本系列应该会持续使用中文书写, 不过某些专业名词将为英文. 本系列的动机始于简明中文群论介绍的欠缺, 其目标为普及主要是有限群的基础群论知识.

1 简单的前置

如果你上过数学课, 应该有能力跳过本节不涉及无限的部分. 无限的部分不必通透理解, 需要掌握的重点只有不存在双射 $X \to \mathcal{P}(X)$!

1.1 集合论

$X \subset Y$ 在本系列中仅指 X 为 Y 的子集, 真子集将用 $X \subsetneq Y$ 表示.

给定集合 (set)$X_1, ...X_n$, $X_1 \times X_2 \times ... \times X_n := \{(x_1, ...x_n) : x_i \in X_i \text{ for all } i \in \{1, ..., n\}\}$, 称为 $X_1, ..., X_n$ 的笛卡尔积 (Cartesian product), $\mathcal{P}(X) := \{A : A \subset X\}$, 称为 X 的幂集 (power set). 若 $X_1 = X_2 = ... = X_n = X$, 我们简记 $X^n = X_1 \times ... \times X_n$.

(除非有特殊情况, 本系列将不会及其严密地书写数学式. 例如, 在 $X_1 \times ... \times X_n$ 的定义中, 我们一般只写 $\{(x_1, ...x_n) : x_i \in X_i\}$; 又如 $\forall x_0, x_1 \in X(...)$ 指的事实是 $\forall x_0 \in X(\forall x_1 \in X(...))$)

一个 X 与 Y 间的关系 (relation)R 是 $X \times Y$ 的一个子集 (subset), 且我们写 xRy 若 $(x, y) \in R$. 例如 $\{(0, 0), (1, 2)\}$ 是 $\mathbb{Z}$ 与 $\mathbb{R}$ 间的一个关系, 我们可以写 $1R2$, 但不能写 $0R\pi$. 若 $X = Y$, 我们简称 R 是 X 上的关系.

若 X, X 间的关系 R 满足:
(i) $\forall x \in X(xRx)$ (反身性 (reflexity))
(ii) $\forall x, y \in X(xRy \to yRx)$ (对称性 (symmetry))
(iii) $\forall x, y, z \in X((xRy \wedge yRz) \to xRz)$ (传递性 (transitivity))

那么称 R 为等价关系 (equivalence relation), 给定 $x \in X$, 称 $[x] := \{y \in X : xRy\}$ 为 x 的等价类 (equivalence class). 等价关系的例子有: 在任意集合 X 上 $=$ 是等价关系, 并且 $\forall x \in X([x] = \{x\})$; 在 $\mathbb{Z}$ 上, 若 xRy 当且仅当 $x \equiv y \mod 2$, 那么 R 为等价关系, 有两个不同的等价类 $[0], [1]$.

容易验证若 $R_i : i \in I$ 都是 X 上的等价关系, $\bigcap_i R_i$ 也为 X 上的等价关系, 于是我们定义由 $A \subset X^2$ 生成的等价关系为

$$\bigcap_{A \subset R, R \text{ equivalence relation}} R$$

例如, 上面 $=$ 是由 $\emptyset$ 生成的, 而 $\mod 2$ 的同余关系是由 $\{(x, x+2)\}$ 生成的. 我们将频繁使用子集生成的方式来定义等价关系, 于是下面的小命题将会很有帮助:

命题 1.1 $A \subset X^2$ 生成的等价关系满足

$$R = \{(x, y) : \exists a_1, ..., a_n \text{ s.t. } a_1 = x, a_n = y, (a_i, a_{i+1}) \in A \text{ or } (a_{i+1}, a_i) \in A\}$$

证明显然 $A \subset R$, 而 R 是等价关系: 对 (x, x) 我们取 $a_1 = x = x$; 若 xRy, 存在满足条件的 $a_1, ..., a_n$, 那么 $a_n, ..., a_1$ 表明 yRx; 若 xRy, yRz, 对 x, y 我们有 $a_1, ..., a_n$, 对 y, z 我们有 $b_1, ..., b_m$, 于是 $a_1, ..., a_n, b_2, ..., b_m$ 就是满足要求的使得 xRz 的序列. 所以 A 生成的等价关系是 R 的子集.

