 是个有限阿贝尔群。利用归纳假设，我们有一个从 G/N 到 $\{eN\}$ 的循环列。取这个循环列的原像，我们就得到了一个从 G 到 N 的循环列，最后再加上从 N 到 $\{e\}$ 的平凡同态，我们就得到了一个从 G 到 $\{e\}$ 的循环列，因为 N 是个循环群。

根据这个命题，我们有一个显然的推论，那就是每一个有限可解群有一个从 G 到 $\{e\}$ 的循环列。

引理 1.16

假设 G 是一个有限可解群，则存在一个从 G 到 $\{e\}$ 的循环列。

证明 可解群就是说存在一个从 G 到 $\{e\}$ 的阿贝尔列。利用上一个命题，我们可以将其改良为一个从 G 到 $\{e\}$ 的循环列。

此即得证。

下一个命题是描述可解群和正规子群的关联。

命题 1.21

令 G 是一个群，而 N 是一个正规子群。则 G

1.6 对称群与交错群

在群论 I 的讨论中，我们略去了一个重要的群，那就是对称群。

定义 1.22

令 $n \in \mathbb{N}_1$，则对称群 S_n，定义为

$$S_n = \{\sigma : \{1, \cdots, n\} \to \{1, \cdots, n\} : \sigma\text{是双射}\} \tag{1.1}$$

对称群 S_n 中的每一个元素，我们称为 $\{1, \cdots, n\}$ 的一个置换，简称为一个置换。

显然，利用双射的性质，对称群在复合运算下构成一个群。

命题 1.22

令 $n \in \mathbb{N}_1$，则对称群 S_n，在复合下构成一个群。

证明 这是自明的。我们留给感兴趣的读者作为练习。S_n 中的单位元是恒等映射，即将 $\{1, \cdots, n\}$ 中的每个元素映到自身的那个双射，我们记恒等映射为 id_n，简记为 id。

如何表示 S_n 中的一个置换呢？我们有两种方法。第一种方法是写成两行的一个矩阵，其中第一行是从 1 到 n 的数字，第二行是对应的 $\sigma(i)$。

定义 1.23

令 $\sigma \in S_n$，则我们形式地将 σ 记作

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix} \tag{1.2}$$

很显然，一个写成这样形式的映射是一个置换，当且仅当第二行的数字取遍了 $1, \cdots, n$，是两两不同的数字。因为映射的复合是从右到左计算的，因此我们采用的规则是从右到左进行置换的复合运算。实际上，也有一种约定是从左到右计算。正如自然数集是否包含 0 并没有广泛的共识，置换的乘积也没有“正确”的顺序。在这本教材中，我们按照映射的本质，一概约定从右到左计算。

下面我们举一个例子。

练习 1.1 求证

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \tag{1.3}$$

证明 只须看 1, 2, 3 分别被映射到哪里去了即可。在右边的置换中，1 被映射到了 2；在左边的置换中，2 又被映射到了 3。因此，这两个置换的乘积，就将 1 映射到了 3，所以我们在 1 的下面写 3。同理，我们也可以得到 2 和 3 分别被映射到了 2 和 1。

下面，我们讲一个简单的引理，那就是每一个较小的对称群都可以嵌入到一个较大的对称群。

引理 1.17

令 $m \leqslant n$ 是两个正整数，则 S_m 可以被嵌入到 S_n 中，即存在一个单同态 $f : S_m \to S_n$。

证明 对于任意 $\sigma \in S_m$，我们想要定义 $f(\sigma) \in S_n$，而这就需要对任意 $i \in \{1, \cdots, n\}$，给出 $f(\sigma)(i)$ 的定义。我们是这么定义的。

如果 $1 \leqslant i \leqslant m$，我们定义 $f(\sigma)(i) = \sigma(i)$。如果 $m+1 \leqslant i \leqslant n$，我们定义 $f(\sigma)(i) = i$ 自身。

也就是说，我们将一个 m 个元素的置换视作一个 n 个元素的置换的一种方法，就是将其视为前 m 个元素的置换，而后 $n-m$ 个元素的恒等置换。

要证明 f 是个同态，只须对 i 分两类情况讨论。若 $i \leqslant m$，那么利用 S_n 是个群的条件即可；若 $i > m$，那么恒等映射显然会给出同态。

要证明 f 是个单射，只须证明它的核是平凡的，即 $\ker(f) = \{id\}$。那么，如果 $f(\sigma) = id$，显然后 $n-m$ 个单位是映到自身的，而且前 m 个元素，在 σ 下也要映到自身。这就迫使 $\sigma = id_m = id$。

综上所述，我们就证明了若 $m < n$ 是两个正整数，就存在一个从 S_m 到 S_n 的单同态，即 S_m 可以嵌入到 S_n 中。

我们有一类重要的置换，称为循环置换。

定义 1.24

令 $x_1, \cdots, x_m \in \{1, \cdots, n\}$ 是两两不同的元素，我们下面定义 $(x_1 \cdots x_m) \in S_n$。

1. 对 $1 \le i \le m-1$，我们定义 $(x_1 \cdots x_m)(x_i) = x_{i+1}$，而 $(x_1 \cdots x_m)(x_m) = x_1$。
2. 对于 $\{1, \cdots, n\}$ 中的其它元素 y，我们定义 $(x_1 \cdots x_m)(y) = y$。

♣

现在，我们叙述循环置换的性质。

引理 1.18

$(x_1 \cdots x_m)^k$ 将每一个 x_i 映到 $x_{i+k(\bmod m)}$。特别地，循环置换 $(x_1 \cdots x_m)$ 的阶是 m。

♡

证明 因为 $(x_1 \cdots x_m)$ 将每一个 x_i 映到 $x_{i+1(\bmod m)}$。利用数学归纳法，显然我们有 $(x_1 \cdots x_m)^k$ 将每一个 x_i 映到 $x_{i+k(\bmod m)}$。

特别地，$(x_1 \cdots x_m)^k$ 将 x_1 映到 $x_{1+k(\bmod m)}$。由于 $x_1, \cdots, x_m$ 是两两不同的，所以对任意的 $1 \le k \le m-1$，$(x_1 \cdots x_m)^k$ 都不等于恒等置换 id。

现在，当 $k = m$ 时，我们有 $i + m \equiv i(\mathrm{mod} m)$，$(x_1 \cdots x_m)^k$ 将每一个 x_i 映到 $x_{i+m(\bmod m)} = x_i$。

这样，我们就证明了 $(x_1 \cdots x_m)$ 的阶是 m。

命题 1.23

令 $(x_1 \cdots x_m)$，$(y_1 \cdots y_l)$ 是 S_n 中的两个置换，则 $(x_1 \cdots x_m) = (y_1 \cdots y_l)$ 当且仅当 $m = l$，并且存在一个 $0 \le k \le m-1$，使得 $y_i = x_{i+k(\bmod m)}$。

♠

证明 先证充分性。假设 $(x_1 \cdots x_m) = (y_1 \cdots y_l)$，则同时取元素的阶，我们得到了 $m = l$。在两个置换中，那些不被映到自身的元素恰好是 $x_1, \cdots, x_m$ 与 $y_1, \cdots, y_m$，因此一定存在一个这些元素间的双射。我们假设 $y_{i_j} = x_j$，则必须有 $y_{i_{j+1(\bmod m)}} = x_{j+1(\bmod m)}$，因此 $j \mapsto i_j$ 是一个 $\mathbb{Z}_m$ 上的一个平移。换言之，存在 $0 \le k \le m-1$，使得 $y_i = x_{i+k(\bmod m)}$。

再证必要性。假设 $m = l$，且存在 $0 \le k \le m-1$，使得 $y_i = x_{i+k(\bmod m)}$。那么

$$(x_1 \cdots x_m) = (x_{1+k(\bmod m)} \cdots x_{m+k(\bmod m)}) = (y_1 \cdots y_m)$$

