抽象代数讲义

（2025 年 2 月更新）

张浩

湖南大学

Pour l'honneur de l'esprit humain—Jacobi

目录

第一章　集合论

1.1　分拆和等价关系

定义 1.1.1. 设 X 是一个集合，设 $\{X_i\}_{i\in I}$ 是 X 的一族非空子集。若其满足 $X=\cup_{i\in I}X_i$ 且对任意 $i\neq j$，$X_i\cap X_j=\emptyset$，那么我们称 $\{X_i\}_{i\in I}$ 是 X 的一个**分拆**，或者称 X 为 $\{X_i\}_{i\in I}$ 的**无交并**，并记作 $X=\coprod_{i\in I}X_i$。

例 1.1.2. *1.* 集合 $X=\{1,2,3\}$ 恰好有五个分拆，分别为 $\{\{1,2,3\}\}$，$\{\{1\},\{2,3\}\}$，$\{\{2\},\{1,3\}\}$，$\{\{3\},\{1,2\}\}$，$\{\{1\},\{2\},\{3\}\}$。

2. 设 $X=\mathbb{Z}$，n 是一个正整数，X_i 为所有和 i 模 n 同余的整数组成的集合。那么 $X_0,X_1,\ldots,X_{n-1}$ 是 X 的一个分拆。

3. 设 $f:X\to Y$ 为一个映射，若 $y\in Y$ 包含在 f 的像中，记

$$X_y=f^{-1}(\{y\})=\{x\in X\mid f(x)=y\}.$$

那么这些 X_y 便组成 X 的一个分拆，并且集合称为 f 在 y 处的**纤维**。

定义 1.1.3. 设 X 是一个集合，我们称 $X\times X$ 的一个子集 R 为一个关系，若 $(x,y)\in R$，我们称 x,y 具有关系 R 并记作 xRy。若关系 R 还满足如下三个条件，

1. 反身性：对任意 $x\in X$，均有 xRx；
2. 对称性：对任意 $x,y\in X$，若 xRy，那么 yRx；
3. 传递性：对任意 $x,y,z\in X$，若 xRy,yRz，那么 xRz。

那么我们称关系 R 为一个**等价关系**。若 x,y 等价，我们记为 $x\sim y$。

对任意 $x\in X$，我们记 $[x]_R=\{y\in X\mid yRx\}$ 为 x 的等价类，那么这些等价类便给出了 X 的一个划分。

命题 1.1.4. 若 R 是集合 X 上的一个等价关系，那么它的所有等价类构成 X 的一个划分。

反之，任意给定一个划分 $X=\coprod_{i\in I}X_i$，我们均可定义一个等价关系使得 X_i 恰好是所有的等价类。

例 1.1.5. *1.* 整数模 m 同余是一个等价关系，即对任意整数 a,b，a 和 b 等价当且仅当 $a-b$ 是 m 的倍数，此时我们称 a 和 b 关于模 m **同余**。

2. 矩阵的相抵，相似，合同关系均是等价关系。

3. 记 $\mathcal{P}=\{(x_n)\in\mathbb{Q}^{\mathbb{N}}\mid (x_n)$构成 *Cauchy* 列$\}$，$\mathcal{P}$ 中两个数列 $(x_n),(y_n)$ 等价当且仅当它们是等价的 *Cauchy* 列，即对任意 $\varepsilon>0$，存在 $N>1$ 使得对任意 $n>N$，均有 $|x_n-y_n|<\varepsilon$。

4. 我们在集合 $\{0,1\}^{\mathbb{N}}$ 上定义如下关系：(x_n) 和 (y_n) 等价当且仅当存在 $N>1$ 使得对任意 $n>N$ 均有 $x_n=y_n$。可以验证这是一个等价关系。

5. 设 V 是 $\mathbb{R}$ 上的线性空间，$X=V\setminus\{0\}$，我们在集合 X 定义如下关系，对于 $\alpha,\beta\in X$，α,β 等价当且仅当存在非零实数 λ 使得 $\alpha=\lambda\beta$，可以验证这个关系是一个等价关系。

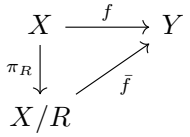
例 1.1.6. 设 $f:X\to X$ 是一个双射，我们在 X 上定义一个等价关系为 x 和 y 等价当且仅当存在 $i\in\mathbb{Z}$ 使得 $y=f^i(x)$，这里当 $i=0$ 时，f^0 为恒等映射，$i>0$ 时，$f^i:=f\circ f\cdots\circ f$ 为 i 个 f 的复合，当 $i<0$ 时，f^i 为 $-i$ 个 f^{-1} 的复合。我们下面验证这是一个等价关系。取 $i=0$ 即可知该关系满足反身性。而 $y=f^i(x)\iff x=f^{-i}(x)$，故该关系满足对称性。由 $f^i(f^j(x))=f^{i+j}(x)$ 可知该关系满足传递性。那么该等价关系的等价类是什么呢？这需要分两种情况讨论，第一种是对任意的 $i\in\mathbb{Z}$，$f^i(x)$ 均不相同，那么 x 所在的等价类即为 $\{x,f^{\pm1}(x),f^{\pm2}(x),\dots\}$。第二种情况是存在 $i<j$ 使得 $f^i(x)=f^j(x)$，那么我们记 $d=j-i$ 是使得 $f^i(x)=f^j(x)$ 成立最小的正整数。那么我我们可以证明当 $d\mid a-b$ 时有 $f^a(x)=f^b(x)$，因此 x 所在的等价类为 $\{x,f(x),f^2(x),\dots,f^{d-1}(x)\}$。这个例子实际上是群作用的一个特例，同时也和对称群有着密切的联系，我们将在后面的例子中多次看到它的影子。

1.2 商集

定义 1.2.1. 设 R 是集合 X 上的一个等价关系，我们记 X/R 为 X 的所有等价类的集合，即 $X/R=\{[x]_R\mid x\in X\}$。我们称 X/R 为 X 在 R 下的**商集**。我们称映射 $\pi_R:X\to X/R$，$x\mapsto[x]_R$ 为**投影映射**。

在不会引起混淆的情况下，后面我们将会把 $[x]_R$ 简记为 $\bar{x}$。上述定义是从集合论的语言来描述商集，事实上，我们可以从泛性质的角度来描述商集。

命题 1.2.2. 设 R 是 X 上的一个等价关系，$f:X\to Y$ 是一个映射。若 f 在每个等价类上是常值，即对任意 $x,y\in X$，若 xRy，则有 $f(x)=f(y)$。那么存在唯一的映射 $\bar{f}:X/R\to Y$ 使得 $f=\bar{f}\circ\pi_R$，即有如下交换图表



证明. 我们先构造映射 $\bar{f}$。对任意 $\bar{x}\in X/R$，我们定义 $\bar{f}(\bar{x})=f(x)$。若取另一个元素 $y\in X$，若 $\bar{y}=\bar{x}$，即有 xRy，那么根据已知有 $f(x)=f(y)$，因此 $\bar{f}(\bar{y})=\bar{f}(/\bar{x})$。这表明 g 是定义良好的。根据定义对任意 $x\in X$ 均有 $(\bar{f}\circ\pi_R)(x)=\bar{f}(\pi_R(x))=\bar{f}(\bar{x})=f(x)$。因此有 $\bar{f}\circ\pi_R=f$。

下面我们再证明唯一性。若存在 $h:X/R\to Y$ 满足 $f=h\circ\pi_R$，那么对任意 $x\in X$ 均有

$$\bar{f}(\bar{x})=(\bar{f}\circ\pi_R)(x)=f(x)=(h\circ\pi_R)(x)=h(\bar{x}).$$

故有 $\bar{f} = h$。

例 1.2.3. 例1.1.5中的第一个例子，我们通常记其商集为 $\mathbb{Z}/m\mathbb{Z}$。这个例子也是抽象代数这门课程中非常重要的一个例子。对于第三个例子，其商集可以视作实数的定义。对于第五个例子，每个向量 α 所在的等价类即为所有和 α 共线的向量组成的集合。从几何上来看，X 在该等价关系下的等价类即为所有过原点的直线。该商集我们称之为n **维射影空间**，记作 $\mathbb{P}^n(V)$。

例 1.2.4 (收缩)**.** 设 A 是 X 的一个子集,我们定义 X 上的一个等价关系为:$xRy \iff x = y$ 或$x, y \in A$，即 A 中所有元素互相等价，而不在 A 中的元素则两两不等价。那么投影映射 $\pi_R : X \to X/R$ 可以视作将 A 收缩至一个点。例如我们假设 $X = [0, 1], A = \{0, 1\}$，那么 X/R 便自然的等同于和单位圆。因为我们考虑如下映射 $f : X \to S^1$，$x \mapsto \mathrm{e}^{2\pi \mathrm{i} x}$，那么我们有 $f(0) = f(1)$。因此根据命题1.2.2可诱导映射 $g : X/A \to S^1$。容易验证该映射是一个双射。

在这门课程中，我们将多次构造不同代数结构的商集，并且将赋予商集对应的代数结构。

1.3 选择公理和 Zorn 引理

假设我们有 n 个篮子，每个篮子里面都有若干个球（球的个数大于等于 1），那么我们一定可以从每个篮子里面选一个球出来。方法也很简单，我们只需要将篮子从 1 到 n 编号，然后按照编号一个一个的取，便可做到不重复不遗漏的从每个篮子中选一个球出来。但是如果篮子的个数变成无限个呢? 上面的方法是否还能使用呢? 一个问题便是无穷个篮子能否还能按照编号 $1, 2, 3, \ldots$ 一直排下去。事实上，无穷也会有大小之分，如果能按照编号 $1, 2, 3, \ldots$ 一直排下去，我们便称这是可数无穷，否则称为不可数的。例如自然数，整数都是可数的。Cantor 利用著名的对角线法证明了实数集是不可数的。回到刚才的问题我们就能发现如果篮子的个数是可数无穷的，那么之前的方法还能继续使用，但是如果变成不可数的，则无法使用了。数学家们惊讶地发现对于一般的情况，我们既无法证明一定能选出一个球，也无法证明选不出来，但是这样的结论却又如此的直观，因此我们便将它作为公理使用，称之为选择公理。下面我们用数学语言来严格地描述选择公理。设 X 是一个非空集合，$P(X)$ 是 X 的所有子集组成的集合。

公理 (选择公理)**.** 对任意集合 X，存在映射 $\tau : P(X) \setminus \emptyset \to X$ 使得对任意 X 的非空子集 E 均有 $\tau(E) \in E$。

我们把 τ 称作 X 上的**选择函数**。如果我们把 X 的一个非空子集看作一个篮子，子集里面的一个元素看作一个球，那么 $\tau(E) \in E$ 即表明我们能从每个篮子中选出一个球。选择公理有许多等价形式，我们将介绍几个我们将会经常用到的等价命题。

命题 1.3.1. 选择公理等价于如下命题：对任意非空集族 $\{X_i\}_{i \in I}$，其乘积 $\prod_{i \in I} X_i$ 是非空的。

最后我们再介绍选择公理的另一个等价形式：Zorn 引理。为此我们需要先给出一些定义。

定义 1.3.2. 设 R 是集合 X 上的一个关系，若它满足反身性，传递性，以及如下性质：

$$\textbf{反对称性：} \forall x, y \in X, xRy, yRx \implies x = y.$$

那么我们称关系 R 为一个**偏序关系**，记作 $\leq$。具有偏序关系的集合我们称为**偏序集**。若 X 还满足对任意 $x, y \in X$，均有 $x \leq y$ 或者 $y \leq x$，那么我们称 X 为**全序集**。

例 1.3.3. 实数集在通常的序关系下构成一个全序集。而对于复数集，我们可以如下关系：

$$\forall a+b\mathrm{i}, c+d\mathrm{i} \in \mathbb{C}, a+b\mathrm{i} \leq c+d\mathrm{i} \iff (b<d) \vee (b=d, a \leq c).$$

容易验证上述关系是复数集上的全序关系，我们称之为**字典序**。更一般地，我们可以考虑笛卡尔积 $X = \mathbb{R}^n$，对于 $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in X$，设 k 是使得 $a_k \neq b_k$ 的最小下标，我们定义其序关系为 $(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n) \iff k$ 不存在或 $a_k < b_k$。通俗来讲，即将 $(a_1, \ldots, a_n)$ 和 $(b_1, \ldots, b_n)$ 从左至右对每个分量逐一比较大小。

例 1.3.4. 正整数在整除关系下构成一个偏序集，即对任意正整数 m, n，我们定义 $m \leq n \iff m \mid n$。因为并不是任意两个正整数之间都存在整除关系，因此这不构成一个全序集。

例 1.3.5. 设 X 是一个非空集合，我们在其子集族 $P(X)$ 上定义如下关系：

$$\forall A, B \in P(X), A \leq B \iff A \subseteq B.$$

容易验证上述关系是 $P(X)$ 上的偏序关系，但是一般而言这不是全序。

定义 1.3.6. 设 $(X, \leq)$ 是一个偏序集，$x \in X$。若对任意 $y \in X$ 且 $x \leq y$ 必有 $x = y$，则称 x 为一个**极大元**。若对任意 $y \in X$ 均有 $y \leq x$，则称 x 为**最大元**。设 X' 是 X 的非空子集，若 $x \in X$ 满足对任意的 $x' \in X'$ 均有 $x' \leq x$，则称 x 是 X' 的一个**上界**。

容易看出最大元一定是极大元，但极大元不一定是最大元，更一般地，若最大元存在，那么一定是唯一的，而若 X 不是全序集，极大元有可能不是唯一的。例1.3.3中的两个全序集均不存在极大元。而例1.3.5中的偏序集则存在唯一的极大元 X。但是如果我们考虑集合 $P_1(X) = P(X) \setminus \{X\}$，它在包含关系下也构成一个偏序集，但是它的极大元则不唯一，X 减去任意一个元素都是极大元。最后我们介绍 Zorn 引理。