反之, 若 $A \subset S$ 是等价关系, 我们归纳证明 $R \subset S$. 当 $n = 1$ 时, 由 S 为等价关系 $(x, x) \in S$. 对 $(x, y) \in R$ 与它们对应的 $a_1, ..., a_n$, (x, a_{n-1}) 间有更短的序列 $a_1, ..., a_{n-1}$, 于是由归纳假设 $(x, a_{n-1}) \in S$. 现在由 $A \subset S$ 以及 S 具有 symmetry, $(a_{n-1}, a_n) \in S$, 于是由 transitivity $(x, y) \in S$. 所以 R 是 A 生成的等价关系的子集.

综上, A 生成的等价关系是 R. □

评论上述证明是关于由交集生成集合的标准论证 - 若我们要证明某个由 A 生成的集合

$$\bigcap_{A \subset S, S \text{ satisfies property } P} S$$

就是 B, 一般证明都是如下两步: (i) 证明 $B \supset A$ 且满足性质 P, 所以生成的集合是 B 的子集; (ii) 证明任何满足 P 的 $S \supset A$ 都有 $B \subset S$, 于是 B 是生成的集合的子集.

另外尽管本证明中归纳确实是由 $n-1$ 到 n, 在更多的情况下只要我们能将现有情况化到归纳量更小的情况, 我们就能用归纳假设; 甚至某些证明是直接取 "(归纳量) 最小的反例".

若 X, Y 间的关系 f 满足 $\forall x \in X$ 有且仅有唯一一个 $y \in Y$ 使得 xfy, 我们称 f 为 X 到 Y 的一个映射 (map) 或函数 (function), 记作 $f : X \to Y$, 并且记 $y = f(x)$ 若 xfy. 对于 $f_0, f_1 : X \to Y$, 显然 $f_0 = f_1$ 当且仅当 $\forall x \in X(f_0(x) = f_1(x))$, 于是我们可以逐点定义一个映射, 并且逐点定义时一般写 $f : x \mapsto s(x)$, 其中 $s(x)$ 是一个易于由 x 计算出的表达式. 恒等映射 (identity map)$\mathrm{id}_X : X \to X : x \mapsto x$ 就是这样的典型例子. 另一个重要的映射是投影 (projection), $p_i : X_1 \times ... \times X_n : (x_1, ..., x_n) \mapsto x_i$. 给定 $f : X \to Y$ 与 $g : Y \to Z$, 定义 $g \circ f : X \to Z : x \mapsto g(f(x))$, 称为 g 合成 (compose)f; 在没有歧义的情况下我们省略 $\circ$; 容易验证 $(hg)f = h(gf)$, 于是我们省略迭代合成时的括号.

对 $A \subset X$, 定义 $f \restriction A := \{(x, f(x)) : x \in A\}$, 一个 $A \to Y$ 的映射. 定义 $\mathrm{Im}f := \{y : \exists x(f(x) = y)\}$, 称为 f 的象 (image); $f(A) := \mathrm{Im}f \restriction A$. 对于任意 $B \subset Y$, 定义 $f^{-1}(B) = \{x : f(x) \in B\}$, 称为 B 的原象 (inverse image); 注意这对不是双射的 f 也是有定义的; 我们简写 $f^{-1}(y) = f^{-1}(\{y\})$.

$f : X \to Y$ 为单射 (injection) 若 $\forall x_0, x_1 \in X(f(x_0) = f(x_1) \to x_0 = x_1)$; f 为满射 (surjection) 若 $\forall y \in Y \exists x \in X(f(x) = y)$; f 为双射 (bijection) 若它既是单射又是满射.

容易验证, $f : X \to Y$ 为单射当且仅当 $\forall Z \forall g_0, g_1 : Z \to X(fg_0 = fg_1 \to g_0 = g_1)$, f 为满射当且仅当 $\forall Z \forall g_0, g_1 : Y \to Z(g_0 f = g_1 f \to g_0 = g_1)$, f 为双射当且仅当 $\exists g : Y \to X(gf = \mathrm{id}_X \wedge fg = \mathrm{id}_Y)$. 显然这样的 g 是唯一的, 我们称其为 f 的逆映射 (inverse map): f^{-1}. 这些更为抽象的刻画将被频繁使用, 尤其双射的正统定义就是存在逆映射. 显然 X, Y 间存在双射是一个等价关系.