此即得证。

对于 S_n 上一般的置换，我们有一个重要的分解，那就是将其分解为循环置换的乘积。

命题 1.24

令 $\sigma \in S_n$，则存在唯一彼此无交的循环置换 σ_1, σ_m，使得 $\sigma = \sigma_1 \circ \circ \cdots \circ \sigma_m$。

♠

证明

1.7 二面体群

1.8 幂零群

1.9 有限生成阿贝尔群

1.10

1.11

第 2 章 模论

2.1 向量空间

我们先复习向量空间的定义。

定义 2.1

令 k 是一个域，我们称 V 是 k 上的一个向量空间当且仅当存在向量加法 $+: V \times V \to V$ 以及标量乘法 $\cdot: k \times V \to V$，使得 $(V, +)$ 是个阿贝尔群，并且对任意 $a, b \in k$ 以及 $v, w \in V$，我们有

1. $1v = v$。
2. $(a+b)v = av + bv$。
3. $a(v+w) = av + aw$。
4. $a(bv) = (ab)v$。

♣

由于阿贝尔群有四条性质，所以加上标量乘法的四条性质，向量空间一共有八条性质，或者说八个公理。更多关于向量空间的知识，我们实际上在抽象代数 I 的域论那一章中已经复习过了。我们不再赘述。

2.2 模与子模

下面，我们给出模的定义。

定义 2.2

令 R 是一个环，我们称 M 是 R 上的一个左模，或 M 是一个 R-左模当且仅当存在加法 $+: M \times M \to M$ 以及标量乘法 $\cdot: R \times M \to M$，使得 $(M, +)$ 是个阿贝尔群，并且对任意 $a, b \in R$ 以及 $v, w \in M$，我们有

1. $1v = v$。
2. $(a+b)v = av + bv$。
3. $a(v+w) = av + aw$。
4. $a(bv) = (ab)v$。

♣

对称地，我们可以定义一个环上的右模。

定义 2.3

令 R 是一个环，我们称 M 是 R 上的一个左模，或 M 是一个 R-右模当且仅当存在加法 $+: M \times M \to M$ 以及标量乘法 $\cdot: M \times R \to M$，使得 $(M, +)$ 是个阿贝尔群，并且对任意 $a, b \in R$ 以及 $v, w \in M$，我们有

1. $v1 = v$。
2. $v(a+b) = va + vb$。
3. $(v+w)a = va + wa$。
4. $(va)b = v(ab)$。

♣

定义 2.4

若 R 是一个交换环，则左模和右模等价，我们简称为模。

♣

注 因此，当我们说 M 是一个 R-模的时候，我们暗示了 R 是一个交换环。

例题 2.1 显然，向量空间就是域上的模。

下面，我们证明阿贝尔群就是整数环上的模。

引理 2.1

阿贝尔群和整数环上的模是一一对应的。

证明 令 $(G,+)$ 是一个阿贝尔群，对任意 $n\in\mathbb{Z}$ 和 $x\in G$，我们定义 $n\cdot x=nx$。换言之，若 $m\in\mathbb{N}_1$，则我们定义 $m\cdot x=x+\cdots+x$，$0\cdot x=0$，$(-m)\cdot x=(-x)+\cdots+(-x)=-(m\cdot x)$。

利用群论的知识，我们很容易证明 G 在上面的定义下是一个 $\mathbb{Z}$-模。

反过来，若 $(G,+)$ 是一个 $\mathbb{Z}$-模，则 $(G,+)$ 显然是一个阿贝尔群。

此即得证。

我们来举一些例子。

例题 2.2 令 R 是一个环，则对任意 $n\in\mathbb{N}_1$，R^n 是一个 R-左模。

证明 显然，R^n 是一个环，特别地，$(R^n,+)$ 是一个阿贝尔群。对任意 $r\in R$ 和 $(r_1,\cdots,r_n)\in R^n$，我们定义 $r\cdot(r_1,\cdots,r_n)=(rr_1,\cdots,rr_n)$。利用环的性质，显然 R^n 在自身的加法和这样的标量乘法下构成一个 R-左模。

此即得证。

注 同理，我们可以证明对任意 $n\in\mathbb{N}_1$，R^n 是一个 R-右模。

特别地，每一个环都是它自己的左模以及右模。更特别地，每一个交换环都是它自己的模。

下面，我们定义子模。

定义 2.5

令 M 是一个 R-左模。我们称 $N\subset M$ 是一个 M 的一个子模，记作 $N<M$，当且仅当 N 在限制下的加法和标量乘法下构成一个 R-左模。

我们同样有子模的判别准则，这和子空间的判别准则是一致的。

引理 2.2

令 M 是一个 R-左模，则 $\emptyset\neq N\subset M$ 是一个 M 的一个子模当且仅当

1. 对于任意的 $x,y\in N$，$x+y\in N$。
2. 对于任意的 $r\in R$ 和 $x\in N$，我们有 $rx\in N$。

证明 充分性是显然的，这就是良定义性。

下面，我们来证明必要性。良定义性显然得证了。模的后四条是显然的，因为都是由全称量词给出的命题。我们只须证明 $(N,+)$ 是 $(M,+)$ 的一个子群。

显然，N 对加法是封闭的，并且是非空的，我们只须证明 N 对逆元封闭，而这是因为 $-1\in R$，所以对任意 $x\in N$，我们有 $-x=(-1)\cdot x\in N$。

此即得证。

例题 2.3 将 R 视为一个 R-模，则 R 的子模就是 R 的理想。

证明 此时，$M=R$，标量乘法就是 R 中的乘法，显然，R 的子模就是 R 的理想。

注 这样，我们就用模的语言来描述出理想。换言之，我们在某种程度上可以认为模是理想的推广。当然，我们一般认为模是向量空间的推广，不过这是不唯一的，模论早已成为现代数学常用的代数语言，而这正是来自模的普遍性。

一如既往地，我们可以定义在一个模中，由子集生成的子模。

定义 2.6

令 M 是一个 R-左模，而 $\emptyset\neq S\subset M$，则由 S 生成的子模指的是

$$\langle S\rangle=\bigcap_{\substack{N<M\\ N\supset S}}N$$

我们当然要证明这样的 $\langle S\rangle$ 是一个子模。

引理 2.3

令 M 是一个 R-左模，而 $\emptyset \neq S \subset M$，则 $\langle S \rangle < M$。

证明 一方面，每一个这样的 N 都是包含了 S 的子群，所以利用群论的知识，我们知道 $\langle S \rangle$ 是 M 的加法子群。

剩下四条的检验是非常简单的，和抽象代数 I 的诸多证明没有任何本质区别。我们留给有兴趣的读者作为练习。

特别地，我们可以给出 $\langle S \rangle$ 的显式表达式。

引理 2.4

令 M 是一个 R-左模，而 $\emptyset \neq S \subset M$，则

$$\langle S \rangle = \{r_1x_1 + \cdots + r_nx_n : n \in \mathbb{N}_1, r_1, \cdots, r_n \in R, x_1, \cdots, x_n \in M\}$$

证明 我们令右侧的集合为 T。显然，$S \subset T$，因为对任意 $s \in S$，我们有 $s = 1s \in T$。

除此以外，我们可以证明 $T < M$。因为 S 是非空的，所以 T 也是非空的。加法和标量乘法的封闭性都是显然的。

现在，我们只须证明每一个包含了 S 的 M 的子模都会包含 T。令 N 是一个包含了 S 的 M 中子模。任取 $r_1, \cdots, r_n \in R$ 和 $x_1, \cdots, x_n \in M$，利用加法和标量乘法的封闭性，我们有当然有 $r_1x_1 + \cdots + r_nx_n \in N$，这就证明了 $N \supset T$。

综上所述，我们就证明了 $\langle S \rangle = T$。此即得证。

正如在一个向量空间中，由一个子向量空间就可以定义出一个商空间。在一个模中，由一个子模就可以定义出一个商模。

定义 2.7

令 M 是一个 R-模，而 $N < M$ 是一个子模，我们下面定义商模 M/N。

在阿贝尔群的意义下，我们首先定义 M/N 是 M 的 N 商群。下面，我们对任意 $r \in R$ 和 $xN \in M/N$，我们定义 $r(xM) = (rx)M$。