定理 1.3.7 (Zorn 引理)**.** 设 X 是一个偏序集，若它的任何一个全序子集都有上界，那么 X 有极大元。

选择公理和 Zorn 引理的等价性比较复杂，我们将不予证明，有兴趣的同学可参考这里。Zorn 引理在数学上有广泛的应用，例如线性代数中证明线性空间均存在一组基；泛函分析中的 Hahn-Banach 定理以及这门课中将会证明的极大理想的存在性以及代数闭域的存在性。作为一个简单的应用，下面我们将证明线性空间中基的存在性。

在证明该结论之前我们先回忆线性空间中的若干概念。设 V 是一个线性空间，$S \subseteq V$ 是一个非空子集。若 S 中的任意有限个向量均线性无关，那么我们称 S 是线性无关的。若 S 是线性无关的，并且 V 中任意一个向量均能通过 S 中的有限个向量线性表出，那么我们称 S 是一组基。

定理 1.3.8. 任意一个线性空间均存在一组基。

证明. 设 $\mathcal{P}$ 是 V 中所有线性无关的子集组成的集合。因为任意一个非零向量是线性无关的，因此 $\mathcal{P}$ 是非空的。那么 $\mathcal{P}$ 在集合的包含关系下构成一个偏序集。设 $\{S_i\}_{i \in I}$ 是 $\mathcal{P}$ 的一个全序子集，并设 $S_0 = \bigcup_{i \in I} S_i$。我们证明 S_0 是 $\{S_i\}_{i \in I}$ 的一个上界。首先对任意 S_0 中的有限个向量 $\alpha_1, \ldots, \alpha_n$，一定存在 $i \in I$ 使得 $\alpha_1, \ldots, \alpha_n \in S_i$，而 S_i 是线性无关的，因此 $\alpha_1, \ldots, \alpha_n$ 是线性无关的，故 S_0 也是线性无关的，所以 $S_0 \in \mathcal{P}$。另一方面，对任意的 $i \in I$，显然有 $S_i \leq S_0$，因此 S_0 是一个上界。故由 Zorn 引理知 $\mathcal{P}$ 存在极大元，设为 S。下面我们证明 S 是一组基。根据定义知 S 是线性无关的，若存在 $\alpha \in V$ 使得 α 不能被 S 中任意有限个向量线性表出，那么 $S \cup \{\alpha\}$ 仍然是线性无关的，但这与 S 是极大元矛盾。因此 S 构成一组基。

注 1. 同样的方法也可以证明任意一个线性无关的子集均可扩充为一组基。但是 Zorn 引理只能保证基的存在性，一般而言要构造一组基则是非常困难的事，甚至是无法具体构造出来的。

习题

练习 1.3.1. 设 $\Omega = \coprod_{i=1}^{s} P_i = \coprod_{j=1}^{t} Q_j$ 是集合 Ω 的两个划分，若对任意 $i = 1, 2, \ldots, s$，均存在 $J_i \subseteq \{1, 2, \ldots, t\}$ 使得

$$P_i = \bigcup_{j \in J_i} Q_j.$$

那么我们称划分 $\{Q_1, \ldots, Q_t\}$ 是划分 $\{P_1, \ldots, P_s\}$ 的加细，并记作 $P \leq Q$。设 $\mathcal{P}_n$ 是集合 $\{1, 2, \ldots, n\}$ 所有划分组成的集合。证明 $\leq$ 是 $\mathcal{P}_n$ 上的一个偏序关系。

练习 1.3.2. 设 $D < 0$ 是一个整数，记 $\mathcal{A}_D$ 为所有判别式为 D 的整系数二元二次型组成的集合，即形如 $ax^2 + bxy + cy^2$ 且满足 $a, b, c \in \mathbb{Z}, b^2 - 4ac = D$ 的二次型。我们在 $\mathcal{A}_D$ 上定义如下关系：

$$f(x, y) \sim g(x, y) \iff \text{存在整数 } p, q, r, s \text{ 使得} f(x, y) = g(px + qy, rx + sy) \text{ 且 } ps - qr = 1.$$

1. 证明上述关系是一个等价关系。
2. 证明商集 $\mathcal{A}_D/\sim$ 是有限集。
3. 计算商集 $\mathcal{A}_{-8}/\sim, \mathcal{A}_{-12}/\sim, \mathcal{A}_{-20}/\sim$ 的元素个数。

第二章　群

2.1　群的概念及例子

2.1.1　群的概念

定义 2.1.1. 设 G 是一个具有二元运算 $\cdot$ 的非空集合，如果它满足如下三条性质：

1. $(a\cdot b)\cdot c = a\cdot(b\cdot c), \qquad \forall a,b,c\in G.$

2. 存在元素 $e\in G$ 使得对任意 $a\in G$ 均有

$$e\cdot a = a\cdot e = a.$$

   元素 e 被称为**单位元**，有时我们也会用 1 表示单位元。

3. 对任意 $a\in G$，均存在元素 $b\in G$ 使得

$$a\cdot b = b\cdot a = e.$$

   元素 b 被称为 a 的**逆元**。

我们则称 G 为一个群。特别地，如果对于 $a,b\in G$，均有 $a\cdot b = b\cdot a$，我们则称 a,b **可交换**。若对任意 $a,b\in G$，a,b 均可交换，则称 G 为**交换群**或者 **Abel 群**。在不会混淆的情况下，我们通常将 $a\cdot b$ 记为 ab。若 G 的元素个数有限，我们则称 G 为**有限群**，并称其元素个数为 G 的**阶**，记作 $|G|$。

例 2.1.2. *1.* 我们常见的数集 $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ 对通常意义下数的加法构成群，其中 0 是单位元，任意元素 a 的逆元是 $-a$。

2. 如果我们记 $\mathbb{Q}^*,\mathbb{R}^*,\mathbb{C}^*$ 分别为 $\mathbb{Q},\mathbb{R},\mathbb{C}$ 去掉 0 元素以后形成的集合，则这些集合关于通常意义下数的乘法构成群，其中 1 是单位元，任意元素 a 的逆元是 $1/a$。但是整数集 $\mathbb{Z}$ 去掉 0 以后关于乘法并不构成一个群！例如 2 的在整数集中不存在逆元。

3. 域 $\mathbb{C}$ 上的所有 n 阶可逆矩阵构成的集合 $\mathrm{GL}_n(\mathbb{C})$ 在矩阵乘法下也构成一个群，但这个群不是交换群。

4. 集合 $\{1,2,\ldots,n\}$ 到自身的所有双射组成的集合在映射的复合下构成一个群。当 $n>2$ 时，这个群也不是交换群。

5. 设 m 是一个正整数，我们可以在 $\mathbb{Z}/m\mathbb{Z}$ 上定义一个群结构（$\mathbb{Z}/m\mathbb{Z}$ 的定义见1.2.3）。记 $\mathbb{Z}/m\mathbb{Z}$ 的元素分别为 $\overline{0},\overline{1},\ldots,\overline{m-1}$，对任意 $\overline{a},\overline{b}\in\mathbb{Z}/m\mathbb{Z}$，我们定义 $\overline{a}+\overline{b}=\overline{c}$，其中 c 是 $a+b$ 除以 m 的余数。可以验证 $\mathbb{Z}/m\mathbb{Z}$ 构成一个加法群，其中单位元是 $\overline{0}$，非单位元 $\overline{a}$ 的逆元为 $\overline{m-a}$。

6. 设 m 是一个正整数，我们记 $(\mathbb{Z}/m\mathbb{Z})^*=\{\overline{a}\mid 1\le a\le m-1,\text{且}a\text{和}m\text{互素}\}$。对任意 $\overline{a},\overline{b}\in(\mathbb{Z}/m\mathbb{Z})^*$，我们定义 $\overline{a}\cdot\overline{b}=\overline{c}$，其中 c 为 ab 除以 m 的余数。可以验证 $(\mathbb{Z}/m\mathbb{Z})^*$ 构成一个乘法群，其中单位元是 $\overline{1}$。逆元的存在性可由初等数论中的 *Bézout* 定理确定。

下面我们将给出更多抽象群的例子。在此之前，我们先给出群的一些基本性质。

命题 2.1.3. 设 G 是一个群，那么

1. 单位元是唯一的；

2. 逆元是唯一的；

3. 对任意 $a,b\in G$，均有 $(a^{-1})^{-1}=a$ 及 $(ab)^{-1}=b^{-1}a^{-1}$；

4. 对任意 $a_1,a_2,\ldots,a_n\in G$，$a_1\cdot a_2\cdots a_n$ 并不依赖于运算的次序。

证明. 1. 若 e_2,e_2 都是群 G 的单位元，那么根据定义可知 $e_1=e_1e_2=e_2$。因此单位元是唯一的。

2. 若 a_1,a_2 都是元素 a 的逆，那么根据定义可知 $a_1=a_1e=a_1(aa_2)=(a_1a)a_2=ea_2=a_2$。因此逆元也是唯一的。

3. 由于 $aa^{-1}=a^{-1}a=e$, 因此 a 是 a^{-1} 的逆元, 即有 $(a^{-1})^{-1}=a$。$(b^{-1}a^{-1})(ab)=((b^{-1}a^{-1})a)b=(b^{-1}(a^{-1}a))b=(b^{-1}e)b=b^{-1}b=e$。同理可证 $(ab)(b^{-1}a^{-1})=e$。因此 ab 的逆元即为 $b^{-1}a^{-1}$。

5. 我们对 n 归纳证明 $a_1\cdot a_2\cdots a_n$ 通过任意次序做运算均可得到 $a_1\cdot(a_2\cdot(\cdots(a_{n-1}\cdot a_n)\cdots))$。当 $n=1,2,3$ 时，结论显然成立，下面假设 $n>3$。我们注意到任意运算次序，我们最终都能分成两部分 $(a_1\cdots a_k)\cdot(a_{k+1}\cdots a_n)$，其中这两部分均通过某种运算次序得到。根据归纳假设可知上述乘积等于

$$(a_1\cdot(\cdots(a_{k-1}\cdot a_k)\cdots))\cdot(a_{k+1}\cdot(\cdots(a_{n-1}\cdot a_n)\cdots)).$$

利用结合律，上述乘积等于

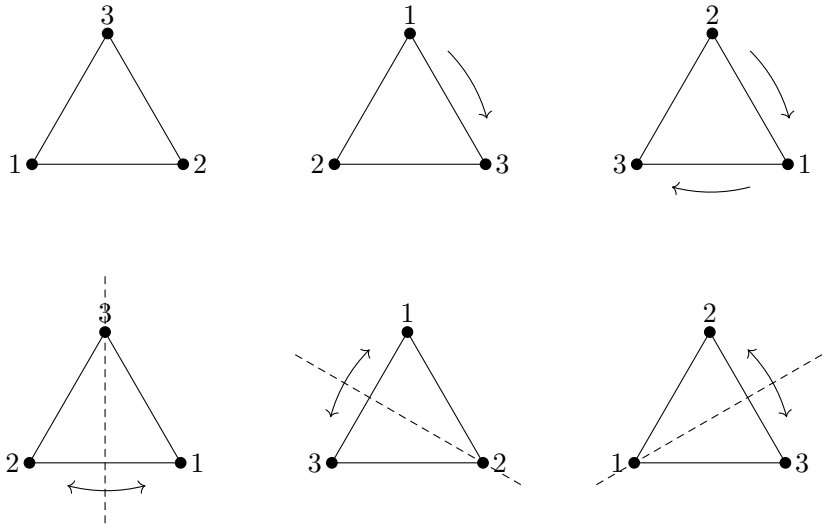
$$a_1\cdot((a_2\cdot(\cdots(a_{k-1}\cdot a_k)\cdots))\cdot(a_{k+1}\cdot(\cdots(a_{n-1}\cdot a_n)\cdots))).$$

最后我们再次利用归纳假设可以知道上述乘积等于 $a_1\cdot(a_2\cdot(\cdots(a_{n-1}\cdot a_n)\cdots))$。

注 2. 设 G 是一个群，$g\in G$，n 是一个正整数。我们记 $g^n:=\underbrace{gg\ldots g}_{n\text{个}}$，$g^0$ 为单位元，而 $g^{-n}:=(g^{-1})^n$。容易证明在该记号下，我们有 $g^n\cdot g^{-n}=e$。并且该记号也满足我们通常意义下的指数运算，即对任意 $n,m\in\mathbb{Z}$，均有 $g^n\cdot g^m=g^{n+m}$ 及 $(g^n)^m=g^{nm}$。类似地，在一些常见的加法群 G 中，我们也同样定义：$ng:=\underbrace{g+g+\cdots+g}_{n\text{个}},0\cdot g=0$ 以及 $(-n)a:=n(-a)$。需要注意的是在 $0\cdot g=0$ 中左边的 0 代表的是数字 0，而右边的 0 是群 G 中的单位元。该记号同样也满足通常的乘法和加法的分配率，即 $ng+mg=(n+m)g,m(ng)=(mn)g$。

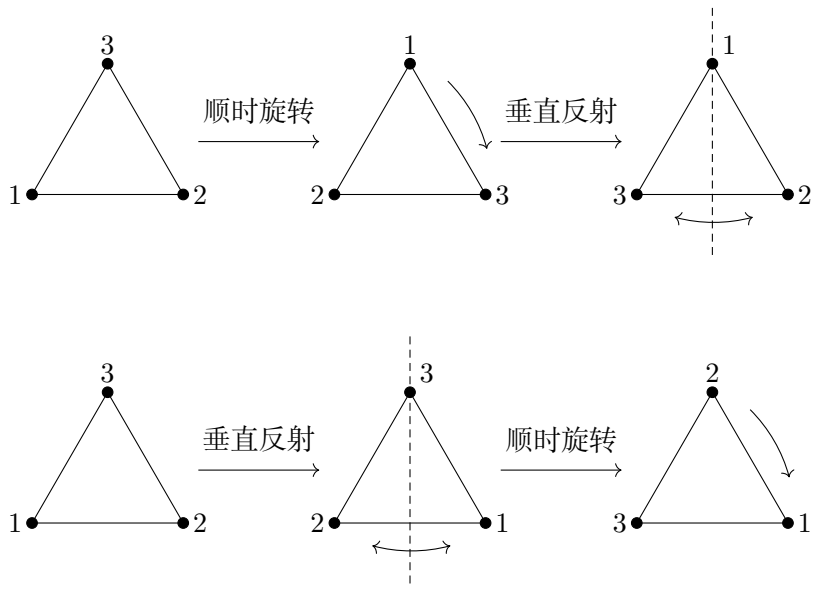
2.1.2 二面体群

考虑一个正 n 边形，假设 n 个顶点编号依次为 $1,2,\ldots,n$，若三维空间中的一个刚体变换将该正 n 变形变到自身，即只改变了顶点的位置，但任意两个顶点之间的距离不发生改变，那么我们称这个刚体变换为正 n 边形的一个对称，我们记正 n 边形的所有对称组成的集合为 D_{2n}。例如下图展示了正三角形的所有对称。