接下来我们承认选择公理 *(Axiom of Choice),* 简单来说即可以在证明里说 "我们挑选一个元素...(使得)".

首先我们弥补一个小缺陷: 对于无穷多个集合 $X_i : i \in I$, 定义

$$\prod_{i \in I} X_i = \{f : I \to \bigcup_{i \in I} X_i : f(i) \in X_i\}$$

在 $I = \{1, 2, ..., n\}$ 的情况下, 这个定义生成的集合与最开始的定义生成的集合之间有典范双射 $f \mapsto (f(1), ..., f(n))$. 在承认选择公理的情况下若 $X_i \neq \emptyset$ 则有它们的 cartesian product 非空. 对无限 cartesian product 依然有投影 $p_i : f \mapsto f(i)$, 并且若 $X_i = X$ 我们还是简记 $X^I = \prod_{i \in I} X_i = \{f : I \to X\}$; 这些新定义与前面的典范双射是兼容的.

给定集合 X, Y, 我们称 X, Y 等势若存在 bijection $f : X \to Y$. 由选择公理易得存在单射 $f : X \to Y$ 当且仅当存在满射 $g : Y \to X$. 可以证明若存在单射 $f : X \to Y$, $g : Y \to X$, 那么 X, Y 等势. $|X| := \min\{\alpha \in \mathrm{On} : \exists f : X \to \alpha \text{ bijection}\}$ 称为集合的势 (cardinality), 其中 On 为序数 (ordinal)构成的类 (class). 简单来说 $|X|$ 是 X 内元素的个数, 如 $|\emptyset| = 0, |\{0, 0, 0, 0, 0\}| = 1, |\{0, 1\}| = 2$; 对于无限集合, 我们有例子 $|\mathbb{Z}| = |\mathbb{N}| = \omega$, 并且通常我们记 $\aleph_0 := \omega = |\mathbb{N}|$. 若 $|X| \leq \aleph_0$, 我们称 X 是可数的 (countable).

不难证明, $|\mathcal{P}(X)| > |X|$, 并且容易构造双射 $\mathcal{P}(\mathbb{Z}) \to \mathbb{R}$(考虑二进制), 于是 $\mathbb{R}$ 是不可数的, 这是最基础也是最重要的 cardinality 关系.

1.2 代数

代数部分请参照 blog 上的 computer algebra 教程 0.

2 群的动机

读者可能之前听说过这么一句经典语录: "群是描述对称性的工具." 这句话尽管在群的标准定义下显得十分抽象, 然而其确实是对群的最好刻画: 所谓对称就是双射, 而群从被投入应用之初就是在描述 automorphism - 某类含有特定性质的双射, 及它们之间的合成关系. 于是我们应该这样理解这条语录:

任何一个群 G 都有一个 X 与单射 $f : G \to \mathrm{Sym}(X) := \{\sigma : \sigma \text{ is a bijection } X \to X\}$; $\mathrm{Im}f$ 此时代表某种 automorphism 构成的集合, 而 f 将这个 automorphism 集的合成结构抽象成群上的运算; 于是我们可以抛弃具体的 X 转而研究更加封装好的对象 - 群, 并由群的各种结构定理总结出原本 $\mathrm{Im}f$ 的结构. 此外, 某些群 H 过于庞大, 但我们可以考察一些 $g : H \to G$, G 的结构较为简单, g 同样保留部分运算结构, 由此从 G 总结出关于 H 的关键结论.

在接下来的定义中, 我们将会明确上一段中出现的各种概念: 群 (group); 群同态 (group homomorphism) - 如 f, g; 子群 (subgroup) - 如 $\mathrm{Im}f \leq \mathrm{Sym}(X)$; 商群 (quotient group) - 如 $\mathrm{Im}g$; 以及最为重要, 也是这条语录的核心: 群作用 (group action), 即 $fg : H \to \mathrm{Sym}(X)$.

3 群的定义

定义 1.2 一个非空集合 G 与配套的一个映射 $\cdot : G \times G \to G$(被称为是乘法 (multiplication)) 被称为一个群 (group), 如果:

(i) $\forall x, y, z \in G(x \cdot (y \cdot z) = (x \cdot y) \cdot z))$, 其中 $x \cdot y = \cdot(x, y)$. 这被称为 associativity.