证明 我们要证明标量乘法是良定义的。假设 $xM = yM$，即 $x - y \in M$，我们只须证明 $rxM = ryM$，而这是因为 $rx - ry = r(x - y) \in M$。

这就证明了标量乘法是良定义的。

引理 2.5

令 M 是一个 R-模，而 $N < M$ 是一个子模，则商模 M/N 是一个 R-模。

证明 利用群论的知识，我们已经知道 M/N 对加法构成一个阿贝尔群。我们只须另外四条。令 $a, b \in R$，$x, y \in M$。

1. $1(xN) = (1x)N = xN$。
2. $(a + b)(xN) = ((a + b)x)N = axN + bxN = a(xN) + b(xN)$。
3. $a(xN + yN) = a((x + y)N) = (a(x + y))N = (ax + ay)N = axN + ayN = a(xN) = a(yN)$。
4. $a(b(xN)) = (a(bx)N) = (a(bx))N = ((ab)x)N = (ab)(xN)$。

此即得证。

2.3 模同态

在这里，我们介绍 R-左模同态。

定义 2.8

令 R 是一个环，而 M, M' 是两个 R-左模，则 $f: M \to M'$ 被称为一个 R-左模同态当且仅当

1. 对任意 $x, y \in M$，$f(x+y) = f(x) + f(y)$。
2. 对任意 $a \in R$ 以及 $x \in M$，我们有 $f(ax) = af(x)$。

换言之，f 保持了线性组合，或者说 f 保持了加法和标量乘法。

引理 2.6

令 R 是一个环，而 M, M' 是两个 R-左模，则 $f: M \to M'$ 是一个 R-左模同态当且仅当对任意 $a \in R$，$x, y \in M$，我们有 $f(ax+y) = af(x) + f(y)$。

证明 充分性和必要性都是显然的，这和我们在线性代数中学习的是一致的，我们留给感兴趣的读者作为练习。

注 类似地，我们可以定义出右模同态。

注 若 R 一个交换环，则 R-左模同态就是 R-右模同态，我们简称为 R-模同态。

例题 2.4 若 k 是一个域，则一个 k-模同态就是一个 k-线性变换。

例题 2.5 若 M 是一个 R-左模，而 $N < M$ 是一个子模，则典范映射 $\pi: M \to M/N$，定义为 $\pi(x) = xN$，是一个 R-左模同态。

证明 令 $a \in R$，$x, y \in M$，我们只须证明 $\pi(ax+y) = a\pi(x) + \pi(y)$，而这是因为

$$\pi(ax+y) = (ax+y)N = (ax)N + yN = a(xN) + yN = a\pi(x) + \pi(y)$$

此即得证。

现在，我们定义 R-模同构。

定义 2.9

令 R 是一个环，而 M, M' 是两个 R-左模，则 $f: M \to M'$ 是一个 R-左模同构当且仅当

1. f 是一个 R-左模同态。
2. f 是一个双射。

当然，我们要证明每一个左模同构的逆映射仍然是一个左模同态（进而是左模同构）。

引理 2.7

令 R 是一个环，而 M, M' 是两个 R-左模。假设 $f: M \to M'$ 是一个 R-左模同构，则 $f^{-1}: M' \to M$ 是一个 R-左模同态。

证明 从群论的角度来说，显然 f^{-1} 对加法构成一个同态。我们只须证明对任意 $r \in R$ 和 $x' \in M'$，我们都有 $f^{-1}(rx') = rf^{-1}(x')$。

由于 f 是一个双射，我们可以假设 $f(x) = x'$。因为 f 是一个 R-左模同态，我们有 $f(rx) = rf(x) = rx'$。反过来，我们就得到了 $f(rx') = rx = rf^{-1}(x')$。

此即得证。

显然，若 R 是一个环，则 R-左模同构给出了 R-左模上的一个等价关系。

当然，我们也有模同构的三定理。由于证明和群同构、环同构三定理是非常类似的，我们完全略去证明，留给感兴趣的读者作为练习。

命题 2.1 (模同构第一定理)

令 $f: M \to N$ 是一个 R-模同态，则 $\ker(f) = \{x \in M : f(x) = 0\}$ 是 M 的一个子模，并且 $M/\ker(f) \simeq \mathrm{im}(f)$。

命题 2.2 (模同构第二定理)

假设 N, L 是 R-模 M 的两个 R-子模，则 $N < N+L = \{x+y : x \in N, y \in L\}$，$N \cap L < L$，并且

$$(N+L)/N \simeq L/(N \cap L)$$

命题 2.3 (模同构第三定理)

假设 $L < N < M$ 是嵌套的 R-子模，则 $L < M$，$N/L < M/L$，并且

$$M/N \simeq (M/L)/(N/L)$$

下面，我们介绍 R-左模的直积与直和。

定义 2.10

令 I 是一个非空指标集，假设对于任意的 $i \in I$，M_i 都是一个 R-左模，我们下面定义这些 M_i 的直积，记作 $\prod_{i\in I} M_i$。对加法而言，$\prod_{i\in I} M_i$ 就是 $\{(M_i, +)\}_{i\in I}$ 的直积。下面，我们定义标量乘法。令 $r \in R$，$(x_i)_{i\in I} \in \prod_{i\in I} M_i$，我们定义 $r\,(x_i)_{i\in I} = (rx_i)_{i\in I}$。

引理 2.8

令 I 是一个非空指标集，假设对于任意的 $i \in I$，M_i 都是一个 R-左模，则它们的直积 $\prod_{i\in I} M_i$ 也是一个 R-左模。

证明 首先，利用群论的知识，我们知道 $\prod_{i\in I} M_i$ 对加法构成阿贝尔群。

我们只须证明余下四条。令 $a, b \in R$，$(x_i)_{i\in I}, (y_i)_{i\in I} \in \prod_{i\in I} M_i$。

1. $1\,(x_i)_{i\in I} = (1x_i)_{i\in I} = (x_i)_{i\in I}$。
2. $(a+b)\,(x_i)_{i\in I} = ((a+b)x_i)_{i\in I} = (ax_i + bx_i)_{i\in I} = (ax_i)_{i\in I} + (bx_i)_{i\in I} = a\,(x_i)_{i\in I} + b\,(x_i)_{i\in I}$。
3. $a\left((x_i)_{i\in I} + (y_i)_{i\in I}\right) = a\,(x_i+y_i)_{i\in I} = (a\,(x_i+y_i))_{i\in I} = (ax_i+ay_i)_{i\in I} = (ax_i)_{i\in I} + (ay_i)_{i\in I} = a\,(x_i)_{i\in I} + a\,(y_i)_{i\in I}$。
4. $a(b\,(x_i)_{i\in I}) = a\,(bx_i)_{i\in I} = (a\,(bx_i))_{i\in I} = ((ab)x_i)_{i\in I} = (ab)\,(x_i)_{i\in I}$。

此即得证。

下面，我们定义一族模的直和。

定义 2.11

令 I 是一个非空指标集，假设对于任意的 $i \in I$，M_i 都是一个 R-左模，我们下面定义这些 M_i 的直和，记作 $\bigoplus_{i\in I} M_i$。它是由 $\prod_{i\in I} M_i$ 中除了有限项外都是 0 的元素所构成的子集。