第一排的第二个为第一个顺时针旋转 120° 得到，第三个由第一个旋转 240° 得到，而第二排的每个三角形均由上一排第一个沿着对应的虚线翻折得到。

我们可以在 D_{2n} 上定义运算为变换的复合。由于刚体变换可以视作从标号集合 $\{1,2,\ldots,n\}$ 到自身的一个双射，因此该二元运算是满足结合律的。另一方面，恒等变换也是 D_{2n} 中的一个元素，我们记为 1，容易看出 1 即为 D_{2n} 中的单位元。而 D_{2n} 中元素的逆元则可视作从标号集合 $\{1,2,\ldots,n\}$ 到自身双射的逆映射。因此 D_{2n} 在变换的复合下构成一个群，我们称之为**二面体群**。我们注意到这个群是非交换群。例如我们可以从图像上直接看出如下两个变换的复合是不交换的：



下面我们证明 D_{2n} 中恰有 $2n$ 个元素。事实上我们假设 $s \in D_{2n}$ 将标号 1 映射到了 k，那么标号 2 只能映射到 $k-1$ 或 $k+1$（在模 n 的意义下），若 2 映射到了 $k+1$，那么根据刚体变换的定义可知，3 只能映射到 $k+2$，以此类推，n 只能映射到 $k-1$；同样地，若 2 映射到了 $k-1$，那么 3 只能映射到 $k-2$，以此类推，n 只能映射到 $k+1$。这意味着整个刚体变换完全由 1 和 2 的像决定，而 1 有 n 个选择，当 1 固定后，2 至多有两个选择，所以 D_{2n} 中至多有 $2n$ 个元素。另一方面，将正 n 变形依次旋转 $\frac{2k\pi}{n}$，$k = 0, 1, \ldots, n-1$ 可以得到 n 个不同的刚体变换，然后将正 n 变形沿着某条对称轴翻折之后再依次旋转 $\frac{2k\pi}{n}$，$k = 0, 1, \ldots, n-1$ 又可以得到 n 个不同的刚体变换。综上所述 D_{2n} 恰有 $2n$ 个元素。

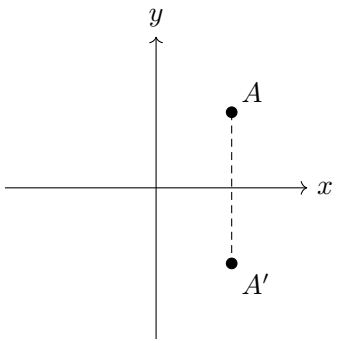
最后我们再从抽象群的角度来研究二面体群。设 r 为将正 n-边形旋转 $\frac{2\pi}{n}$，那么所有的旋转可以表示为 $1, r, r^2, \ldots, r^{n-1}$，并且 $r^n = 1$。我们再设 s 为沿着某条对称轴翻折的变换，那么显然有 $s^2 = 1$，并且有

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\},$$

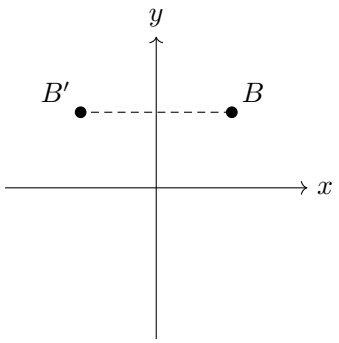
即 D_{2n} 中任意一个元素均可写成 $s^i r^j$ 的形式，其中 $i = 0, 1, j = 0, 1, \ldots, n-1$。

命题 2.1.4. *对任意 i 我们有 $r^i s = sr^{-i}$。*

类似地，我们可以考虑如下平面上的刚体变换。

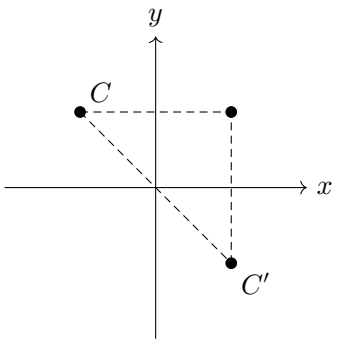


σ_x =沿x−轴作镜面反射



σ_y =沿y−轴作镜面反射

容易看出这两个变换和自身的复合是恒等变换，即 $\sigma_x \cdot \sigma_x = \sigma_y \cdot \sigma_y =$ 恒等变换。我们记这两个变换的复合为 σ_{xy}，容易看出 $\sigma_{xy} = \sigma_x \cdot \sigma_y = \sigma_y \cdot \sigma_x$，从几何上来看，$\sigma_{xy}$ 即为关于原点作对称：



σ_{xy} =关于原点作对称

我们考虑 σ_{xy} 和 σ_x 及 σ_y 的复合可以得到：

$$\sigma_{xy} \cdot \sigma_x = \sigma_x \cdot \sigma_{xy} = \sigma_y, \qquad \sigma_{xy} \cdot \sigma_y = \sigma_y \cdot \sigma_{xy} = \sigma_x.$$

于是这些变换 $\{1, \sigma_x, \sigma_y, \sigma_{xy}\}$ 构成一个交换群，我们称之为 **Klein 四元群**。

最后我们讨论一下群的表现。设 $S \subseteq G$，若 G 中任意一个元素均能写成有限个 S 中的元素或者它的逆的乘积，那么则称 S 是 G 的生成元集，或者 G 由 S 生成。例如 D_{2n} 是由 r, s 生成。生成元之间满足的方程都被称为**关系**。例如在 D_{2n} 中，$r^n = 1, s^2 = 1, rs = sr^{-1}$ 都是关系。更进一步，D_{2n} 中的任何关系都能用这三个关系表示出来，因为这三个关系唯一的决定了 D_{2n} 的所有元素。例如

$$r^2 s = r \cdot rs = r \cdot sr^{-1} = sr^{-1} \cdot r^{-1} = sr^{-2}.$$

一般地，如果群 G 可由 S 生成且 G 中元素的关系均可由关系 $R_1, R_2, \ldots, R_m$ 得到，那么我们称生成集合 S 和关系 $R_1, R_2, \ldots, R_m$ 为群 G 的一个**表现**，记为

$$G = \langle S \mid R_1, R_2, \ldots, R_m \rangle.$$

例如 $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$。一个群的表现显然不是唯一的，例如 D_{2n} 还有如下表现：

$$\langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle.$$

它和上一个表现的联系是 $a = s, b = sr$。而 $G = \langle x, y \mid x^2 = y^2 = (xy)^2 = 1 \rangle$ 则是上面所述的 Klein 四元群。

2.1.3 对称群

这一节我们介绍另一类非常重要的群：对称群。

设 X 是任意非空集合，令 S_X 为所有 X 到自身的双射组成的集合。S_X 在映射的复合下构成一个群，我们称之为**对称群**，S_X 中的元素我们称之为**置换**。特别地，若 $X = \{1, 2, \ldots, n\}$，我们将简记为 S_n。

命题 2.1.5. *设 n 为一个正整数，那么 $|S_n| = n!$。*

我们知道 S_n 中的元素是 $\{1, 2 \ldots, n\}$ 到自身的双射，因此要唯一确定一个元素需要知道每个元素的像，然而这样描述 S_n 中的元素过于麻烦，因此我们介绍一种简单的表达形式：轮换分解。

假设 $\sigma \in S_n$，我们考虑如下序列：

$$1 \to \sigma(1) \to \sigma(\sigma(1)) \to \ldots$$

我们注意到由于 n 是有限的数字，因此上述序列总会回到 1，例如我们考虑下面这样一个映射 $\sigma \in S_{10}$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 9 & 5 & 8 & 6 & 4 & 7 & 10 & 2 \end{pmatrix},$$

这里第一排代表 σ 的原像，而第二排则代表第一排的像。那么 1 的像是 3，3 的像是 9，9 的像是 10，10 的像是 2，2 的像是 1，因此上面的序列便是

$$1 \to 3 \to 9 \to 10 \to 2 \to 1.$$

因此这样一个序列我们可以简记为 (1 3 9 10 2)，这样记号代表后一个数字是前一个数字在 σ 下的像，而第一个数字是最后一个数字在 σ 下的像，我们称这样一种表示为一个**轮换**，若该轮换中有 m 个元素，

则称为 m-**轮换**。例如 (1 3 9 10 2) 是一个 5-轮换。但是我们要注意到 σ 的原像集总共有 10 个元素，而上面的轮换只包含了 5 个元素，因此为了把其它元素囊括尽来，我们还需要再考虑其它的轮换。不难发现 (4 5 8 7) 也是一个轮换，而 (6) 自己则单独形成一个轮换。最终我们用三个轮换便完全确定了 σ，因此我们可以使用如下记号表示 σ

$$(1\ 3\ 9\ 10\ 2)(4\ 5\ 8\ 7)(6).$$

事实上，利用例1.1.6的语言我们知道集合上述三个轮换分别为双射 σ 对应的三个等价类。根据上面的方法我们很容易看出 S_n 中的元素都可以写成若干个轮换的形式，并且在不考虑顺序的情况下表示方法是唯一的。而如果一个轮换只有一个元素的话，我们不需要写出来也知道它是把自身映射到自身，因此我们可以把它省略不写，因此上面的记号我们可以简写成

$$(1\ 3\ 9\ 10\ 2)(4\ 5\ 8\ 7).$$

而单位元我们则直接简写成 (1)。我们把这样的表达方式称为**轮换分解**。下表展示了 S_5 中若干个元素的轮换分解。

σ	σ 的轮换分解
$\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\1&2&3&4&5\end{smallmatrix}\right)$	(1)
$\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\2&1&3&4&5\end{smallmatrix}\right)$	(1 2)
$\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\2&3&1&4&5\end{smallmatrix}\right)$	(1 2 3)
$\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\2&3&4&1&5\end{smallmatrix}\right)$	(1 2 3 4)
$\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\2&3&4&5&1\end{smallmatrix}\right)$	(1 2 3 4 5)
$\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\2&1&4&3&5\end{smallmatrix}\right)$	(1 2)(3 4)
$\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\2&1&4&5&3\end{smallmatrix}\right)$	(1 2)(3 4 5)

表 2.1: S_5

最后我们再介绍如何利用这个记号来做运算。逆运算非常的简单，根据定义 σ^{-1} 是把像映射到原像，因此在轮换分解中我们只需要把轮换倒过来即可，例如 $\sigma = (1\ 3\ 9\ 10\ 2)(4\ 5\ 8\ 7)$，那么 $\sigma^{-1} = (2\ 10\ 9\ 3\ 1)(7\ 8\ 5\ 4)$。而元素的乘法即为映射的复合，映射的复合需要先作用右侧的映射，再作用左侧的映射，因此元素乘法的轮换分解需要将两个元素的轮换分解从右往左依次读取出来。例如 $\sigma = (1\ 3\ 9\ 10\ 2)(4\ 5\ 8\ 7), \tau = (1\ 2\ 5\ 9)(3\ 4)(6\ 10)$，那么

$$\sigma \circ \tau = (1\ 3\ 9\ 10\ 2)(4\ 5\ 8\ 7)(1\ 2\ 5\ 9)(3\ 4)(6\ 10),$$

我们再依次将右边的乘积依次写成轮换分解的形式，例如 1 在从右到左的第三个轮换中映射到了 2，而 2 在从右到左的第五个轮换中映射到了 1，因此在整个乘积中，1 映射到了自身，然后再考虑 2，2 从右到左的第三个轮换中映射到了 5，5 在从右到左的第四个轮换中映射到了 8，因此在整个乘积中，2 映射到了 8，接下来考虑 8，同样的方法可以看出 8 映射到了 7，7 映射到了 4，4 映射到了 9，9 映射到了 3，3 映射到了 5，5 映射到了 10，10 映射到了 6，6 映射到了 2，因此我们便得到了 $\sigma \circ \tau$ 的轮换分解为

$$(2\ 8\ 7\ 4\ 9\ 3\ 5\ 10\ 6).$$

同样的方法我们可以计算

$$\tau \circ \sigma = (1\ 2\ 5\ 9)(3\ 4)(6\ 10)(1\ 3\ 9\ 10\ 2)(4\ 5\ 8\ 7) = (1\ 4\ 9\ 6\ 10\ 5\ 8\ 7\ 3).$$

从定义也可以看出每个轮换其实也代表着 S_n 中的一个元素，并且如果两个循环没有公共的数字，那么这两个轮换是可以交换的。通过将不交的轮换交换顺序，我们不妨假设 $\sigma \in S_n$ 可以分解为长度分别为 $n_1, n_2, \ldots, n_r$ 的轮换的乘积，其中 $1 \leq n_1 \leq n_2 \leq \cdots \leq n_r$。我们称 $n_1, n_2, \ldots, n_r$ 为 σ 的**轮换类型**。容易验证表2.1展示了 S_5 中所有可能的轮换类型。