(ii) $\exists e \in G \forall x \in G(e \cdot x = x \cdot e = x)$, ~~任意一个~~这样的 e_0 被称为 identity.

(iii) 对 (任意一个)identity e_0, $\forall x \in G \exists y \in G(x \cdot y = y \cdot x = e_0)$. 固定 x, ~~任何~~满足这个存在公式的 y_0 被称为 x 的 inverse.

如同映射的合成, 我们一般省略 $\cdot$, 而且由 associativity $(xy)z = x(yz)$, 所以对长度大于 2 的迭代乘法我们直接省略括号, 如 $x((yz)w)$ 将被直接写作 $xyzw$, 而若 n 为正整数, n 个 x 相乘将被记作 x^n, 如 $x^3 = xxx$. 尽管算数中的通常乘法是交换的, 群中乘法通常是不交换的, 尤其当我们的研究重点是双射的合成.

其次上述定义中存在两个带有删除线的量词, 因为接下来我们将会证明它们是多余的, 证明也与双射的逆唯一十分类似:

命题 1.3 在任何一个群 G 中, (i)Identity 是唯一的; (ii) 对任何一个 $x \in G$, 它的 inverse 是唯一的.

证明 (i) 若 e_0, e_1 都是 identity, $e_0 = e_0 e_1 = e_1$. 由此我们一般将 identity 记作 1.

(ii) 若 y_0, y_1 都是 x 的 inverse, $y_0 = y_0 1 = y_0 x y_1 = 1 y_1 = y_1$. 由此我们记 x 的 inverse 为 x^{-1}. □

这样一来我们可以进一步简化书写: 若 n 为整数, $n > 0$ 时 x^n 定义如上, $x^0 = 1$, $n < 0$ 时 $x^n = (x^{-1})^n$. 容易通过归纳验证 $x^{n+m} = x^n x^m$. 另外不要犯低级的符号错误: 1 只是一个代号, 如在 $\mathbb{Z}$, $\cdot$ 为通常加法的情况下, identity 是整数 0 而非整数 1!

另外, 群中等式的变换由于 inverse 存在而非常简单: $xy = z$ 当且仅当 $y = x^{-1}z$ 当且仅当 $x = zy^{-1}$, 所以若 $xy = xz$, $y = x^{-1}xz = z$; $yx = zx$ 同样有 $y = z$, 这在算数的通常乘法中因 0 的存在是不成立的.

当然, 上述定义看起来十分抽象, 并且似乎没有什么应用价值. 不过, 遵循着经典语录的思路, 将 identity 看作 identity map, 乘法看作合成, inverse 看作逆映射, 我们来看一些例子:

(i) $\{1\}$ 是最简单的群, 通常称为 1, 所以在看见 1 代表一个群的时候不要惊慌.

(ii) (finite cyclic group) $\mathbb{Z}_n := \{1, x, x^2, ..., x^n\}$ 配上 $x^a x^b = x^{a+b \mod n}$ 是一个群, 我们可以将其看作 $\mathbb{R}^2 \to \mathbb{R}^2$ 的一系列旋转: x^a 代表着旋转 $\frac{2a\pi}{n}$ 弧度, 即 $(u, v) \mapsto (u\cos\frac{2a\pi}{n} - v\sin\frac{2a\pi}{n}, u\sin\frac{2a\pi}{n} + v\cos\frac{2a\pi}{n})$.

(iii) (infinite cyclic group) $\mathbb{Z}$ 配上通常加法是一个群, 我们可以将 n 看作在 $\mathbb{Z}$ 上平移 n 个单位, 即 $x \mapsto x + n$.

(iv) (symmetric group) 给定集合 X, $\mathrm{Sym}(X)$ 为 X 的对称群 (symmetric group), 乘法为合成. 若 $|X| \geq 3$, $\mathrm{Sym}(X)$ 上的乘法就不交换.

(v) (general linear group) 给定一个 field F, 一个正整数 n, $GL_n(F) := \{T : F^n \to F^n \text{ linear bijection}\}$, 乘法为合成, 或者等价地, $\{M : M \text{ is } n \times n \text{ matrix s.t. } \det(M) \neq 0\}$, 乘法为矩阵乘法. 很明显 $GL_n(F)$ 代表 F^n 的一切线性对称.