引理 2.9

令 I 是一个非空指标集，假设对于任意的 $i \in I$，M_i 都是一个 R-左模，则

$$\bigoplus_{i\in I} M_i < \prod_{i\in I} M_i$$

证明 由于 $(0)_{i\in I}$ 的每一位都是 0，所以当然属于 $\bigoplus_{i\in I} M_i$。

因此，我们只须证明 $\bigoplus_{i\in I} M_i$ 在加法和标量乘法下是封闭的。

令 $a \in R$，$(x_i)_{i\in I}, (y_i)_{i\in I} \in \bigoplus_{i\in I} M_i$，则除了有限项外的所有 x_i 和 y_i 都等于 0，因此，除了有限项外的所有 $x_i + y_i$ 都等于 0（如果 $x_i + y_i \neq 0$，那么至少有一个不等于 0，而这样的 x_i 或 y_i 的个数都是有限的），这就证明了

$$(x_i)_{i\in I} + (y_i)_{i\in I} \in \bigoplus_{i\in I} M_i$$

除此以外，由于除了有限项外的所有 x_i 都等于 0，因此显然有除了有限项外的所有 ax_i 都等于 0，这就证明

了

$$a\,(x_i)_{i\in I} \in \bigoplus_{i\in I} M_i$$

综上所述，我们就证明了集族 $\{M_i\}_{i\in I}$ 的直和是直积的子模。此即得证。

下面，我们来说明，若 M, N 是两个 R-模，则所有从 M 到 N 的模同态也构成一个模。

定义 2.12

令 M, N 是两个 R-模，我们定义 $\mathrm{Hom}(M, N)$ 是由所有从 M 到 N 的 R-模同态所构成的集合。若 $a \in R$，$f, g \in \mathrm{Hom}(M, N)$，则对任意 $x \in M$，我们定义

1. $(f+g)(x) = f(x) + g(x)$。
2. $(af)(x) = af(x)$。

♣

命题 2.4

若 M, N 是两个 R-模，则 $\mathrm{Hom}(M, N)$ 是一个 R-模。

♠

证明 我们首先证明加法和标量乘法是良定义的。令 $a \in R$，$f, g \in \mathrm{Hom}(M, N)$。我们只须证明 $f+g \in \mathrm{Hom}(M, N)$，$af \in \mathrm{Hom}(M, N)$。任取 $r \in R$ 以及 $x, y \in R$，我们有

1. $(f+g)(rx+y) = f(rx+y) + g(rx+y) = rf(x) + f(y) + rg(x) + g(y) = r(f(x)+g(x)) + (f(y)+g(y)) = r((f+g)(x)) + (f+g)(y)$。
2. $(af)(rx+y) = af(rx+y) = a(rf(x)+f(y)) = r((af)(x)) + (af)(y)$。

接下来，我们要证明 $\mathrm{Hom}(M, N)$ 对加法构成阿贝尔群。

结合律和交换律是显然的。单位元是平凡模同态 $0 : x \mapsto 0$，这是因为对任意 $f \in \mathrm{Hom}(M, N)$ 和 $x \in M$，我们有

$$(f+0)(x) = f(x) + 0(x) = f(x) + 0 = f(x)$$

所以 $f + 0 = f$，这就说明了平凡模同态 0 是 $\mathrm{Hom}(M, N)$ 的加法单位元。

接着，对任意 $f \in \mathrm{Hom}(M, N)$，它的加法逆元是 $-f : x \mapsto -f(x)$，这是因为对任意 $x \in M$，我们有

$$(f+(-f))(x) = f(x) + (-f)(x) = f(x) + (-f(x)) = 0$$

所以 $f + (-f) = 0$，这就说明了 $-f$ 是 f 的加法逆元。

我们还需要证明四条性质。令 $a, b \in R$，$f, g \in \mathrm{Hom}(M, N)$。假设 $x \in M$。

1. $(1f)(x) = 1f(x) = f(x)$，所以 $1f = f$。
2. $((a+b)f)(x) = (a+b)f(x) = af(x) + bf(x) = (af)(x) + (bf)(x)$，所以 $(a+b)f = af + bf$。
3. $(a(f+g))(x) = a((f+g)(x)) = a(f(x)+g(x)) = (af)(x) + (ag)(x)$，所以 $a(f+g) = af + ag$。
4. $(a(bf))(x) = a((bf)(x)) = a(b(f(x))) = (ab)(f(x)) = ((ab)f)(x)$，所以 $a(bf) = (ab)f$。

此即得证。

注 若 R 是个域，这就是我们在线性代数中熟悉的结论：从一个 k-向量空间到另一个 k-向量空间的所有线性映射构成了一个 k-向量空间。

有人可能会说，直积的性质已经很好了，为什么还要定义直和呢？直积和直和又满足什么比较好的性质呢？下面，我们来证明直积与直和最重要的性质。

要证明直积和直和的性质，我们先证明每一个投影映射都是一个模同态。

引理 2.10

假设 I 是一个非空指标集，并且对于任意的 $i \in I$，M_i 都是一个 R-模，则嵌入映射 $\pi_j : (x_i)_{i\in I} \mapsto x_j$ 是一个从 $\prod_{i\in I} M_i$ 到 M_j 的 R-模同态。

♡

证明 这几乎是显然的。令 $a \in R$，$(x_i)_{i\in I}, (y_i)_{i\in I}$，则我们有

$$\pi_j\left(a\left(x_i\right)_{i\in I}+\left(y_i\right)_{i\in I}\right)=\pi_j\left(\left(ax_i+y_i\right)_{i\in I}\right)=ax_j+y_j=a\pi_j\left(\left(x_i\right)_{i\in I}\right)+\pi_j\left(\left(y_i\right)_{i\in I}\right)$$

此即得证。

更显然地，每一个嵌入映射都是一个模同态。

引理 2.11

假设 I 是一个非空指标集，并且对于任意的 $i\in I$，M_i 都是一个 R-模，则投影映射 $i_j: x_j\mapsto (x_j)_{\substack{i\in I\\ i=j}}\times(0)_{\substack{i\in I\\ i\neq j}}$ 是一个从 M_j 到 $\bigoplus_{i\in I}M_i$ 的 R-模同态。

证明 证明是显然的，我们留给感兴趣的读者作为练习，唯一要注意的是之所以这个映射是映到 $\bigoplus_{i\in I}M_i$ 的，是因为像中的每一个元素都只有至多一个非零的项。

命题 2.5

假设 M 是一个 R-模，I 是一个非空指标集，假设对于任意的 $i\in I$，N_i 都是一个 R-模，则

$$\operatorname{Hom}\left(M,\prod_{i\in I}N_i\right)\simeq\prod_{i\in I}\operatorname{Hom}\left(M,N_i\right)$$

证明 下面，我们定义 $\phi:\operatorname{Hom}\left(M,\prod_{i\in I}N_i\right)\to\prod_{i\in I}\operatorname{Hom}\left(M,N_i\right)$。

令 $f\in\prod_{i\in I}N_i$，我们定义

$$\phi(f)=\left(\pi_i\circ f\right)_{i\in I}$$

由于每一个 π_i 都是模同态，因此每一个 $\pi_i\circ f$ 都是模同态，这就证明了 ϕ 是一个模同态。

现在，我们只须证明 ϕ 是一个双射。反过来，对任意的 $(f_i)_{i\in I}$，我们下面定义 $\phi^{-1}\left((f_i)_{i\in I}\right)$。对任意 $x\in M$，我们定义 $\left(\phi^{-1}\left((f_i)_{i\in I}\right)(x)\right)_{i\in I}=f_i(x)$。

我们很容易证明 ϕ^{-1} 是 ϕ 的逆映射，因此 ϕ 是一个双射。

综上所述，ϕ 是一个 R 上的模同构，这就证明了

$$\operatorname{Hom}\left(M,\prod_{i\in I}N_i\right)\simeq\prod_{i\in I}\operatorname{Hom}\left(M,N_i\right)$$

命题 2.6

假设 I 是一个非空指标集，对于任意的 $i\in I$，M_i 都是一个 R-模，N 也是一个 R-模，则

$$\operatorname{Hom}\left(\bigoplus_{i\in I}M_i,N\right)\simeq\prod_{i\in I}\operatorname{Hom}\left(M_i,N\right)$$