2.1.4 矩阵群和四元数群

设 V 是 $\mathbb{R}$ 上的 n 维线性空间。我们记 $\mathrm{GL}(V)$ 为 V 到自身的所有可逆线性变换组成的集合。那么 $\mathrm{GL}(V)$ 在映射的复合下构成一个群，我们称之为 V 上的**一般线性群**。但一般而言，它不是交换群。类似地，我们可以定义 $\mathrm{SL}(V)$ 为 $\mathrm{GL}(V)$ 中所有行列式等于 1 的线性变换构成的集合，那么 $\mathrm{SL}(V)$ 也构成一个乘法群。我们称之为域 F 上的**特殊线性群**。如果我们选定 V 的一组基，那么 $\mathrm{GL}(V)$ 便可视为所有的 n 阶可逆实矩阵组成的集合，而 $\mathrm{SL}(V)$ 则为所有行列式等于 1 的实矩阵组成的集合。此时我们将一般线性群和特殊先行区分别记为 $\mathrm{GL}(n), \mathrm{SL}(n)$。

如果我们取 V 为 n 为欧式空间，$(\cdot,\cdot)$ 为 V 上的内积。我们可以定义 V 上的**正交群**为

$$\mathrm{O}(V) = \{g \in \mathrm{GL}(V) \mid (gx, gy) = (x, y), \forall x, y \in V\}.$$

同样可以证明 $\mathrm{O}(V)$ 也构成一个乘法群。我们称 $\mathrm{SO}(V) := \mathrm{O}(V) \cap \mathrm{SL}(V)$ 为**特殊正交群**。特别地，如果我们取 $V = \mathbb{R}^n$，那么正交群即为 $\{g \in \mathrm{GL}_n(\mathbb{R}) \mid gg^T = I_n\}$，我们此时将正交群简记为 $\mathrm{O}(n)$，而特殊正交群为 $\{g \in \mathrm{O}(n) \mid \det(g) = 1\}$，我们将简记为 $\mathrm{SO}(n)$。

最后我们再定义四元数群为

$$Q_8 = \{1, -1, i, j, k, -i, -j, -k\}.$$

Q_8 上的运算定义为

$$1 \cdot a = a, -1 \cdot a = -a \quad \forall a \in Q_8, \quad (-1) \cdot (-1) = 1, \quad i \cdot i = j \cdot j = k \cdot k = -1,$$

$$i \cdot j = -(j \cdot i) = k, \quad j \cdot k = -(k \cdot j) = i, \quad (k \cdot i) = -(i \cdot k) = j.$$

可以直接验证 Q_8 是一个 8 阶非交换群。

2.1.5 群的直积

从已有的群构造新的群的一个办法是群的直积。从集合的角度来说，它就是集合的笛卡尔积，只是对笛卡尔积赋予了群结构。

定义 2.1.6. 设 $(G_i, *_i)_{i \in I}$ 是一族群，我们定义其笛卡尔积上的运算为

$$(g_i)_i * (h_i)_i = (g_i *_i h_i)_i.$$

我们称具有上述运算的集合为 $G_i, i \in I$ 的**直积**，记作 $\prod_{i \in I} G_i$。特别地，当 I 是有限集时，我们直接记为 $G_1 \times G_2 \times \cdots \times G_n$。

可以直接验证在上述运算下 $\prod_{i \in I} G_i$ 构成一个群。在不会引起混淆的情况，我们会把上述运算简写为 $(g_i)_i (h_i)_i = (g_i h_i)_i$

命题 2.1.7. *设 $G_1, G_2, \ldots, G_n$ 是 n 个有限群，那么它们的直积是阶为 $|G_1||G_2| \cdots |G_n|$ 的群。*

习题

练习 2.1.1. 记 $G=\{z\in\mathbb{C}\mid$ 存在整数 n 使得$z^n=1\}$。证明 G 在复数乘法下构成一个群。

练习 2.1.2. 设 G 是一个群，$a_1,a_2,\ldots,a_n\in G$。证明 $(a_1a_2\cdots a_n)^{-1}=a_n^{-1}\cdots a_2^{-1}a_1^{-1}$。

练习 2.1.3. 设 G 是一个群，$g,h\in G$ 满足 $gh=hg$，证明对任意整数 n 有 $(gh)^n=g^nh^n$。举例说明若 $gh\neq hg$，$(gh)^2=g^2h^2$ 不一定成立。

练习 2.1.4. 设 G 是一个群且对任意 $g\in G$ 均有 $g^2=1$。证明 G 是 *Abel* 群。

练习 2.1.5. 设 G 是一个群且对任意 $g,h\in G$ 有 $(gh)^2=g^2h^2$，证明 G 是 *Abel* 群。

练习 2.1.6. 设 G 是一个有限群，且元素个数是偶数。证明存在 $1\neq g\in G$ 使得 $g^2=1$。

练习 2.1.7. 设 G 是具有二元关系的一个集合，且该运算满足结合律（我们称这样的集合 G 为**半群**）。若 G 满足如下两个条件：

1. 存在 $e\in G$ 使得对任意 $g\in G$ 均有 $ge=g$；
2. 对任意 $g\in G$ 存在 $g'\in G$ 使得 $gg'=e$。

证明 G 是一个群。

练习 2.1.8. 设 G 是一个有限半群，且满足

1. 存在 $e\in G$ 使得对任意 $g\in G$ 均有 $ge=g$；
2. 对任意 $g\in G$，若 $gh=gk$，那么必有 $h=k$。

证明 G 是一个群。

练习 2.1.9. 设 G 是一个有限集，在其上定义运算 $*$：

$$\begin{array}{rccc} *: & G\times G & \longrightarrow & G \\ & (a,b) & \longmapsto & a*b \end{array}$$

满足：

1. $(a*b)*c=a*(b*c)$；
2. $a*b=c*b\Rightarrow a=c$；
3. $b*a=b*c\Rightarrow a=c$。

证明：$(G,*)$ 构成一个群。

练习 2.1.10. 设 G 是一个半群，且对任意 $g\in G$，均存在唯一的元素 $g'\in G$ 使得 $(gg')^2=gg'$。证明 G 是一个群。

练习 2.1.11. 设 G 是一个群，$g,h\in G$ 且满足 $ghg=h,h^{2k+1}=1$，其中 k 是一个正整数。证明 $g^2=1$。

练习 2.1.12. 设 D_{2n} 为二面体群。

1. 若 n 是偶数，记 $n=2k\geq 4$，证明 $z=r^k$ 与 D_{2n} 中的所有元素都交换；

2. 若 n 是奇数，证明和 D_{2n} 中所有元素均交换的只有单位元。

练习 2.1.13. 记 σ 为如下置换：

$$1\mapsto 13\quad 2\mapsto 2\quad 3\mapsto 15\quad 4\mapsto 14\quad 5\mapsto 10\quad 6\mapsto 6\quad 7\mapsto 12\quad 8\mapsto 3$$
$$9\mapsto 4\quad 10\mapsto 1\quad 11\mapsto 7\quad 12\mapsto 9\quad 13\mapsto 5\quad 14\mapsto 11\quad 15\mapsto 8$$

记 τ 为如下置换：

$$1\mapsto 14\quad 2\mapsto 9\quad 3\mapsto 10\quad 4\mapsto 2\quad 5\mapsto 12\quad 6\mapsto 6\quad 7\mapsto 5\quad 8\mapsto 11$$
$$9\mapsto 15\quad 10\mapsto 3\quad 11\mapsto 8\quad 12\mapsto 7\quad 13\mapsto 4\quad 14\mapsto 1\quad 15\mapsto 13$$

计算置换 $\sigma,\tau,\sigma^2,\sigma\tau$ 和 $\tau\sigma$ 的轮换分解。

练习 2.1.14. 计算下列置换在 S_9 中的轮换类型：

$$\sigma=(1\ 9\ 2)(4\ 9\ 8\ 5),\qquad \tau=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&6&3&5&8&7&9&4&2\end{pmatrix}.$$

练习 2.1.15. 设 $\sigma=(1\ 2\ \ldots\ m)$ 为 m-轮换，证明 σ^i 仍然是 m-轮换当且仅当 i 和 m 互素。

练习 2.1.16. 设 $n\geq m$，证明 S_n 中的 m-轮换的个数是

$$\frac{n(n-1)(n-2)\cdots(n-m+1)}{m}.$$

练习 2.1.17. 设 G 是一个群，$g\in G$ 的阶为 n。设 $n=rs$，其中 r,s 互素。

1. 证明存在 $g_1,g_2\in G$ 使得 $g_1^r=g_2^s=1$ 且 $g_1g_2=g_2g_1=g$；

2. 证明上述 g_1,g_2 是唯一的。

练习 2.1.18. 设 p 是一个素数，$\sigma\in S_p$ 的阶为 p。

1. 证明 σ 是一个 p-轮换；

2. 证明存在一个 p-轮换 $\tau\in\langle\sigma\rangle$ 使得 $\tau(1)=2$；

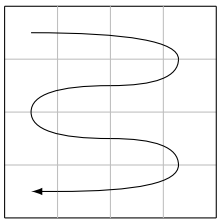
3. 证明 S_p 中恰有 $(p-2)!$ 个阶为 p 的子群。

练习 2.1.19. 数字华容道是一个由 4×4 的方格组成的正方形，其中有 15 个格子分别放置数字 1 至 15，剩下一个是空的，每次移动是将空方格上下左右中的一个移至空方格中。例如我们的初始位置如下图左边所示，经过若干次移动可变成右图。

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9		10	12
13	14	11	15

我们记 $\mathcal{E}$ 为所有由初始位置移动得到的数字华容道组成的集合。对于每个元素 $E \in \mathcal{E}$，我们都可以对应一个序列 $s(E) = (x_1, x_2, \ldots, x_{15})$，该序列按照下图所示顺序依次得到，



如果遇到空方格，则直接跳过，例如初始位置对应的序列为 $(1,2,3,4,8,7,6,5,9,10,11,12,15,14,13)$。对于每一个元素 $E \in \mathcal{E}$ 及其对应的序列 $s(E) = (x_1, x_2, \ldots, x_{15})$，存在唯一的置换 $\sigma(E) \in S_{15}$ 使得 $\sigma(i) = x_i$。

1. 设 $E, F \in \mathcal{E}$ 使得 F 是 E 通过移动一次所得的的。证明 $\sigma(E)^{-1}\sigma(F) \in S_{15}$ 只依赖于空方格的初始位置和最终位置，并给出它的轮换类型。

2. 求集合 $\{\sigma(E)^{-1}\sigma(F) \mid E, F \in \mathcal{E}\} \subseteq S_{15}$。

3. 试问下面哪个数字华容道会出现在 $\mathcal{E}$ 中？

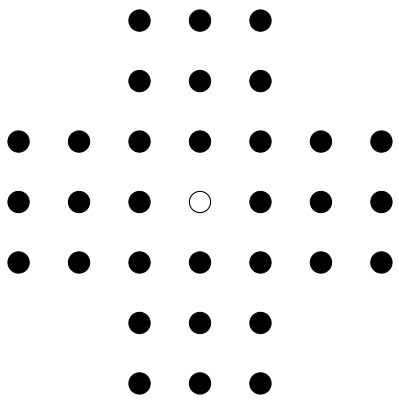
1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

	1	2	3
4	5	6	7
8	9	10	11
12	13	15	14

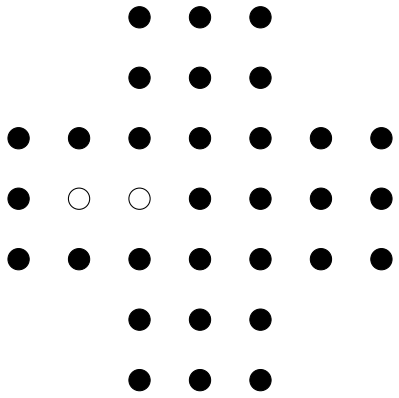
4. 证明 $|\mathcal{E}| = \frac{16!}{2}$。

练习 2.1.20. 我们考虑如下游戏，初始盘面如下图，共有 32 个黑子和一个空白位置：



其游戏规则是每次将一个黑子隔着相邻（水平或者垂直）的另一个黑子跳到空白处，同时将被跳过的黑子移除。例如我们将第五排左起第二颗黑子跳过同一排左起第三颗黑子可以跳到空白位置，此时游戏界

面变为下图



请问是否可以使得棋盘上只剩一颗黑子？如果可以，这个黑子可能落在哪里？(提示：考虑将每个位置赋予 *Klein* 四元群中的三个非单位元素。)

2.2 子群和循环群

2.2.1 子群

定义 2.2.1. 设 H 为群 G 的非空子集，若 H 关于 G 的运算也构成一个群，那么 H 被称为 G 的**子群**，记作 $H \leq G$。若 $H \neq G$，则称 H 为 G 的真子群，记作 $H < G$。

我们要注意 H 和 G 的运算必须相同才能被称为子群，例如 $\mathbb{Q}^*$ 是 $\mathbb{Q}$ 的子集，并且也是一个群，但是 $\mathbb{Q}^*$ 是在乘法运算下构成一个群，而 $\mathbb{Q}$ 是在加法运算下构成一个群，因此 $\mathbb{Q}^*$ 不是 $\mathbb{Q}$ 的子群。

例 2.2.2. *1.* 作为加法群，我们易知有 $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$。

2. 作为乘法群，同样有 $\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$。

3. 对任意整数 m，$m\mathbb{Z}$ 是 $\mathbb{Z}$ 的子群。另一方面，$\mathbb{Z}$ 的子群均形如 $m\mathbb{Z}$。

4. 更一般地，设 G 是一个群，设 $g \in G$，记 $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$，那么 $\langle g \rangle$ 是 G 的一个子群。

5. $\mathrm{SL}(n), \mathrm{O}(n), \mathrm{SO}(n)$ 均为 $\mathrm{GL}(n)$ 的子群，而 $\mathrm{SO}(n)$ 又是 $\mathrm{SL}(n)$ 的子群。

从子群的定义出发如果要证明一个群是子群我们需要验证乘法封闭性，还要验证逆元是否存在，但是我们如下更简洁的办法来验证。

命题 2.2.3. 设 G 是一个群，H 是 G 的一个非空子集，若对任意 $g, h \in H$ 均有 $gh^{-1} \in H$，那么 H 是 G 的一个子群。