(vi) (Galois group) 若 F 是 K 的 extension, $\mathrm{Gal}_K(F) := \{\sigma : F \to F \text{ field homomorphism s.t. } \forall x \in K, \sigma(x) = x\}$, 乘法为合成. 这是群论的第一次重大应用.

在所有群中有一类特殊的群 - 阿贝尔群 (Abelian group), 它们的乘法是交换的:

定义 1.4 若群 A 满足 $\forall x, y \in A(xy = yx)$, A 被称为 Abelian group. 在 Abelian group 中, identity 通常写为 0, xy 写为 $x + y$, x^{-1} 写为 $-x$, x^n 写为 nx.

例如, vector space, ring, 或 field 配上各自的加法就是 Abelian group. 具有有限 generating set(下面定义) 的 Abelian group 结构类似 finite dimensional vector space, 相对于大多数群来说十分简单, 可以参考本 blog 上的 computer algebra 教程.

4 Group homomorphism(群同态) 与 subgroup(子群)

首先我们明确什么叫做 "保留运算结构".

定义 1.5 给定群 G, H, 一个映射 $f : G \to H$ 被称为 group homomorphism 若 $\forall x, y \in G, f(xy) = f(x)f(y)$. 显然, 对任何群 G, id_G 是 homomorphism; 对任何 homomorphism $f : G \to H, g : H \to K$, gf 是 homomorphism.

首先是一个小评论: 若读者接触过一些 ring 或 field 乃至 category, 可能会期望 homomorphism 保留 identity, 否则会出现 image 没有良好结构的情况; 然而在 group homomorphism 的情况下 $f(1) = f(1 \cdot 1) = f(1)f(1)$, 所以 $f(1) = f(1)^{-1}f(1) = 1$. 相似地, $f(x)^{-1} = f(x^{-1})$.

就像在线性代数里一样, 群之间的 homomorphism 可以极大辅助我们对群之间关系的理解; 特别地, 我们不想分开考虑实质一样的群:

定义 1.6 Homomorphism $f : G \to H$ 被称为 isomorphism 若存在 homomorphism $g : H \to G$ 使得 $gf = \mathrm{id}_G, fg = \mathrm{id}_H$, 由双射的性质可知这样的 g 是唯一的 f^{-1}. 若存在 $f : G \to H$ isomorphism, 我们称 G 与 H isomorphic, 写作 $G \simeq H$, 有时也直接写 $G = H$, 尽管作为集合有可能 $G \neq H$. 容易验证 $\simeq$ 是等价关系.

下面是两个简单却广泛应用的小命题:

定理 1.7 若 homomorphism $f : G \to H$ 为双射, f 便已经是 isomorphism.

证明取 $g = f^{-1}$. $f(g(x)g(y)) = f(g(x))f(g(y)) = xy$, 所以 $g(xy) = gf(g(x)g(y)) = g(x)g(y)$, 即 g 就是我们想要的 homomorphism. □

命题 1.8 $f : G \to H$ 为单射若 $f^{-1}(1) = 1$.

证明若 $f(x) = f(y)$, $1 = f(x)f(y)^{-1} = f(xy^{-1})$, 所以 $xy^{-1} = 1$, 即 $x = y$. □

这样一来, 想要了解一个 homomorphism $f : G \to H$ 是否为 isomorphism, 我们可以直接考察 $\ker f := f^{-1}(1)$(称为核 (kernel)) 与 $\mathrm{Im}f$: f 为 isomorphism 当且仅当 $\ker f = 1$ 且 $\mathrm{Im}f = G$. 而就如线性代数中一样, 这两个集合有着特殊的性质:

定义 1.9 若 $H \subset G$ 且 H 在 G 的乘法下任然构成一个群, 我们称 H 为 G 的一个子群, 记为 $H \leq G$. 注意为了乘法能被继承, 我们要求 $\forall x, y \in H, xy \in H$. 反之, 由于乘法是继承的, 我们无需验证 associativity. 当然, 我们无需担心 H 的 identity 与 G 的不同, 因为 $H \to G : x \mapsto x$ 显然是 injective homomorphism, 于是 $1 \in G$ 的 inverse image, 即 H 的 identity, 还是 $1 \in G$.