证明 下面，我们定义 $\phi:\operatorname{Hom}\left(\bigoplus_{i\in I}M_i,N\right)\to\prod_{i\in I}\operatorname{Hom}\left(M_i,N\right)$。

令 $f\in\bigoplus_{i\in I}\left(M_i,N\right)$，我们定义

$$\phi(f)=\left(f\circ i_j\right)_{j\in I}$$

由于每一个 i_j 都是模同态，因此每一个 $f\circ i_j$ 都是模同态，这就证明了 ϕ 是一个模同态。

现在，我们只须证明 ϕ 是一个双射。反过来，对任意的 $\left(f_j\right)_{j\in I}$，我们下面定义 $\phi^{-1}\left(\left(f_j\right)_{j\in I}\right)$。对任意 $\left(x_j\right)_{j\in I}$，我们定义 $\phi^{-1}\left(\left(f_j\right)_{j\in I}\right)\left(\left(x_j\right)_{j\in I}\right)=\sum_{j\in I}f_j\left(x_j\right)$。

因为除了有限项外的每一个 x_j 都是 0，所以这样的和一定是有限和，也就是良定义的。

我们很容易证明 ϕ^{-1} 是 ϕ 的逆映射，因此 ϕ 是一个双射。

综上所述，ϕ 是一个 R 上的模同构，这就证明了

$$\operatorname{Hom}\left(\bigoplus_{i\in I}M_i,N\right)\simeq\prod_{i\in I}\operatorname{Hom}\left(M_i,N\right)$$

注 未来我们会知道，R-模的直积和直和用范畴论的语言来说就是 R-模范畴上的积和余积。

2.4 循环模、有限生成模与自由模

我们先给出一些定义。

定义 2.13

令 M 是一个 R-模。我们称 M 是一个循环模当且仅当存在一个 $a \in M$，使得 $M = Ra$。换言之，$M = \langle a \rangle$，即 M 可以由一个元素生成。 ♣

定义 2.14

令 M 是一个 R-模。我们称 M 是一个有限生成模当且仅当存在 $a_1, \cdots, a_n \in M$，使得 $M = Ra_1 + \cdots + Ra_n$。换言之，$M = \langle a_1, \cdots, a_n \rangle$，即 M 可以由有限多个元素生成。 ♣

例题 2.6 显然，每一个循环模都是有限生成模。

同线性代数中一样，我们可以给出线性相关和线性无关的概念。

定义 2.15

假设 M 是一个 R-模，而 $S \subset M$ 是一个子集。我们称 S 是线性无关的，当且仅当对任意 $n \in \mathbb{N}_1$ 和 $s_1, \cdots, s_n \in S$，如果存在 $a_1, \cdots, a_n \in R$，使得 $a_1s_1 + \cdots + a_ns_n = 0$，则我们一定有 $a_1 = \cdots = a_n = 0$。换言之，不存在非平凡的使得值为 0 的线性组合。 ♣

定义 2.16

假设 M 是一个 R-模，而 $S \subset M$ 是一个子集。我们称 S 是线性相关的，当且仅当存在 $s_1, \cdots, s_n \in S$ 以及不全为零的 $a_1, \cdots, a_n \in R$，使得 $a_1s_1 + \cdots + a_ns_n = 0$。换言之，存在至少一个非平凡的使得值为 0 的线性组合。 ♣

由于这样的线性组合一定是有限的（除非引入极限的概念，一般来说我们不能定义无限的线性组合），因此每一个线性相关组都可以简化为一个有限的线性相关组。

根据定义，我们显然可以证明下列引理。

引理 2.12

假设 M 是一个 R-模，而 $S \subset T \subset M$ 是两个子集。

1. 若 T 是线性无关的，则 S 也是线性无关的。
2. 若 S 是线性相关的，则 T 也是线性相关的。

♡

现在，我们定义自由模。

定义 2.17

令 M 是一个 R-模。我们称 M 是一个自由模当且仅当存在 $S \subset M$，使得

1. $M = \langle S \rangle$，即 M 可以由 S 生成。
2. S 是线性无关的。

此时，我们称 S 是 M 的一组基。

若 S 可以是有限的，那我们就说 M 是一个有限秩的 R-模。 ♣

引理 2.13

假设 M 是一个有限秩的 R-自由模，S 是一个 M 的一个有限基，$|S| = n$，则 $M \simeq R^n$。 ♡

证明 假设 $S=\{x_1,\cdots,x_n\}$ 是 M 的一组基。我们定义 $f:R^n\to S$ 为 $f(a_1,\cdots,a_n)=a_1x_1+\cdots+a_nx_n$。这显然是一个模同态。下面，我们来证明这是个双射。

由于 S 生成了 M，所以根据定义，我们知道 f 是一个满射。

由于 S 是线性无关的，所以 $\ker(f)=\{0\}$。只通过模对加法构成阿贝尔群的事实，我们就知道 f 是一个单射。

此即得证。

为了熟悉有限秩的 R-模，我们给一个引理来帮助大家理解。

引理 2.14

假设 M 是一个有限秩的 R-自由模，N 是一个 R-模，S 是一个 M 的一个有限基，则 $\mathrm{Hom}(M,N)$ 和 $\{f:S\to N\}$ 是一一对应的。 ♡

注 换言之，一个有限秩的 R-自由模 M 到另一个 R-模 N 的模同态由 M 的一组基被映射到的值所确定。

证明 令 $S=\{x_1,\cdots,x_n\}$ 是 M 的一组基，显然每一个 $f:M\to N$ 确定了 f 在每一个 $x_i\in S$ 上的值。因此，我们只须证明，如果我们指定了 $g(x_i)\in N$，我们就可以唯一地将其延拓至一个从 M 到 N 的模同态。

利用基的定义（生成了 M 并且是线性无关的），任意的 $x\in M$ 都可以唯一地写成

$$x=a_1x_1+\cdots+a_nx_n$$

的形式，其中 $a_1,\cdots,a_n\in R$。

现在，我们只须定义

$$g(a_1x_1+\cdots+a_nx_n)=a_1g(x_1)+a_ng(x_n)$$

这显然是一个良定义的从 M 到 N 的模同态，我们将完整的证明留给感兴趣的观众。

此即得证。

下面，我们证明一个重要的引理。

命题 2.7

假设 R 是一个非零交换环，且 $m<n$ 是两个不同的正整数，则 $R^m\not\simeq R^n$。 ♠

注 这里的不同构指的是作为 R-模不同构。

证明 用反证法，假设 $f:R^m\to R^n$ 是一个 R-模同构，令 $e_i=(0,\cdots,i\cdots,1)$，则 $\{e_i\}_{1\le i\le m}$ 显然构成了 R^n 的一组基。因此，对任意 $a_1,\cdots,a_n\in R$，我们都有

$$f(a_1e_1+\cdots+a_ne_n)=a_1f(e_1)+\cdots+a_nf(e_n)$$

这样的 $f:R^m\to R^n$ 是一个双射的模同态，

在后续的交换代数这门课中，我们会用 Zorn 引理证明每一个非零交换环都有至少一个极大理想。在这里，我们假定这个命题是成立的。令 $\mathfrak{m}$ 是 R 的一个极大理想，因此 $R/\mathfrak{m}$ 是一个域。现在，我们不难证明 $R/\mathfrak{m}$ 在显然的标量乘法下也构成一个 R-模，即 $a(r\mathfrak{m})=(ar)\mathfrak{m}$。因此，$f$ 会引出

$$\tilde{f}:R^m/\mathfrak{m}^m\simeq(R/\mathfrak{m})^m\to(R/\mathfrak{m})^n\simeq R^n/\mathfrak{m}^n$$

而 $\tilde{f}$ 依然是双射的模同态。在这里，因为 $k=R/\mathfrak{m}$ 是一个域，所以实际上 $\tilde{f}$ 是一个从 k^m 到 k^n 的 k-线性同构，而根据线性代数的知识，我们必须有 $m=n$。