证明. 取 $g = h$ 可知 H 包含单位元。于是对任意 $h \in H$，均有 $1 \cdot h^{-1} = h^{-1} \in H$。因此 H 中任意元素都在 H 中有逆元。最后我们验证乘法封闭性，事实上，对任意 $g, h \in H$，h^{-1} 也在 H 中，因此 $gh = g(h^{-1})^{-1} \in H$，故 H 满足乘法封闭性，因此 H 是 G 的子群。

下面我们介绍一些常见的子群。

定义 2.2.4. 设 G 是一个群，A 是 G 的一个非空子集，我们称集合 $C_G(A)=\{g\in G\mid ga=ag,\ \forall a\in A\}$ 为 A 在 G 中的**中心化子**。特别地，当 $A=G$ 时，我们称 $C_G(G)$ 为 G 的**中心**，简记为 $Z(G)$。我们称集合 $N_G(A)=\{g\in G\mid gAg^{-1}=A\}$ 为 A 在 G 中的**正规化子**。

根据定义可知 A 的中心化子即为和 A 中所有可交换的元素组成的集合，并且 $C_G(A)$ 一定是 $N_G(A)$ 的子群。

命题 2.2.5. *设 G 是一个群，A 是 G 的非空子集，那么 $C_G(A),N_G(A)$ 均为 G 的子群。*

证明. 根据命题2.2.3，我们只需验证对任意 $g,h\in C_G(A)$ 均有 $gh^{-1}\in C_G(A)$ 即可。对任意 $a\in A$，由于 $h\in C_G(A)$，因此 $ha=ah$，即有 $ah^{-1}=h^{-1}a$。因此我们有

$$(gh^{-1})a=g(h^{-1}a)=g(ah^{-1})=(ga)h^{-1}=(ag)h^{-1}=a(gh^{-1}).$$

故 $gh^{-1}C_G(A)$，所有 $C_G(A)$ 是 G 的子群。同样地，对任意 $g,h\in N_G(A)$，$hAh^{-1}=A$，因此 $A=h^{-1}Ah$。所以

$$(gh^{-1})A(gh^{-1})^{-1}=(gh^{-1})A(hg^{-1})=g(h^{-1}Ah)g^{-1}=gAg^{-1}=A.$$

故 $gh^{-1}\in N_G(A)$，所以 $N_G(A)$ 是 G 的子群。

例 2.2.6. *1. 当 G 是交换群时，那么对任意非空子集 $A\subseteq G$ 均有 $C_G(A)=N_G(A)=G$。*

2. 设 $G=S_3$，$A=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$，那么 $C_G(A)=N_G(A)=A$。

3. $Z(Q_8)=\{\pm1\}$，$Z(D_8)=\{1,r^2\}$。

4. 当 $n\geq 3$ 时，$Z(S_n)=\{(1)\}$。

5. $\mathrm{GL}(n)$ 的中心是 $\{kI_n\mid k\in\mathbb{R}^*\}$。

2.2.2 循环群

定义 2.2.7. 设 G 是一个群，$(g_i)_{i\in I}\in G$。我们称 G 中包含 $(g_i)_{i\in I}$ 的最小子群为 $(g_i)_{i\in I}$ **生成的子群**，记作 $\langle g_i\mid i\in I\rangle$，$g_i,i\in I$ 被称为 $\langle g_i\mid i\in I\rangle$ 的**生成元**。若 $G=\langle g_1,\dots,g_k\rangle$，我们则称 G 是**有限生成的**。特别地，若 $G=\langle g\rangle$，我们称 G 是由 g 生成的**循环群**。

根据定义容易看出来 $\mathbb{Z}$ 是由 1 生成的循环群（同样也可以视为由 -1 生成）。设 m 是一个正整数，群 $\{\mathrm{e}^{2k\pi\mathrm{i}/m}\mid k=1,2,\dots,m\}$ 则是由 $\mathrm{e}^{2\pi\mathrm{i}/m}$ 生成的 m 阶循环群。同样地，群 $\mathbb{Z}/m\mathbb{Z}$ 也是一个 m 阶循环群，其一个生成元是 $\overline{1}$。更一般地，容易知道 m 阶循环群有如下表现：$G=\langle x\mid x^m=1\rangle$。在下一节我们将会看到这些 m 阶循环群其实本质上都是一样的。而 $\mathbb{Z}[\sqrt{-1}]$ 则不是循环群，它由两个元素生成 $1,\sqrt{-1}$。循环群是最简单的一类交换群，它有一个很好的性质是它的子群仍然是循环群。

定理 2.2.8. *设 G 是由 g 生成的循环群，H 是 G 的子群，那么存在非负整数 n 使得 H 是 g^n 生成的循环群。*

证明. 由于 G 中元素均可表示为 g^n 的形式，其中 $n\in\mathbb{Z}$。不妨设 n 是使得 $ga^n\in H$ 的最小正整数。下面我们证明 $H=\langle g^n\rangle$。显然有 $\langle g^n\rangle\subseteq H$。若存在整数 m 使得 $g^m\in H$ 但 $g^m\notin\langle g^n\rangle$。根据欧几里得算法，存在整数 q,r 使得 $m=qn+r$ 其中 $0\leq r<n$。由于 $g^m\notin\langle g^n\rangle$，因此 $r\neq 0$。于是 $g^r=g^m\cdot(g^n)^q\in H$，这与 n 的最小性矛盾。

定义 2.2.9. 设 G 是一个群，$g \in G$。若存在正整数 n 使得 $g^n = 1$，则称 g 是有限阶的，使得 $g^n = 1$ 成立的最小正整数 n 称为 g 的**阶**，记作 $\mathrm{ord}(g)$ 或者 $|g|$。

从定义可以看出群 G 是 n 阶循环群当且仅当存在阶为 n 的元素。下面我们介绍几个关于元素阶的简单性质。

命题 2.2.10. 设 $g \in G$ 的阶为 k，若 $g^m = 1$，那么必有 $k \mid m$。

证明. 根据带余除法知存在整数 q, r 使得 $m = qk + r$，其中 $0 \leq r < k$。若 $r \neq 0$，那么 $g^r = g^{m-qk} = g^m(g^k)^{-q} = 1$。这与 k 的最小性矛盾。因此 $r = 0$，即有 $k \mid m$。

命题 2.2.11. 设 $g \in G$ 的阶为 k，则 g^m 的阶为 $\frac{k}{(k,m)}$。

证明. 设 ℓ 是 g^m 的阶。由于 $\frac{mk}{(k,m)}$ 是 k 的倍数，因此 $(g^m)^{\frac{k}{(k,m)}} = 1$。因此根据命题2.2.10可知 $\ell \mid \frac{k}{(k,m)}$。另一方面由于 $g^{m\ell} = 1$，同样利用命题2.2.10可知 $k \mid m\ell$，因此 $\frac{k}{(k,m)} \mid \ell$，因此必有 $\ell = \frac{k}{(k,m)}$。

命题 2.2.12. 设 G 是一个群，$g, h \in G$ 的阶分别为 n, m 且满足 $gh = hg$。若 m, n 互素，那么 gh 的阶为 mn。

证明. 设 gh 的阶为 ℓ。一方面显然有 $(gh)^{mn} = g^{mn}h^{mn} = 1$，故 $\ell \mid mn$。另一方面根据命题2.2.11可知 $(gh)^n = g^n h^n = h^n$ 的阶为 $\frac{m}{(n,m)} = m$，因此 $m \mid \ell$。同样地 $n \mid \ell$，由于 m, n 互素，因此 $mn \mid \ell$，故 $\ell = mn$。

命题 2.2.13. 设 G 是一个有限交换群，若 G 中元素阶的最大值为 m，那么对任意 $g \in G$ 均有 $g^m = 1$。

证明. 首先不妨设 g 的阶为 m，若存在 $h \in G$ 使得 $h^m \neq 1$。设 h 的阶为 n，那么 n 不整除 m。因此存在素数 p 使得 $n = n_1 p^t, m = m_1 p^k$，其中 $(n_1, p) = (m_1, p) = 1$ 且 $t > k$。根据命题2.2.11知 g^{p^k} 的阶为 m_1，而 h^{n_1} 的阶为 p^t。于是根据命题2.2.12，$g^{p^k}h^{n_1}$ 的阶为 $m_1 p^t$。但是根据假设 $t > k$，因此 $m_1 p^t > m$，这与 m 的最大性矛盾。

习题

练习 2.2.1. 讨论下列集合是否是对应群的子群。

1. $\{a + a\mathrm{i} \mid a \in \mathbb{R}\}$ 是否是 $(\mathbb{C}, +)$ 的子群。
2. S_n 中所有 2-轮换组成的集合是否是 S_n 的子群。
3. $\{a \in \mathbb{R}^* \mid a^2 \in \mathbb{Q}\}$ 是否是 $(\mathbb{R}^*, \times)$ 的子群。
4. D_{2n} 中所有反射组成的集合是否是 D_{2n} 的子群。
5. $\{1, r^2, s, sr^2\}$ 是否够成 D_8 的子群。

练习 2.2.2. 计算 (1 12 8 10 2)(4 5)(13 11)(7 6 9) 的阶。

练习 2.2.3. 设 p 是一个素数，证明 $\tau \in S_n$ 的阶为 p 当且仅当 τ 是若干可交换的 p-轮换的乘积。举例说明合数的情况该结论不对。

练习 2.2.4. 设 $H_1, H_2, H_3, \ldots$ 是 G 的一列子群，且 $H_1 \subseteq H_2 \subseteq H_3 \subseteq \ldots$，证明 $\bigcup_{i\geq 1} H_i$ 是 G 的子群。反之设 H, K 是群 G 的子群，若 $H \cup K$ 仍是 G 的子群，那么必有 $H \subseteq K$ 或 $K \subseteq H$。

练习 2.2.5. 设 H 是群 G 的子集，且满足对任意 $g, h \in H$ 均有 $gh \in H$，H 是否一定是 G 的子群？

练习 2.2.6. 给出 $\mathbb{Z}$ 的所有加法子群。

练习 2.2.7. 给出 $\mathbb{Q}$ 的所有有限生成的加法子群。

练习 2.2.8. 设 H, K 为群 G 的子群，记 $HK = \{hk \mid h \in H, k \in K\}$。证明 HK 是 G 的子群的充要条件是 $HK = KH$。

练习 2.2.9. 设 G 是一个 *Abel* 群，H 是 G 中所有有限阶元素组成的集合，证明 H 是 G 的子群。举例说明该结论对非 *Abel* 群不成立。

练习 2.2.10. 证明群 G 的子群个数是有限的当且仅当 G 是有限群。

练习 2.2.11. 设 G 是一个群，证明 $C_G(Z(G)) = G$。

练习 2.2.12. 设 H 是群 G 的子群，集合 $\{g \in G \mid gHg^{-1} \subseteq H\}$ 是否构成 G 的子群？

练习 2.2.13. 证明：$Z(G_1 \times G_2 \times \cdots \times G_n) = Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n)$。

练习 2.2.14. 设 $n \geq 3$，证明 $Z(S_n) = 1$。

练习 2.2.15. 证明当 $n \geq 3$ 时，$(\mathbb{Z}/2^n\mathbb{Z})^*$ 不是循环群。

练习 2.2.16. 考虑如下两个复矩阵：

$$A = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

设 H 是 $\mathrm{GL}_2(\mathbb{C})$ 中由 A, B 生成的子群。

1. 证明 $A^4 = I_2, A^2 = B^2, BA = A^3B$。
2. 证明 H 的阶为 8。

练习 2.2.17. 设 $(G_i)_{i\in I}$ 是一族群，我们称集合

$$\{(g_i) \in \prod_{i\in I} G_i \mid \text{除有限个指标 } i \text{ 以外 } g_i \text{ 均为群 } G_i \text{ 的单位元}\}$$

为群 G_i 的**直和**，我们记作 $\bigoplus_{i\in I} G_i$。证明 G_i 的直和是 $\prod_{i\in I} G_i$ 的子群。

练习 2.2.18. 设 $k \geq 3$ 是一个正整数，求阶数最小的非交换群 G 使得对任意的 $g \in G$ 均有 $g^k = 1$。

练习 2.2.19. 设 G 为一个非平凡群，并且任意两个非单位的元素均共轭，即对任意 $x, y \in G \setminus \{1\}$，存在 $g \in G$ 使得 $gxg^{-1} = y$。若存在 $g \in G \setminus \{1\}$ 使得 g 的阶是有限的，证明

(1) G 的所有非单位元素的阶均是素数；
(2) G 的所有非单位元素的阶均是 2；

(3) G 是阿贝尔群，由此得到 $G \simeq \mathbb{Z}/2\mathbb{Z}$。

练习 2.2.20. 设 p 是一个素数，记 $\mu_{p^\infty} := \{z \in \mathbb{C} \mid$ 存在 n 使得$z^{p^n} = 1\}$。对正整数 k 记 $\mu_{p^k} = \{z \in \mathbb{C} \mid z^{p^k} = 1\}$。证明

1. μ_{p^k} 是 μ_{p^m} 的子群当且仅当 $k \leq m$；

2. 对任意 k，μ_{p^k} 均是循环群；

3. μ_{p^k}，$k = 1, 2, \ldots$ 是 μ_{p^∞} 的所有真子群；

4. μ_{p^∞} 不是有限生成的，即不存在 μ_{p^∞} 中的有限个元素 $z_1, \ldots, z_t$ 使得 $\mu_{p^\infty} = \langle z_1, \ldots, z_t \rangle$。

群 μ_{p^∞} 被称为 ***Prüfer* 群**，它是一个所有真子群均为有限群的无限群。

练习 2.2.21. 证明 $\mathrm{SL}_2(\mathbb{Z})$ 是由 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 和 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 生成的。

练习 2.2.22. 设 I_n 是 n 阶单位群，E_{ij} 是 (i, j) 位置等于 1，其余位置等于 0 的矩阵。

(1) 证明 $\mathrm{GL}_n(\mathbb{Z})$ 由如下矩阵生成：

- $I_n + E_{ij},\ i, j = 1, 2, \ldots, n,\ i \neq j$；
- $I_n + E_{ij} + E_{ji} - E_{ii} - E_{jj},\ i, j = 1, 2, \ldots, n,\ i \neq j$。