命题 1.10 给定 homomorphism $f : G \to H$, $\ker f \leq G$, $\mathrm{Im}f \leq H$.

证明若 $f(x) = f(y) = 1$, $f(xy) = f(x)f(y) = 1$; $f(1) = 1$; 若 $f(x) = 1$, $f(x^{-1}) = f(x)^{-1} = 1$, 即 $\ker f \leq G$. $f(x)f(y) = f(xy)$, $1 = f(1)$, $f(x)^{-1} = f(x^{-1})$, 所以 $\mathrm{Im}f \leq H$. □

容易验证若 $H_i \leq G$, $\bigcap H_i \leq G$, 于是我们可以模仿线性代数中的 span 做如下定义:

定义 1.11 给定群 G, $X \subset G$, X 生成的子群定义为

$$\langle X \rangle := \bigcap_{X \subset H, H \leq G} H$$

若 $\langle X\rangle = G$, 我们称 X 为 G 的一个 generating set. 若 X 为 G 的 generating set 且 $X \subset H$, $H = G$; 这将会在验证满射时被用到.

命题 1.12

$$\langle X\rangle = \{w_1 w_2 ... w_n : w_i \in X \text{ or } w_i^{-1} \in X\}$$

其中我们允许 $n = 0$, 长度为 0 的乘积定义为 1.

证明模仿命题 1.1 的证明, 我们先论证右边的集合 - 命名为 H - 是包含 X 的子群: 显然 $X \subset H \subset G$; 由条件 $1 \in H$; 若 $w_1...w_n, v_1, ..., v_m \in H$, $w_1...w_n v_1...v_m \in H$; 若 $w_1...w_n \in H$, $(w_1...w_n)^{-1} = w_n^{-1}...w_1^{-1} \in H$.

接着如果 $X \subset K \leq G$, 对 n 归纳证明任何 $w_1...w_n \in K$: $n = 0$ 时 $1 \in K$ 是 $K \leq G$ 的定义. 对任意 $w_1...w_n$, 由归纳假设 $w_1...w_{n-1} \in K$, 而 $X \subset K \leq G$, 所以 $w_n \in K$, 于是 $w_1...w_n \in K$. □

了解的上述定义后, 我们给出几个例子. 首先是 subgroup 的:

(i) $\forall G(1 \leq G)$.

(ii) 所有 n 的倍数构成 $\mathbb{Z}$ 的子群, 称为 $n\mathbb{Z}$. 显然 $n\mathbb{Z} = \langle n\rangle$

(iii) $O_n = \{M \in GL_n(\mathbb{R}) : M^T = M^{-1}\} \leq \mathrm{GL}_n(\mathbb{R})$, 称作 orthogonal group, 是 $\mathbb{R}^n$ 的所有线性保距变换 (isometry). 同样我们有 $U_n = \{M \in GL_n(\mathbb{C}) : M^* = M^{-1}\}$, 称作 unitary group.

(iii) (dihedral group) 给定正整数 n 定义

$$D_{2n} := \left\langle \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \right\rangle \leq O_2$$

即反射与旋转 $\frac{2\pi}{n}$ 生成的子群. 这是平面上正 n 边形的所有线性保距对称.

(iv) (fixed group) 若 F 是 K 的 extension, E 是 intermediate field, 那么 $E' := \{\sigma \in \mathrm{Gal}_K(F) : \forall x \in E(\sigma(x) = x)\} \leq \mathrm{Gal}_K(F)$. Galois theory 的最基本定理是若 F galois over K, 那么 $E \mapsto E'$ 是 intermediate field 集合到 $\mathrm{Gal}_K(F)$ 的所有子群的集合的双射.

接下来是 homomorphism 的例子.

(i) 对任意群 G 我们都有唯一的 homomorphism $G \to 1 : g \mapsto 1$, 也有唯一的 homomorphism $1 \to G : 1 \mapsto 1$(注意群非空!), 了解过 category 的读者应知道这意味着 1 是 terminal 与 initial object.

(ii) 若 $H \leq G$, $i : H \to G : x \mapsto x$. 我们通常称之为 inclusion, 记作 $i : H \hookrightarrow G$.