此即得证。

我们有一个显然的推论。

引理 2.15

假设 R 是一个非零交换环，并且 R-自由模 M 有一个有限的基，则这个基的元素个数是固定的。

证明 假设 M 有两组基 S,T，其中 $|S|=m$，$|T|=n$，则我们知道在 R-模的意义下，

$$M \simeq R^m \simeq R^n$$

由于 R 是一个非零交换环，利用上面的条件，我们就知道 $m=n$，此即得证。

因此，我们可以良好地给出下列定义。

定义 2.18

假设 M 是一个有限秩的 R-自由模，而 S 是一个 M 的一个有限基，则我们称 M 的秩为 $|S|$。

证明 利用上面的命题，我们知道这是良定义的。

下面，我们继续讲有限生成模。

为了研究有限生成模，我们给出由 R-模的一个子集生成的自由模。

定义 2.19

令 M 是一个 R-模，$S \subset M$ 是一个非空子集。我们下面定义由 S 生成的自由模，记作 $F(S)$。

$$F(S) = \{f : S \to R : \text{除了有限项外的所有 } f(s) \text{ 都等于 } 0\}$$

若 $f,g \in F(S)$，$a \in R$，对任意 $s \in S$，我们定义

1. $(f+g)(s) = f(s)+g(s)$。
2. $(af)(s) = af(s)$

证明 这显然是良定义的，我们把证明留给感兴趣的读者。

命题 2.8

令 M 是一个 R-模，$S \subset M$ 是一个非空子集，则 $F(S)$ 是 R 上的一个自由模，而 S 在双射的意义下可以作为 $F(S)$ 的一组基。

证明

我们容易证明 $F(S)$ 是一个 R-模。我们将证明留给感兴趣的读者。

对任意 $s \in S$，我们下面定义 s 的示性函数

$$\delta_s : S \to R$$

我们定义 $\delta_s(s)=1$，而对于任意 $t \in S \setminus \{s\}$，我们定义 $\delta_s(t)=0$。

显然，根据 $F(S)$ 的定义，$F(S)$ 中的每一个元素可以写成有限多个 δ_s 的线性组合。

现在，我们来证明这些 δ_s 是线性无关的。

假设对两两不同的 $s_1, \cdot, s_n \in S$，我们有 $a_1\delta_{s_1} + \cdots + a_n\delta_{s_n} = 0$。显然，这里的 0 指的是将所有元素映到 0 的常值映射。

现在，我们只须在每一个 s_i 上取值，就得到了 $a_i\delta_{s_i}(s_i) = a_i = 0$，而这就迫使每一个 a_i 都等于 0。这就证明了这些 δ_s 是线性无关的。

根据自由模的定义，这就证明了 $F(S)$ 是一个自由模。

为了熟悉这样的 $F(S)$，我们再介绍 $R^{\bigoplus S}$。

定义 2.20

令 R 是一个交换环，我们下面定义 $R^{\bigoplus S}$.
对任意 $s \in S$，我们定义 $R_s = R$，则 $R^{\bigoplus S}$ 指的是

$$R^{\bigoplus S} = \bigoplus_{s\in S} R_s = \bigoplus_{s\in S} R$$

显然，我们有下列命题。

命题 2.9

$R^{\bigoplus S}$ 也是一个 R 上的自由模，而 S 在双射的意义下可以作为 $F(S)$ 的一组基。

证明

对任意 $t \in S$，我们定义 $e_t = (x_s)_{s\in S}$，其中 $x_t = 1$，而对于任意的 $t \neq s$，$x_s = 0$。
根据直和的定义，显然所有的 $\{e_s\}_{s\in S}$ 构成了 $R^{\bigoplus S}$ 的一组基。
事实上，这两个模是同构的。

引理 2.16

令 M 是一个 R-模，$S \subset M$ 是一个非空子集，则 $F(S) \simeq R^{\bigoplus S}$。

证明 我们只须将每一个 δ_s （$s \in S$）都一一对应地映射到 e_s，再利用所有的 δ_s 和所有的 e_s 分别构成两边的基，就能证明 $F(S)$ 与 $R^{\bigoplus S}$ 作为 R-模是同构的。
此即得证。
事实上，若 M 是一个自由模，我们就可以把 M 写成循环子模的直和。

引理 2.17

假设 M 是一个 R-自由模，且 $\{x_i\}_{i\in I}$ 是 M 的一组基，则

$$M \simeq \bigoplus_{i\in I} Rx_i$$

证明 根据自由模的基的性质，M 中的每一个元素可以唯一地写成有限多个 x_i 在 R 中的线性组合。注意到 $\{ax_i : a \in R\}$ 刚好是 $Rx_i = \langle x_i \rangle$，因此根据直和的定义，我们正好有

$$M \simeq \bigoplus_{i\in I} Rx_i \simeq R^{\bigoplus I}$$

此即得证。
特别地，对于有限秩的自由模，我们有推论。

引理 2.18

假设 M 是一个有限秩的 R-自由模，且 $\{x_i\}_{1\le i\le n}$ 是 M 的一组基，则

$$M \simeq \bigoplus_{i=1}^{n} Rx_i \simeq R^n$$

证明 这是显然的。
对于有限生成模，我们有显然的满同态。

引理 2.19

假设 R-模 M 可以被 $x_1, \cdots, x_n \in M$ 生成，换言之，我们有 $M = Rx_1 + \cdots + Rx_n$，则典范映射 $\pi(a_1, \cdots, a_n) = a_1x_1 + \cdots + a_nx_n$ 是一个从 R^n 到 M 的 R-模的满同态。

证明 利用有限生成模的定义，这是显然的。

这个满同态让我们有一个自然的推论，那就是每个 R-模都有一个同构于 R 的商模。

命题 2.10

若 M 是一个有限生成的模，则存在一个 $N < R^n$，使得 R^n/N 作为一个 R-模同构于 M。

证明 只须令 $N = \ker(\pi)$。注意到 $\pi : R^n \to M$ 是一个 R-模的满同态，因此利用模同构第一定理，我们就得到了

$$R^n/N = R^n/\ker(\pi) \simeq \mathrm{im}(\pi) = M$$

此即得证。

2.5 模、环与理想

在这一节中，我们来探讨模、环与理想的关系。

命题 2.11

假设 M 是一个 R-模，而 $f : S \to R$ 是一个交换环的环同态。我们如果将 $\cdot : S \times M \to M$ 定义为 $s \cdot m = f(s)m$，则 M 在这个标量乘法下构成一个 S-模。

证明 首先，M 上的加法没有变，因此 $(M, +)$ 还是一个阿贝尔群。

此外，这个标量乘法显然是良定义的。我们只须证明剩下四个条件。

令 $x, y \in M$，$a, b \in S$。

1. $1 \cdot x = f(1)x = 1x = x$。
2. $(a + b) \cdot x = f(a + b)x = (f(a) + f(b))x = f(a)x + f(b)x = a \cdot x + b \cdot x$。
3. $a \cdot (x + y) = f(a)(x + y) = f(a)x + f(a)y = a \cdot x + a \cdot y$。
4. $a \cdot (b \cdot x) = a \cdot (f(b)x) = f(a)(f(b)x) = (f(a)f(b))x = f(ab)x = (ab) \cdot x$。

综上所述，我们就证明了 M 是一个 S-模。

我们来看一个例子。

例题 2.7 若 M 是一个 R-模，$I \lhd R$，则 M 对应地是一个 R/I 模。

证明

有时，我们希望将模 M 所对应的环 R 扩张为一个更大的环 R'（一般地，我们说环 R 可以嵌入到 R' 中，即存在一个从 R 到 R' 的单同态），并且保持 $R \subset R'$ 上的作用（即标量乘法）不变。我们称这样的 R'-模是由 R-模 M 引出的。