(2) 证明 $\mathrm{SL}_n(\mathbb{Z})$ 由矩阵 $I_n + E_{ij},\ i, j = 1, 2, \ldots, n,\ i \neq j$ 生成。

(3) 证明 $\mathrm{GL}_n(\mathbb{Z})$ 由矩阵 $I_n + E_{ij},\ i, j = 1, 2, \ldots, n,\ i \neq j$ 及 $I_n - 2E_{nn}$ 生成。

(4) 证明 $\mathrm{GL}_n(\mathbb{Z})$ 可由三个矩阵生成。(提示：其中一个取 $I_n + E_{12}$，另两个取合适的置换矩阵。)

练习 2.2.23. 设 G 是有限生成的，试问 G 的子群是否一定是有限生成的？

2.3 陪集和商群

2.3.1 群同态

定义 2.3.1. 设 $(G, \cdot)$ 和 $(H, \circ)$ 是两个群。若映射 $f : G \to H$ 满足对任意 $g_1, g_2 \in G$ 均有 $f(g_1 \cdot g_2) = f(g_1) \circ f(g_2)$，那么我们称 f 是一个**群同态**。我们称 $\ker f := \{g \in G \mid f(g) = 1\}$ 为 f 的**核**。若 f 还是一个双射，那么我们称 f 是一个**群同构**，记作 $G \simeq H$。

在不会引起混淆的情况下，我们会省略两个群的运算符号，即写成 $f(g_1 g_2) = f(g_1) f(g_2)$。注意到群同态总是将单位元映射到单位元，事实上，我们取 $g_1 = g_2 = 1$，即有 $f(1) = f(1)f(1)$，两边同时乘以 $f(1)^{-1}$ 即得 $f(1) = 1$。

例 2.3.2. *1.* 注意在群同态的定义中 a 和 b 之间的运算是 G 中的运算，而 $f(a)$ 和 $f(b)$ 之间的运算则是 H 中的运算，两者不需要相同。例如考虑加法群 $\mathbb{R}$ 和乘法群 $\mathbb{R}_{>0}$，那么指数映射给出了一个群同态：

$$\begin{array}{rccc} \exp: & \mathbb{R} & \longrightarrow & \mathbb{R}_{>0} \\ & x & \longmapsto & \exp(x). \end{array}$$

事实上这还是一个群同构。

2. 高等代数中的行列式也可以给出 $\mathrm{GL}_n(K)$ 到 K^* 的一个群同态：

$$\begin{array}{rccc} \det: & \mathrm{GL}_n(K) & \longrightarrow & K^* \\ & A & \longmapsto & \det(A). \end{array}$$

3. 设 G 是一个群，g 是群 G 中的一个元素，那么我们有如下群同态

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & g^n. \end{array}$$

4. 考虑映射 $f: D_6 \to S_3$，其中 $f(s^i r^j) = (1\ 2)^i (1\ 2\ 3)^j$。可以验证 f 是一个群同构。更一般地，因为 D_{2n} 中的元素即为正 n 边形的刚体变换，因此它可以被视作 n 个顶点上的置换，由此可以构造 D_{2n} 到 S_n 的一个自然映射：$r \mapsto (1\ 2\ \dots\ n), s \mapsto (1\ n)(2\ n-1)\cdots([\frac{n+1}{2}]\ [\frac{n+2}{2}])$。

命题 2.3.3. 设 $f: G \to G', f': G' \to G''$ 为两个群同态，那么 $f' \circ f: G \to G''$ 也是群同态。更进一步，若 f, f' 都是同构，那么 $f' \circ f$ 也是同构。

证明. 直接验证即可。

命题 2.3.4. 设 $f: G \to G'$ 是一个群同态。

1. 若 H 是 G 的一个子群，那么 $f(H)$ 是 G' 的一个子群；
2. 若 H' 是 G' 的一个子群，那么 $f^{-1}(H')$ 是 G 的一个子群；
3. G 中所有包含 $\ker f$ 的子群和 G' 中所有包含在 $\mathrm{Im}\, f$ 中的子群一一对应。

证明. 1 和 2 可由子群的定义直接验证。对于第三条，我们考虑如下对应：

$$\left\{\begin{array}{c} G \text{ 中包含} \\ \ker f \text{ 的子群 } H \end{array}\right\} \underset{H' \mapsto f^{-1}(H')}{\overset{H \mapsto f(H)}{\rightleftarrows}} \left\{\begin{array}{c} G' \text{ 中包含在} \\ \mathrm{Im}\, f \text{ 中的子群 } H' \end{array}\right\}.$$

我们只需验证 $\Psi \circ \Phi$ 和 $\Phi \circ \Psi$ 均为恒等映射即可。对任意 G' 中包含在 $\mathrm{Im}\, f$ 中的子群 H'，$\Psi \circ \Phi(H') = \Psi(f^{-1}(H')) = f(f^{-1}(H'))$。根据定义显然有 $f(f^{-1}(H')) \subseteq H'$。另一方面，对任意 $h' \in H'$，由于 $H' \subseteq \mathrm{Im}\, f$，因此存在 $h \in G$ 使得 $f(h) = h'$，即有 $h \in f^{-1}(H')$。因此 $H' \subseteq f(f^{-1}(H'))$。故 $\Psi \circ \Phi(H') = H'$。

反之，对任意 G 中包含 $\ker f$ 的子群 H，我们有 $\Phi \circ \Psi(H) = \Phi(f(H)) = f^{-1}(f(H))$。根据定义显然有 $H \subseteq f^{-1}(f(H))$。另一方面，对任意 $h \in H$，若 $g \in f^{-1}(f(h))$，即有 $f(g) = f(h)$，于是 $h^{-1}g \in \ker f$，而 H 包含 $\ker f$，因此 $g \in H$，即有 $f^{-1}(f(h)) \subseteq H$，故 $\Phi \circ \Psi(H) = H$。

定义 2.3.5. 设 G 是一个群，我们称 G 到自身的同构为 G 的**自同构**，我们记 G 上所有的自同构组成的集合为 $\mathrm{Aut}(G)$。

命题 2.3.6. 设 G 是一个群，那么 $\mathrm{Aut}(G)$ 在映射的复合运算下构成一个群，我们称该群为**自同构群**。

证明. 设 $f_1, f_2 \in \mathrm{Aut}(G)$，根据命题2.3.3可知 $f_1 f_2$ 也是 G 上的自同构，因此 $\mathrm{Aut}(G)$ 在映射的复合运算下是封闭的。容易看出 id_G 是 $\mathrm{Aut}(G)$ 中的单位元，f^{-1} 是 f 的逆元。

例 2.3.7. 一般来说，计算一个群的自同构群并不是一件简单的事，我们下面计算一些比较简单的群的自同构群。

1. 当 $G \simeq \mathbb{Z}/2\mathbb{Z}$ 时，设 $f \in \mathrm{Aut}(G)$，由于 f 将单位元映射到单位元，并且 f 是双射，所以只能将唯一的非单位元映射到自身，这意味着 f 只能是恒等映射。故 $\mathrm{Aut}(G) \simeq \{1\}$。

2. 更一般地，假设 $G = \mathbb{Z}/n\mathbb{Z}$ 其中 $n \geq 2$ 是一个正整数，那么我们可以证明 $\mathrm{Aut}(G) \simeq (\mathbb{Z}/n\mathbb{Z})^*$。事实上，我们构造如下映射

$$\begin{array}{rccc} \Psi: & (\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & \mathrm{Aut}(G) \\ & \overline{a} & \longmapsto & \Psi(\overline{a}) : \overline{k} \mapsto \overline{ak}. \end{array}$$

   容易看出上述映射是定义良好的。下面我们验证它是群同态，对任意 $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^*$，及 $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$，我们有

$$(\Psi(\overline{a}) \circ \Psi(\overline{b}))(\overline{k}) = \Psi(\overline{a})(\overline{bk}) = \overline{a}\overline{bk} = \Psi(\overline{ab})(\overline{k}).$$

   这表明 $\Psi(\overline{a}) \circ \Psi(\overline{b}) = \Psi(\overline{ab})$，即 Ψ 是群同态。若 $\overline{a} \in \ker \Psi$，那么对任意 $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ 均有 $\overline{k} = \overline{ak}$，特别地，取 $k = 1$ 即可知 $\overline{a} = \overline{1}$。因此 Ψ 是单射。最后我们证明 Ψ 是满射。对任意 $f \in \mathrm{Aut}(G)$，由于 G 是循环群，因此 f 由 $f(\overline{1})$ 唯一决定，因此不妨设 $f(\overline{1}) = \overline{a}$，于是我们有 $\Psi(\overline{a}) = f$。因此 Ψ 是满射。

3. 对于非交换群而言，计算其自同构群往往更加困难，但是我们有如下方法可以找到一类自同构。设 G 是一个群，对任意 $g \in G$，记

$$\begin{array}{rccc} \varphi_g: & G & \longrightarrow & G \\ & h & \longmapsto & ghg^{-1}. \end{array}$$

   那么 $\varphi_g \in \mathrm{Aut}\, G$ 且 $\mathrm{Inn}\, G = \{\varphi_g \mid g \in G\}$ 是 $\mathrm{Aut}\, G$ 的一个子群。我们称其为 G 的**内自同构群**。

2.3.2 陪集

定义 2.3.8. 设 H 是群 G 的子群，对任意 $g \in G$，我们称集合 $gH = \{gh \mid h \in H\}, Hg = \{hg \mid h \in H\}$ 分别为 H 在 G 中的**左陪集**和**右陪集**。陪集中的任意元素都称为该陪集的一个表示。

从定义可以看出若 G 是交换群，那么它的所有左陪集和右陪集均是相等的。然而一般的群，左右陪集却不一定相等。

例 2.3.9. 设 $G = S_3$，$H = \{(1), (1\ 2)\}$。那么 H 有三个左陪集，分别为

$$\{(1), (1\ 2)\}, \quad \{(1\ 3), (1\ 2\ 3)\}, \quad \{(2\ 3), (1\ 3\ 2)\}.$$

H 同样有三个右陪集，分别为

$$\{(1), (1\ 2)\}, \quad \{(1\ 3), (1\ 3\ 2)\}, \quad \{(2\ 3), (1\ 2\ 3)\}.$$

容易看出 H 在 G 中的左右陪集并不完全相同。

那么一个自然的问题便是什么时候 H 的左陪集和右陪集会相等，在回答这个问题之前，我们先给出陪集的一些基本性质。

引理 2.3.10. *设 H 是 G 的一个子群，$a,b\in G$，那么我们有*

1. $aH=bH\iff a^{-1}b\in H\iff b\in aH$。对右陪集同样也有 $Ha=Hb\iff ab^{-1}\in H\iff a\in Hb$。
2. $|aH|=|Ha|=|H|$。
3. *若 $aH\cap bH\neq\emptyset$，那么 $aH=bH$。*

证明. 1. 若 $aH=bH$，那么存在 $h\in H$ 使得 $a\cdot h=b\cdot 1$，因此 $a^{-1}b=h\in H$。若 $a^{-1}b\in H$，那么存在 $h\in H$ 使得 $a^{-1}b=h$，因此 $b=ah\in aH$。若 $b\in aH$，那么存在 $h\in H$ 使得 $b=ah$，因此对任意 $h'\in H$ 均有 $bh'=ahh'\in aH$，故 $bH\subseteq aH$。同理 $ah'=bh^{-1}h'\in bH$，因此 $aH\subseteq bH$。故 $bH=aH$。右陪集同理可证。

2. 由定义知 aH,Ha,H 之间有一一对应，故必有 $|aH|=|Ha|=|H|$。

3. 若 $aH\cap bH\neq\emptyset$，不妨设 $h_1,h_2\in H$ 使得 $ah1=bh_2$。即有 $b=ah_1h_2^{-1}\in aH$，由 1 可知 $aH=bH$。

上述引理的第三条表明 G 可以写成 H 的左陪集的无交并：

$$G=\coprod_{i\in I}a_iH. \tag{2.1}$$

我们称 $\{a_i\}_{i\in I}$ 为 H 在 G 中的（左）**陪集代表元**，I 的基数称作 H 在 G 中的**指数**，记作 $|G:H|$。这些结论对右陪集也同样成立，并且左右陪集的个数是相等的。事实上，我们可以定义如下双射：

$$\begin{array}{rccc}\rho: & \{aH\mid a\in G\} & \longrightarrow & \{Ha\mid a\in G\}\\ & aH & \longmapsto & Ha^{-1}.\end{array}$$

利用上面的结论我们可以得到著名的 Lagrange 定理。

定理 2.3.11 (Lagrange 定理)**.** *设 H 是 G 的一个子群，那么我们有*

$$|G|=|H||G:H|.$$

特别地，$|H|$ 整除 $|G|$。

证明. 若 G 是无限群，当 H 也是无限群时，结论显然成立。当 H 是有限群时，由于 G 可以写成 $|G:H|$ 个元素个数均为 $|H|$ 的集合的无交并，因此必有 $|G:H|=\infty$。故结论同样成立。

若 G 是有限群，由 (2.1) 即引理2.3.10的第二条可知

$$|G|=\sum_{i\in I}|a_iH|=\sum_{i\in I}|H|=|I||H|=|H||G:H|.$$

从 Lagrange 定理可以容易得到如下推论。

推论 2.3.12. *设 G 是 n 阶有限群，$g\in G$，那么我们有 $g^n=1$。*

证明. 设 $H=\langle g\rangle$ 为由 g 生成的子群，于是 $g^{|H|}=1$。另一方面由 Lagrange 定理2.3.11可知 $|H|$ 整除 n，因此 $g^n=1$。

Lagrange 定理表明 G 的子群的阶一定整除 $|G|$。那么 Lagrange 定理逆命题是否成立呢？即对任意整除 $|G|$ 的整数 n，是否一定存在阶为 n 的子群？一般来说这个结论并不成立，但是对一些特殊的 n，这个结论是成立的。这便是我们接下来要证明的 Cauchy 定理和 Sylow 定理。

2.3.3 商群

从第一章我们知道，给定集合上的一个等价关系，我们便可定义该集合在这个等价关系下的商集。而从上一节我们知道 H 的所有左陪集构成了 G 的一个划分，从而给出了一个等价关系。因此我们可以定义商集 $G/H = \{aH \mid a \in G\}$。然而仅从集合论的角度讨论商没有太大意义，我们需要讨论何时 G/H 有一个自然的群结构并且使得投影映射 $\pi : G \to G/H$ 是一个群同态?