(iii) 若 $f : G \to H$ 是 homomorphism, $K \leq G$, $f \restriction K$ 是 homomorphism(注意 $f \restriction K = fi$, $i : K \hookrightarrow G$). 有时我们直接简写 $f : K \to H$.

(iv) 若 $G \leq GL_n(F)$, $\det : G \to F^*$, 其中 $F^* := \{x \in F : x \neq 0\}$, 乘法为 F 的乘法. $G = GL_n(F)$ 时 $SL_n(F) := \ker\det$, 称为 special linear group. $G = O_n$ 时 $\ker\det = SO_n$, special orthogonal group; $G = U_n$ 时 $\ker\det = SU_n$, special unitary group.

接下来两个例子较不显然, 我们详细解释:

命题 1.13 若 $|X| = |Y|$, 则 $\mathrm{Sym}(X) \simeq \mathrm{Sym}(Y)$.

证明由于 $|X| = |Y|$, 取一个双射 $f : X \to Y$. 考虑映射 $F : \mathrm{Sym}(X) \to Y^Y : \sigma \mapsto f\sigma f^{-1}$.

首先我们证明 $\mathrm{Im}f \subset \mathrm{Sym}(Y)$ - $f\sigma f^{-1}$ 的逆映射为 $f\sigma^{-1}f^{-1}$: $f\sigma f^{-1}f\sigma^{-1}f^{-1} = f\sigma\sigma^{-1}f^{-1} = ff^{-1} = \mathrm{id}_Y$, 反面同理.

接着 F 是 homomorphism: $F(\sigma\tau) = f\sigma\tau f^{-1} = f\sigma f^{-1} f\tau f^{-1} = F(\sigma)F(\tau)$.

最后同理 $G : \mathrm{Sym}(Y) \to \mathrm{Sym}(X) : \tau \mapsto f^{-1}\tau f$ 是 homomorphism, 且显然 F, G 互为逆. □

评论大多数证明 isomorphic 的命题思路都是简单直接的构造映射与逆映射, 且大多时候构造只有一条自然的路可走. 如本命题中给定 $\sigma \in \mathrm{Sym}(X)$, 双射 $f : X \to Y$, 想要构造 $Y \to Y$ 的最直接想法就是 $Y \xrightarrow{f^{-1}} X \xrightarrow{\sigma} X \xrightarrow{f} Y$.

于是当 $|X| = n$ 时统称 $\mathrm{Sym}(X)$ 为 S_n, 并且一般取 $\mathrm{Sym}(\{1, ..., n\})$ 作为代表. 不过接下来我们要定义的重要 homomorphism 依赖于命题 1.13:

定义 1.14 $\mathrm{sgn} : S_n \to \mathbb{R}^*$ 是下列映射的合成:

$$S_n = \mathrm{Sym}(\{1, ..., n\}) \xrightarrow{F} \mathrm{Sym}(\{e_1, ..., e_n\}) \xrightarrow{\det} \mathbb{R}^*$$

其中 e_i 是 $\mathbb{R}^n$ 的标准 basis, F 是双射 $f : i \mapsto e_i$ 如命题 1.13 中生成的 isomorphism.

$A_n := \ker \mathrm{sgn} \leq S_n$ 被称为 alternate group.

由 determinant 的计算易得 $\mathrm{Im\ sgn} \leq \{-1, 1\}$, 当 $n \geq 2$ 时取等. 事实上 sgn 的定义不依赖于 F 的选取: 若 g 是另一个双射, G 是 g 引出的 isomorphism, $\det G(\sigma) = \det gf^{-1}F(\sigma)(gf^{-1})^{-1}$, 而 $gf^{-1} \in \mathrm{Sym}(\{e_1, ..., e_n\})$ 定义在一组 basis 上, 于是可以引出一个 F 上的 linear map T 使得 $T(e_i) = gf^{-1}(e_i)$; $(gf^{-1})^{-1}$ 同理引出 linear map S, 并且 $TS = ST(e_i) = e_i$, 即 $TS = ST = \mathrm{id}_{\mathbb{R}^n}$, 所以 $\det G(\sigma) = \det T \det F(\sigma) \det T^{-1} = \det F(\sigma)$.

sgn 可以说是有限群中最重要的非自然 homomorphism, A_n 更是证明 $n \geq 5$ 次 polynomial equation 没有 radical solution formula 的最终工具.