定义 2.21

假设 M 是一个 R-模，假设 R 是 R' 的子环，则我们称 R'-模 M 是 R-模 M 的一个提升当且仅当对任意 $r \in R$，r 在 M 上的作用不变；换言之，对任意 $r \in R$ 和 $x \in M$，我们有

$$r \cdot x = rx$$

有时，若 M 是一个 R-模，我们希望将 M 视作一个 $R[x]$-模。事实上，这样的 $R[x]$-模仅仅是由 M 上的一个 R-模自同态确定的。

命题 2.12

若 M 是一个 R-模，则由这个模引出的 $R[x]$-模与 M 上的 R-模自同态是一一对应的。换言之，任给一个由 R-模 M 引出的 $R[x]$-模，我们可以找到一个 M 上的 R-模自同态与之对应；反过来，任给一个 M 上的 R-模自同态，我们可以构造出一个由 R-模 M 引出的 $R[x]$-模。

证明 我们首先注意到 $R[x]$ 是由 R 和 x 生成的。我们现在要从 R-模 M 中引出一个 $R[x]$-模。注意到利用模的右分配律，我们知道对任意标量 a,b 以及 $m \in M$，我们应该有

$$(a+b)m = am + bm$$

因此，对任意 R 上多项式 $p(x) = a_0 + a_1x + \cdots + a_nx^n$，我们应该有

$$\begin{aligned}(p(x)) \cdot m &= (a_0 + a_1x + \cdots + a_nx^n) \cdot m = a_0 \cdot m + (a_1x) \cdot m + \cdots + (a_nx^n) \cdot m \\ &= a_0m + a_1(x \cdot m) + \cdots + a_n(x^n \cdot m) \\ &= a_0m + a_1(x \cdot m) + \cdots + a_n(x \cdot (x \cdots (x \cdot m) \cdots))\end{aligned}$$

因此，整个 $R[x]$ 的标量乘法由 x 的标量乘法唯一确定。换言之，我们只要规定了 x 如何作用在 M 上，我们就规定了从 R-模 M 到 $R[x]$-模的一个提升。

那么 x 的 M 上的作用是什么呢？我们希望 x 是一个标量，即它要将 M 中的元素变为 M 中的元素，并且满足 R-模同态的一些性质。事实上，我们容易证明，每一个标量都等价于一个 R-模自同态。

综上所述，我们就证明了由 R-模 M 引出的 $R[x]$-模与 M 上的 R-模自同态是一一对应的。

更一般地，我们有下列命题。

命题 2.13

假设 $n \in \mathbb{N}_1$。若 M 是一个 R-模，则由这个模提升出的 $R[x_1, \cdots, x_n]$-模与 M 上的 n 个 R-模自同态是一一对应的。

证明 同理，我们只须对每一个 x_i 指代一个 M 上的 R-模自同态。

此即得证。

接下来，我们来看理想与模可以有什么关联。

若 M 是一个 R-模，I 是 R 的一个理想，我们或许会问，M 是否会自然地成为商环 R/I 上的一个模呢？

回答是不一定。我们为了良定义性，要加上一个条件：$IM = \{0\}$，即 I 中的元素作用在 M 上都是 0。

引理 2.20

假设 M 是一个 R-模，$I \lhd R$ 是一个理想，并且 $IM = \{0\}$，则 M 是一个 R/I-模。这里的标量乘法指的是对 $r \in R$ 和 $x \in M$，我们定义 $(rI)(x) = rx$。

证明 我们先证明这是良定义的。假设 $r, r' \in R$，使得 $rI = r'I$，即 $r - r' \in I$。设 $x \in M$，由于 $IM = \{0\}$，我们有 $rx - r'x = (r - r')x = 0$，故 $rx = r'x$。

下面，我们证明模的后四条性质。

1. $(1I)(x) = 1x = 1$。
2. $(aI + bI)(x) = ((a+b)I)(x) = (a+b)(x) = ax + bx = (aI)(x) + (bI)(x)$。
3. $(aI)(x+y) = a(x+y) = ax + ay = (aI)(x) + (aI)(y)$。
4. $(aI)(bI(x)) = (aI)(bx) = a(bx) = (ab)x = ((aI)(bI))x$。

此即得证。

很显然，上一个引理中 $IM = \{0\}$ 的条件是为了强行让 M 成为 R/I 上的模。

$IM = \{0\}$ 的条件我们如何进一步理解呢？我们有两种理解方式，第一种方式是关注环中的元素，第二种方式是关注模中的元素。第一种方式给出了零化理想和忠实模的定义，第二种方式给出了挠子模和无挠模。

第一种理解方式就是 I 中的每一个元素 $x \in I$ 都“零化”了 M 的所有元素。对于这样的 R 元素，我们称为 M 的一个零化子。所有零化子的 R 的子集被称为 M 的零化理想。

定义 2.22

令 M 是一个 R-模，我们称 $r \in R$ 是 M 的一个零化子当且仅当 $rM = \{0\}$。换言之，对任意 $x \in M$，我们有 $rx = 0$。M 的所有零化子构成的 R 的子集，称为 M 的零化理想，指的是

$$\mathrm{Ann}(M) = \{r \in R : \forall x \in M, rx = 0\}$$

♣

进一步地，我们补充忠实 R-模的定义。

定义 2.23

令 M 是一个 R-模，我们称 M 是一个忠实的 R-模当且仅当 $\mathrm{Ann}(M) = \{0\}$。换言之，没有非平凡的零化子。♣

既然叫零化理想，当然是个理想。

引理 2.21

令 M 是一个 R-模，则 $\mathrm{Ann}(M) \lhd R$。

♡

证明 显然，$0 \in \mathrm{Ann}(M)$，因为对任意 $x \in M$，$0x = 0$。

令 $r, s \in \mathrm{Ann}(M)$，$a \in R$。我们只须证明 $r + s \in \mathrm{Ann}(M)$，$ar \in \mathrm{Ann}(M)$。

假设 $x \in M$。

1. $(r + s)(x) = rx + sx = 0 + 0 = 0$。
2. $(ar)(x) = a(rx) = a0 = 0$。

此即得证。

现在，显然我们有 $\mathrm{Ann}(M)M = \{0\}$。

引理 2.22

令 M 是一个 R-模，则 $\mathrm{Ann}(M)M = \{0\}$。

♡

证明 令 $r \in \mathrm{Ann}(M)$，$x \in M$。根据零化子的定义，我们有 $rx = 0$。

此即得证。

由于这个显然的结论以及我们上面证明过的引理，我们可以将 M 视作 $R/\mathrm{Ann}(M)$ 上的一个模。

由于模掉了所有的零化子，M 在商环 $R/\mathrm{Ann}(M)$ 上是否是忠实的呢（没有非平凡的零化子)?

回答是肯定的。

命题 2.14

令 M 是一个 R-模，则 M 自然地成为一个忠实的 $R/\mathrm{Ann}(M)$-模。

♠

证明 用反证法。假设 M 不是忠实的 $R/\mathrm{Ann}(M)$-模，则存在 $r\,\mathrm{Ann}(M) \neq \mathrm{Ann}(M)$（即 $r \notin \mathrm{Ann}(M)$），使得对于 $x \in M$，$(r\,\mathrm{Ann}(M))(x) = rx = 0$。

因此，对于 $x \in M$，我们有 $rx = 0$。

这就说明 $x \in \mathrm{Ann}(M)$，而这与假设矛盾。

因此，我们就证明了 M 是一个忠实的 $R/\mathrm{Ann}(M)$-模。

我们讲完了第一种理解方式，下面我们讲第二种理解方式，从模中的元素来理解，定义挠子模和无挠模。

定义 2.24

令 M 是一个 R-模，我们称 $x \in M$ 是一个挠元当且仅当存在 $r \in R \setminus \{0\}$，使得 $rx = 0$。我们定义由所有的挠元所构成的 M 中子集为 $\mathrm{T}(M) = \mathrm{Tor}(M) = \{x \in M : \exists r \in R \setminus \{0\}, rx = 0\}$，称为 M 的挠子模。