如果存在这样的群结构，设其乘法为 $\circ$，那么我们一定有

$$(gH) \circ (g'H) = \pi(g) \circ \pi(g') = \pi(gg') = gg'H.$$

因此如果群结构存在，那么一定是唯一。所以现在的问题变成了上述运算是否给出了 G/H 上的一个群结构? 然而答案是否定的。我们注意到

$$\ker \pi = \{g \in G \mid gH = H\} = H.$$

而 $\ker \pi$ 满足对任意 $g \in G$ 均有 $g \ker \pi g^{-1} \subseteq \ker \pi$。由此我们可以给出如下定义。

定义 2.3.13. 设 H 是 G 的一个子群，若对任意 $g \in G$ 均有 $gHg^{-1} \subseteq H$，则称 H 是一个**正规子群**，记作 $H \trianglelefteq G$。

例 2.3.14. *1.* 对任意群 G，$\{1\}$ 和 G 都是 G 的正规子群。

2. 交换群的所有子群都是正规子群。

3. $H_1 = \langle (1\ 2) \rangle$ 不是 S_3 的正规子群，但 $H_2 = \langle (1\ 2\ 3) \rangle$ 是 S_3 的正规子群。

4. $\langle s \rangle$ 不是 D_8 的正规子群，但 $\langle r \rangle, \langle r^2, s \rangle$ 均是 D_8 的正规子群。

5. 设 $f : G \to G'$ 是一个群同态，那么 $\ker f$ 是 G 的正规子群。

6. $Z(G)$ 是 G 的正规子群。

7. 设 H 是 G 的任意一个子群，那么 H 是 $N_G(H)$ 的正规子群。

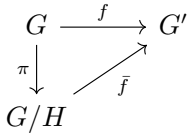
定理 2.3.15. 设 H 是 G 的一个子群，那么 G/H 存在一个群结构且使得投影映射 $\pi : G \to G/H$ 是群同态当且仅当 H 是 G 的正规子群。

证明. 若 G/H 是一个群，且 $\pi : G \to G/H$ 是群同态，由于 $H = \ker \pi$，而 $\ker \pi$ 是 G 的正规子群，因此 H 是 G 的正规子群。反之。若 H 是 G 的正规子群，我们定义 G/H 上的运算为 $aH \cdot bH = aHbH$，由于 H 是正规子群，因此 $b^{-1}Hb = H$，故 $aHbH = abb^{-1}HbH = abH$。由于

$$(aH \cdot bH) \cdot cH = abH \cdot cH = abcH = aH \cdot bcH = aH \cdot (bH \cdot cH).$$

因此该运算满足结合律。容易看出 H 是 G/H 的单位元，$(aH)^{-1} = a^{-1}H$。这表明 G/H 是一个群。

命题 2.3.16 (商群的泛性)**.** 设 H 是 G 的一个正规子群，$f : G \to G'$ 是一个群同态且满足 $H \subset \ker f$。那么存在唯一的群同态 $\bar{f} : G/H \to G'$ 使得 $f = \bar{f} \circ \pi$，即有如下交换图表



证明. 若这样的群同态存在，那么我们一定有 $\bar{f}(aH) = f(a)$ 因此，这样的群同态一定是唯一的。下面我们验证 $\bar{f}(aH) = f(a)$ 是满足条件的群同态。首先我们需要验证它是定义良好的，若 $aH = bH$，由引理2.3.10知 $a^{-1}b \in H$，由于 $H \subseteq \ker f$，因此 $f(a^{-1}b) = 1$，即有 $f(a) = f(b)$。故 $\bar{f}(aH) = f(a) = f(b) = \bar{f}(bH)$。因此 $\bar{f}$ 是定义良好的。因为

$$\bar{f}(aH)\bar{f}(bH) = f(a)f(b) = f(ab) = \bar{f}(abH),$$

故 $\bar{f}$ 是群同态。最后根据定义显然有 $f = \bar{f} \circ \pi$。

例 2.3.17. *1.* $m\mathbb{Z}$ 均为 $\mathbb{Z}$ 的正规子群，因此其对应的商群为 $\mathbb{Z}/m\mathbb{Z}$，该商群上的运算和我们在例2.1.2中的第五个例子是一致的，只是在例五中我们在陪集 $k+m\mathbb{Z}$ 中选了一个特定的代表元，即为大于等于 0 小于 m 的数。

2. $H = \langle(1\ 2\ 3)\rangle$ 是 S_3 的正规子群，而且 S_3/H 的阶等于 2，所以我们有 $S_3/H \simeq \mathbb{Z}/2\mathbb{Z}$。

3. $\langle \mathrm{i} \rangle$ 是 Q_8 的正规子群，由于 $Q_8/\langle \mathrm{i} \rangle$ 的阶为 2，因此我们同样有 $Q_8/\langle \mathrm{i} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$。$\langle -1 \rangle$ 同样是 Q_8 的正规子群，此时 $Q_8/\langle -1 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$。

4. $\langle r^2 \rangle$ 是 D_8 的正规子群，此时我们有 $D_8/\langle r^2 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$。

2.3.4 同构定理

这一节我们介绍几个同构定理。

定理 2.3.18 (第一同构定理)**.** 设 $\varphi : G \to H$ 是一个群同态，那么 $\ker\varphi$ 是 G 的正规子群，并且有群同构 $G/\ker\varphi \simeq \varphi(G)$。

证明. 根据商群的泛性2.3.16可知我们有同态 $\bar{\varphi} : G/\ker\varphi \to \varphi(G)$。该同态显然是满射，我们只需验证它是单射即可。若 $\bar{\varphi}(a\ker\varphi) = 1$，根据定义可知 $\varphi(a) = 1$，即有 $a \in \ker\varphi$，故 $\bar{\varphi}$ 是单射。

定理 2.3.19 (第二同构定理)**.** 设 G 是一个群，A, B 是 G 的子群并满足 $A \leq N_G(B)$。那么 AB 是 G 的子群，且 $B \trianglelefteq AB, A \cap B \trianglelefteq A$ 以及同构 $AB/B \simeq A/A \cap B$。

证明. 设 $a_1, a_2 \in A, b_1, b_2 \in B$，由于 A 包含在 $N_G(B)$ 中，因此 $a_2 B a_2^{-1} = B$。故 $a_1b_1(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1} = a_1a_2^{-1}(a_2b_1b_2^{-1}a_2^{-1}) \in AB$，故根据命题2.2.3知 AB 是 G 的子群。

定理 2.3.20 (第三同构定理)**.** 设 G 是一个群，H, K 均为 G 的正规子群，且 $H \leq K$。那么 $K/H \trianglelefteq G/H$ 且 $(G/H)/(K/H) \simeq G/K$。

证明. 对任意 $gH \in G/H$ 及 $kH \in K/H$，有 $(gH)(kH)(gH)^{-1} = gkg^{-1}H \in K/H$。故 K/H 是 G/H 的正规子群。考虑自然同态 $G/H \to G/K$，$gH \mapsto gK$。该同态的核即为 $\{gH \mid g \in K\} = K/H$。因此由第一同构定理即得 $(G/H)/(K/H) \simeq G/K$。

习题

练习 2.3.1. 设 $f: G \to H$ 是一个群同态。

1. 证明对任意 $g \in G, n \in \mathbb{Z}$ 均有 $f(g^n) = f(g)^n$。
2. 若 f 是群同构，证明对任意 $g \in G$ 均有 $\operatorname{ord}(f(g)) = \operatorname{ord}(g)$

练习 2.3.2. 判断下列群是否是同构

1. 作为乘法群的 $\mathbb{R}^*$ 和 $\mathbb{C}^*$;
2. 作为加法群的 $\mathbb{Z}$ 和 $\mathbb{Q}$;
3. S_n 和 S_m;
4. D_{24} 和 S_4。
5. 习题2.2.16中的群 H 和四元数群 Q_8。

练习 2.3.3. 设 $G_1, G_2, \ldots, G_n$ 是 n 个群，$\sigma \in S_n$。证明下列映射是群同构：

$$\begin{array}{rccc} \varphi_\sigma: & G_1 \times G_2 \times \cdots \times G_n & \longrightarrow & G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)} \\ & (g_1, g_2, \ldots, g_n) & \longmapsto & (g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(n)}). \end{array}$$

练习 2.3.4. 1. 证明映射 $f: G \to G$，$f(g) = g^{-1}$ 是同构当且仅当 G 是 *Abel* 群。

2. 证明映射 $f: G \to G$，$f(g) = g^2$ 是同态当且仅当 G 是 *Abel* 群。

练习 2.3.5. 1. 求所有从 $(\mathbb{Q}, +)$ 到 $(\mathbb{Z}, +)$ 的群同态。

2. 求所有从 $(\mathbb{Q}, +)$ 到 $(\mathbb{Q}^*_{>0}, \times)$ 的群同态。

练习 2.3.6. 记 $\mu_\infty := \{z \in \mathbb{C} \mid \text{存在正整数 } n \text{ 使得} z^n = 1\}$。

1. 证明 $\bigoplus_p \mu_{p^\infty} \simeq \mu_\infty$，这里 $\bigoplus$ 是练习2.2.17中的直和，其中 p 遍历所有的素数，μ_{p^∞} 是练习2.2.20中的 *Prüfer* 群。
2. 证明加法群 $\mathbb{Q}/\mathbb{Z}$ 中的每个元素均是有限阶的。
3. 证明 $\mathbb{Q}/\mathbb{Z} \simeq \mu_\infty$。

练习 2.3.7. 设 G 是一个群且 $|\operatorname{Aut} G| = 1$，证明 $|G| \leq 2$。

练习 2.3.8. 证明 $\operatorname{Aut}(D_8) \simeq D_8$。

练习 2.3.9. 设 H 是群 G 的子群，K 是 H 的子群，若 $|G:H|$ 和 $|H:K|$ 均是有限数，证明 $|G:K|$ 也是有限的，并且有 $|G:K| = |G:H||H:K|$。

练习 2.3.10. 设 H, K 是群 G 的子群，其中 $|G:H| = m, |G:K| = n$。若 m, n 互素，证明 $|G: H \cap K| = mn$。

练习 2.3.11. 设 H, K 是群 G 的子群且 $[G:H] = [G:K] = n < \infty$。

1. 证明存在 $g_1, g_2, \ldots, g_n \in G$ 使得
$$G = \bigcup_{i=1}^{n} g_i H = \bigcup_{i=1}^{n} H g_i.$$

2. 证明存在 $g_1, g_2, \ldots, g_n \in G$ 使得
$$G = \bigcup_{i=1}^{n} g_i H = \bigcup_{i=1}^{n} K g_i.$$

练习 2.3.12. 证明一族正规子群的交仍是正规子群。

练习 2.3.13. 设 H 是群 G 的子群，且其指数是有限的。证明对任意 $g \in G$ 均存在整数 n 使得 $g^n \in H$。

练习 2.3.14. 设 H 是群 G 的子群且 $[G : H] = 2$，证明 H 是正规子群。

练习 2.3.15. 设 H 是 G 的正规子群，K 是 G 的子群，证明 KH 是 G 的子群。

练习 2.3.16. 设 k 整除 n。证明 $\langle r^k \rangle$ 是 D_{2n} 的正规子群且 $D_{2n}/\langle r^k \rangle \simeq D_{2k}$。

练习 2.3.17. 设 G_1, G_2 是两个群，证明 $(G_1 \times G_2)/G_1 \simeq G_2$。

练习 2.3.18. 设 $H_1, H_2, \ldots, H_n$ 分别为 $G_1, G_2, \ldots, G_n$ 的正规子群。证明 $H_1 \times H_2 \times \cdots \times H_n$ 是 $G_1 \times G_2 \times \cdots \times G_n$ 的正规子群，并且有同构
$$(G_1 \times G_2 \times \cdots \times G_n)/(H_1 \times H_2 \times \cdots \times H_n) \simeq (G_1/H_1) \times (G_2/H_2) \times \cdots \times (G_n/H_n).$$

练习 2.3.19. 设 H, K 是群 G 的两个正规子群，且 $H \bigcap K = \{1\}$。证明对任意 $h \in H, k \in K$，均有 $hk = kh$。

练习 2.3.20. 设 G 是一个有限群，N 是 G 的正规子群。若存在 G 的子群 H 使得 $H \bigcap N = \{1\}$ 且 $G = NH$，则称 H 是 N 在 G 中的一个**补**。

1. 证明若 N 在 G 中的补存在，则所有的补都是同构的。

2. 假设 $Z(N) = \{1\}$ 且 $\mathrm{Aut}(N) = \mathrm{Inn}(N)$。证明 N 在 G 中的补存在，并且存在唯一一个补 H 使得 H 是 G 的正规子群。

练习 2.3.21. 设 G 是一个有限群，H 是 G 的子群，N 是 G 的正规子群。若 $|H|$ 和 $|G : N|$ 互素，证明 H 是 N 的子群。

练习 2.3.22. 1. 证明 $\mathbb{Q}$ 没有指数有限的真子群。

2. 证明 $\mathbb{Q}$ 没有极大子群，即对任意真子群 $H \subsetneq \mathbb{Q}$，均存在真子群 H' 使得 $H \subsetneq H' \subsetneq \mathbb{Q}$。

练习 2.3.23. 设 G 是一个群，对任意 $g, h \in G$，记 $[g, h] = g^{-1}h^{-1}gh$ 为 g, h 的**换位子**，并记 G 中的所有的换位子生成的子群为 $D(G)$，我们称之为 G 的**换位子群**或**导出子群**。