♣

注 因为三个字母太多了，我们常常只用 T 来表示挠元构成的集合。如果读者喜欢 Tor，当然可以使用 Tor。

我们不是很喜欢。

所有的挠元构成的集合应该也满足一些性质，实际上在 R 是整环的情况下，挠子模是一个子模。可是一般来说，如果 R 只是交换环，则挠子模不是一个子模。我们把反例留给感兴趣的读者。下面，我们来证明，若 R 是个整环，则挠子模是个子模。

引理 2.23

假设 R 是一个整环，M 是一个 R-模，则 $\mathrm{T}(M)$ 是 M 的一个子模。

证明 显然，$1 \neq 0$，并且 $10 = 0$，因此 $0 \in \mathrm{T}(M)$。

接下来，我们只需证明 $\mathrm{T}(M)$ 对加法和标量乘法是封闭的。

令 $x, y \in \mathrm{T}(M)$，$r \in R$。我们只须证明 $x + y \in \mathrm{T}(M)$，$rx \in \mathrm{T}(M)$。假设 $a, b \in R \setminus \{0\}$，使得 $ax = by = 0$

1. 注意到 $(ab)x = b(ax) = b0 = 0$ 以及 $(ab)y = a(by) = a0 = 0$，所以 $(ab)(x + y) = (ab)x + (ab)y = 0 + 0 = 0$。注意到在整环中非零元素的乘积还是非零的，所以 $ab \neq 0$，故 $x + y \in \mathrm{T}(M)$。
2. 注意到 $a(rx) = r(ax) = r0 = 0$，故 $rx \in \mathrm{T}(M)$。

此即得证。

现在，$\mathrm{T}(M)$ 是 M 的一个子模，我们有商模 $M/\mathrm{T}(M)$。既然我们模掉了所有的挠元，商模中应该没有非平凡（非零）的挠元吧。这就是下一个命题。

命题 2.15

令 M 是一个 R-模，则 $M/\mathrm{T}(M)$ 是无挠的，即没有非平凡（非零）的挠元。

证明 假设 $x\,\mathrm{T}(M) \in M/\mathrm{T}(M)$（$x \in M$）是 $M/\mathrm{T}(M)$ 中的一个挠元。我们只须证明 $x\,\mathrm{T}(M) = \mathrm{T}(M)$，即 $x \in \mathrm{T}(M)$。

由于 $x\,\mathrm{T}(M)$ 是 $M/\mathrm{T}(M)$ 中的一个挠元，所以存在一个 $r \in R \setminus \{0\}$，使得

$$r(x\,\mathrm{T}(M)) = (rx)\,\mathrm{T}(M) = 0 + \mathrm{T}(M) = \mathrm{T}(M)$$

因此 $rx \in \mathrm{T}(M)$。我们可以取到 $a \in R \setminus \{0\}$，使得 $a(rx) = (ar)x = 0$

我们只须证明 $x \in \mathrm{T}(M)$。

根据前面的条件，我们知道 $a \neq 0$，$r \neq 0$。由于 R 是一个整环，我们就得到了 $ar \neq 0$ 的结论。这就说明了 $x \in \mathrm{T}(M)$。

此即得证。

为了熟悉挠子模，我们再介绍一些性质。

引理 2.24

假设 M, N 是两个 R-模，$f : M \to N$ 是一个 R-模同态，则 $f(\mathrm{T}(M)) \subset \mathrm{T}(N)$，我们可以定义 $\tilde{f} : M/\mathrm{T}(M) \to N/\mathrm{T}(N)$。

证明

1. 假设 $x \in T(M)$，则存在 $a \in R - \{0\}$，使得 $ax = 0$。我们只须证明 $f(x) \in \mathrm{T}(M)$。而这是因为 $0 = f(0) = f(ax) = af(x) = 0$。这就证明了 $f(\mathrm{T}(M)) \subset \mathrm{T}(N)$。
2. 对任意 $a \in M$，我们只须定义 $\tilde{f}(a + \mathrm{T}(M)) = f(a) + T(N)$。由于 $f(\mathrm{T}(M)) \subset \mathrm{T}(N)$，$\tilde{f}$ 是良定义的。利用商模的性质，$\tilde{f}$ 显然是一个 R-模同态。

此即得证。

2.6 主理想整环上的模

在这一节中，我们来研究主理想整环上的模。在这一节中，所有讨论的环都是主理想整环。

我们先来证明一个引理。

引理 2.25

假设 R 是一个主理想整环，M 是一个 R-循环模，则 M 的每一个子模都是 R-循环模。

注 这个引理的类比就是整数加群 $\mathbb{Z}$ 上每个循环子群的子群还是循环群。

证明 假设 $M = Rx = \langle x \rangle$，而 $N < M$ 是一个子模。

如果 $N = \{0\}$，那是显然的。所以我们假设 $N \neq \{0\}$。

由于 $N < M$，所以 N 中的每个元素都可以写成 rx 的形式，其中 $r \in R$。

我们令

$$S = \{r \in R : rx \in M\} \subset R$$

为了利用主理想整环的性质，我们下面证明 S 是 R 的一个理想。令 $a, b \in S$ 和 $r \in R$，我们有 $ax = bx = 0$。

1. 由于 $(a+b)(x) = ax + bx = 0 + 0 = 0$，所以 $a + b \in S$。
2. 由于 $(ra)(x) = r(ax) = r0 = 0$，所以 $ra \in S$。

这样，我们就证明了 $S \lhd R$。由于 R 是一个主理想整环，我们可以找到一个 $a \in R$，使得 $S = Ra = (a)$。

因此，我们就知道

$$N = Sx = (Ra)x = R(ax) = \langle ax \rangle$$

此即得证。

命题 2.16

假设 R 是一个主理想整环，M 是一个有限秩的 R-自由模，$N < M$ 是一个子模，则 N 也是一个有限秩的 R-自由模，并且 N 的秩不超过 M 的秩。

证明 假设 $S = \{x_1, \cdots, x_n\}$ 是 M 的一组基，因此 $M = \langle x_1, \cdots, x_n \rangle$。由于 $N < M$，我们有

$$N = N \cap \langle x_1, \cdots, x_n \rangle$$

对任意 $1 \leq i \leq n$，令 $N_i = N \cap \langle x_1, \cdots, x_i \rangle$。

利用数学归纳法，我们只须证明每一个 N_i 都是秩不超过 n 的 R-自由模即可。

1. 当 $i = 1$ 时，$N_1 = N \cap \langle x_1 \rangle < \langle x_1 \rangle$。利用上面的引理，我们知道存在一个 $a_1 \in R$，使得 $N_1 = \langle a_1 x_1 \rangle$。
2. 假设命题对于某个 $i < n$ 成立，即 N_i 是一个秩不超过 i 的 R-自由模，我们只须证明 N_{i+1} 是一个秩不超过 $i+1$ 的 R-自由模。现在我们知道

$$N_i = N \cap \langle x_1, \cdots, x_i \rangle$$

是一个自由模。注意到

$$N_{i+1} = N \cap \langle x_1, \cdots, x_i, x_{i+1} \rangle$$

我们想要描述 N_{i+1} 在 N_i 的基础上多了哪些元素。

类似地，利用 N_{i+1} 的定义，令

$$S = \{r \in R : \langle x_1, \cdots, x_i \rangle + r x_{i+1} \subset N_{i+1}\} = \{r \in R : \langle x_1, \cdots, x_i \rangle + r x_{i+1} \subset N\}$$

同理，我们可以证明 $S \lhd R$。

(a).

(b).

2.7

2.8

2.9

2.10

2.11

2.12

第 3 章 环论 II——Ring theory II

3.1 诺特环

3.2

3.3

3.4

3.5

3.6

3.7

3.8

3.9

3.10

3.11

3.12

第 4 章 域论 2

4.1

4.2

4.3

4.4

4.5

4.6

4.7

4.8

4.9

4.10

4.11

4.12

第 5 章 伽罗瓦理论

5.1

5.2

5.3

5.4

5.5

5.6

5.7

5.8

5.9

5.10

5.11

5.12