1. 证明 $D(G)$ 是 G 的正规子群。

2. 证明 G 是 *Abel* 群当且仅当 $D(G) = \{1\}$。

3. 证明 $G/D(G)$ 是 *Abel* 群。

练习 2.3.24. 1. 证明当 $n \geq 2$ 时，证明 $D(\mathrm{GL}_n(\mathbb{R})) = D(\mathrm{SL}_n(\mathbb{R})) = \mathrm{SL}_n(\mathbb{R})$。

2. 当 $n \geq 3$ 时，证明导出子群 $D(\mathrm{SL}_n(\mathbb{Z}))$ 等于 $\mathrm{SL}_n(\mathbb{Z})$。

3. $D(\mathrm{SL}_2(\mathbb{Z}))$ 是否等于 $\mathrm{SL}_2(\mathbb{Z})$？如果不相等，$[\mathrm{SL}_2(\mathbb{Z}) : D(\mathrm{SL}_2(\mathbb{Z}))]$ 等于多少？

练习 2.3.25. 证明 $\mathrm{Inn}\, G$ 是 $\mathrm{Aut}\, G$ 的正规子群，且有 $\mathrm{Inn}\, G \simeq G/Z(G)$。

练习 2.3.26. 1. 设 G 是一个群，若 $G/Z(G)$ 是循环群，证明 G 是 *Abel* 群。

2. 设 p 是一个素数，证明 p^2 阶群必同构于 $\mathbb{Z}/p^2\mathbb{Z}$ 或 $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$。

练习 2.3.27. 设 G 是一个阶为 p^n 的群，其中 p 是素数，证明对任意 $0 \leq k \leq n$，G 有一个阶为 p^k 的正规子群。

练习 2.3.28. 设群 G 是有限生成的，H 是 G 的子群且 G/H 是有限群，是否有 H 也是有限生成的？

练习 2.3.29. 设 $G = D_{16}$ 为 16 阶的二面体群。

1. 证明由 r^4 生成的子群是 G 的正规子群。记 $\overline{G} = G/\langle r^4 \rangle$。

2. 将元素 $\overline{rs}, \overline{sr^{-2}s}, \overline{s^{-1}r^{-1}sr}$ 写成 $\overline{s}^a\overline{r}^b$ 的形式，其中 a, b 是整数。

3. 证明 $\overline{H} = \langle \overline{s}, \overline{r}^2 \rangle$ 是 $\overline{G}$ 的正规子群，且 $\overline{H}$ 同构于 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$。

练习 2.3.30. 设 $G = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$。

1. 证明 $\langle \sigma^4 \rangle$ 是 G 的正规子群。记 $\overline{G} = G/\langle \sigma^4 \rangle$。

2. 计算 $\overline{\tau\sigma}, \overline{\tau\sigma}^2, \overline{\tau\sigma}^3$ 的阶。

3. 将 $\overline{\sigma\tau}, \overline{\tau\sigma^{-2}\tau}, \overline{\tau^{-1}\sigma^{-1}\tau\sigma}$ 写成 $\overline{\tau}^a\overline{\sigma}^b$ 的形式。

4. 证明 $\overline{G} \simeq D_8$。

练习 2.3.31. 设 H, K 是两个子群，$f : K \to \mathrm{Aut}(H)$ 是一个群同态。我们在集合 $H \times K$ 上定义如下运算 $\star_f$：

$$(h, k) \star_f (h', k') := (h(f(k))(h'), kk').$$

1. 证明集合 $H \times K$ 在上述运算下构成一个群，我们称之为 H, K 关于 f 的 **（外）半直积**，并记作 $H \rtimes_f K$。

2. 设 $f : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ 定义为 $(f(\overline{k}))(\overline{m}) := \overline{(-1)^k m}$，证明 $\mathbb{Z}/n\mathbb{Z} \rtimes_f \mathbb{Z}/2\mathbb{Z} \simeq D_{2n}$。

3. 设 H 是群 G 的一个正规子群，K 是 H 在 G 中的补（见习题2.3.20）。定义 $f : K \to \mathrm{Aut}(H)$ 为 $k \mapsto (h \mapsto khk^{-1})$。那么映射 $H \rtimes_f K \to G, (h, k) \mapsto hk$ 是一个群同构。我们称 G 是 H, K 的**内半直积**。

4. 记 $S \subseteq S_4$ 为 $\{1\}$ 的稳定化子，即为 $\{\sigma \in S_4 \mid \sigma(1) = 1\}$。证明 $S \simeq S_3$ 且 S 是 $K = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ 在 S_4 中的补。

5. 证明 $S_4 \simeq K \rtimes S$。

练习 2.3.32. 设 A 是有限阿贝尔群，$\phi: A \to A$ 是一个群同态。定义

$$A_{\mathrm{nil}} := \{x \in A \mid \text{存在 } k \geq 1 \text{ 使得 } \phi^k(x) = 0\}.$$

证明存在唯一的子群 A_0 使得 $\phi|_{A_0}$ 是 A_0 上的一个同构且 $A = A_0 \oplus A_{\mathrm{nil}}$。

2.4 群作用

2.4.1 群作用和置换表示

这一节我们考虑群在集合上的作用，群作用的思想在数学中是非常重要的思想，因为我们对群和集合赋予了更多的结构，因此我们能得到更多的信息。例如群表示则是研究的群在线性空间上的作用。我们首先给出群作用的定义。

定义 2.4.1. 群 G 在集合 X 上的一个**群作用**是指从 $G \times X$ 到 X 的一个映射并满足如下几条性质：

1. 对任意 $g_1, g_2 \in G$ 及 $x \in X$ 均有 $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$；
2. 对任意 $x \in X$ 均有 $1 \cdot x = x$。

为简单起见，在不引起混淆的情况下我们将把 $g \cdot x$ 简记为 gx，但是大家要注意区分它和群中元素的乘法。

下面我们给出几个简单的例子。更多的例子将在后面给出。

例 2.4.2. *1.* 若对任意 $g \in G$ 及 $x \in X$ 均有 $gx = x$，那么这显然是一个群作用，我们称之为平凡作用。

2. 设 V 是实数域 $\mathbb{R}$ 上的线性空间，那么数乘运算给出了乘法群 $\mathbb{R}^*$ 到 V 上的一个作用。

3. 设 V 是实数域 $\mathbb{R}$ 上的线性空间，那么 $\mathrm{GL}(V)$ 在 $\mathbb{P}(V)$ 上有一个自然的作用，即对任意 $\mathcal{A} \in \mathrm{GL}(V), \overline{\alpha} \in \mathbb{P}(V)$，我们有 $\mathcal{A} \cdot \overline{\alpha} = \overline{\mathcal{A}(\alpha)}$，其中 $\mathbb{P}(V)$ 的定义见例*1.2.3*。

4. 设 X 是一个非空集合，S_X 是 X 上的对称群，那么 $\sigma \cdot x = \sigma(x)$ 是 S_X 在 X 上的一个作用。

5. 记 $S^{n-1} = \{\alpha = (a_1, \ldots, a_n)^T \in \mathbb{R}^n \mid \alpha^T \alpha = 1\}$。那么 $\mathrm{O}(n)$ 在 S^{n-1} 上有一个自然的作用，即为 $g \cdot \alpha = g\alpha$，其中 $g\alpha$ 是矩阵的乘法。

例 2.4.3. 记 $\mathcal{H} = \{x + y\mathrm{i} \mid y > 0\}$ 为上半平面，我们考虑矩阵群 $\mathrm{SL}_2(\mathbb{Z})$ 在 $\mathcal{H}$ 上的作用：对任意 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), z \in \mathcal{H}$，我们定义

$$\gamma \cdot z = \frac{az + b}{cz + d}. \tag{2.2}$$

由于

$$\mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \mathrm{Im}\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right) = \frac{y}{|cz+d|^2} > 0,$$

其中 $z=x+y\mathrm{i}$，因此 $\gamma\cdot z\in\mathcal{H}$。下面我们验证上面确实定义了 $\mathrm{SL}_2(\mathbb{Z})$ 在 $\mathcal{H}$ 上的作用。根据定义显然有 $\begin{pmatrix}1&0\\0&1\end{pmatrix}\cdot z=z$，因此我们只需验证第一条即可。设 $\gamma_1=\begin{pmatrix}a_1&b_1\\c_1&d_1\end{pmatrix},\gamma_2=\begin{pmatrix}a_2&b_2\\c_2&d_2\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$。一方面我们有

$$\gamma_1\cdot(\gamma_2\cdot z)=\gamma_1\cdot\frac{a_2z+b_2}{c_2z+d_2}=\frac{a_1\frac{a_2z+b_2}{c_2z+d_2}+b_1}{c_1\frac{a_2z+b_2}{c_2z+d_2}+d_1}=\frac{(a_1a_2+b_1c_2)z+(a_1b_2+b_1d_2)}{(c_1a_2+d_1c_2)z+(c_1b_2+d_1d_2)}.$$

另一方面我们有

$$\gamma_1\gamma_2=\begin{pmatrix}a_1a_2+b_1c_2&a_1b_2+b_1d_2\\c_1a_2+d_1c_2&c_1b_2+d_1d_2\end{pmatrix}.$$

因此有

$$(\gamma_1\gamma_2)\cdot z=\frac{(a_1a_2+b_1c_2)z+(a_1b_2+b_1d_2)}{(c_1a_2+d_1c_2)z+(c_1b_2+d_1d_2)}=\gamma_1\cdot(\gamma_2\cdot z).$$

这便验证了群作用定义的第一条，因此(2.2)给出了 $\mathrm{SL}_2(\mathbb{Z})$ 在 $\mathcal{H}$ 上的一个作用。

例2.4.2中的第四个例子指出了对称群可以自然的看作一个群作用。事实上，反过来，任何一个群作用，也能视作集合 X 上的置换。

定理 2.4.4. 设 G 在 X 上有一个群作用，设 $g\in G$，定义

$$\begin{aligned}\sigma_g:\ X&\longrightarrow X\\ x&\longmapsto g\cdot x.\end{aligned}$$

那么 σ_g 是 X 上的一个置换，即 $\sigma_g\in S_X$，并且 $g\mapsto\sigma_g$ 是从群 G 到 S_X 的一个群同态。

证明. 我们先证明 σ_g 是 X 到 X 的一个双射，对任意 $y\in X$，根据定义可知

$$\sigma_g(g^{-1}\cdot y)=g\cdot(g^{-1}\cdot y)=(gg^{-1})\cdot y=1\cdot y=y.$$

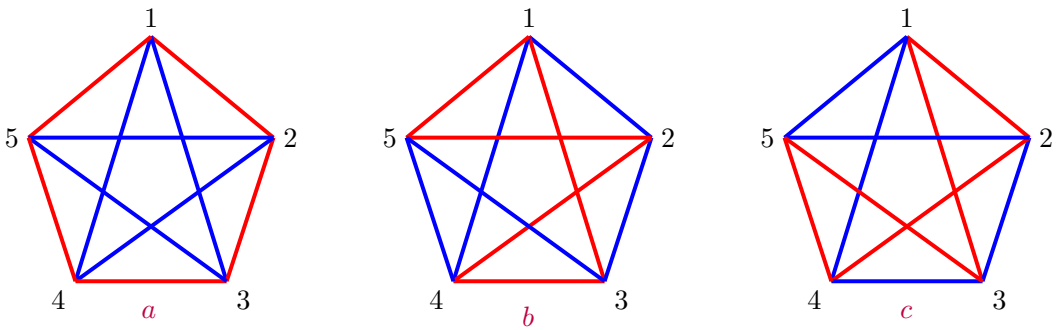
这表明 σ_g 是满射。另一方面若存在 $x_1,x_2\in X$ 使得 $\sigma_g(x_1)=\sigma_g(x_2)$，即 $g\cdot x_1=g\cdot x_2$，将此式两边同时用 g^{-1} 作用可得 $x_1=x_2$，因此 σ_g 也是单射。下面我们证明 $g\to\sigma_g$ 是群同态。事实上，对任意 $g_1,g_2\in G$ 以及 $x\in X$，我们有

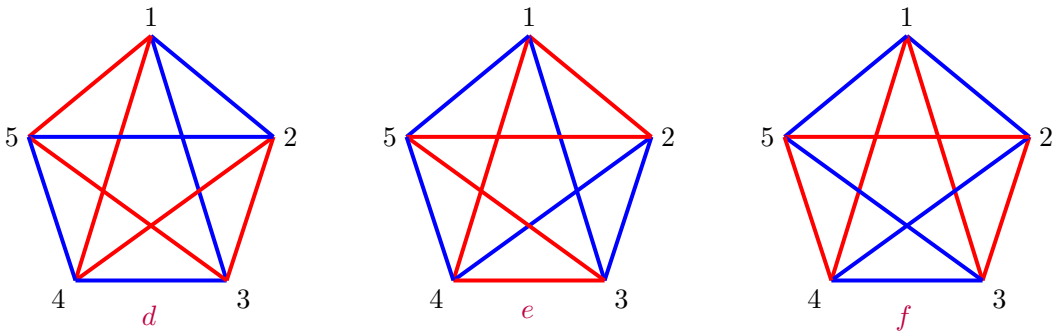
$$(\sigma_{g_1}\circ\sigma_{g_2})(x)=\sigma_{g_1}(\sigma_{g_2}(x))=g_1\cdot(g_2\cdot x)=(g_1g_2)\cdot x=\sigma_{g_1g_2}(x).$$

因此 $\sigma_{g_1}\circ\sigma_{g_2}=\sigma_{g_1g_2}$。

下面我们通过一个更具体的例子来展示如何把群作用视作集合 X 上的置换。

例 2.4.5. 我们构造一个 S_5 在六元集合上的作用。我们记 $X=\{a,b,c,d,e,f\}$ 为如下六个图组成的集合。





这六个图均可以看成两个闭环组成的图形，即红色闭环和蓝色闭环。例如，图 a 的红色闭环可视为 $1-2-3-4-5$，蓝色闭环可视为 $1-3-5-2-4$。我们定义 S_5 在 X 上的作用为 S_5 分别作用在两个不同颜色的闭环上，例如我们考虑 $\sigma=(1\ 2)\in S_5$，那么它将红色闭环作用为 $2-1-3-4-5$，将蓝色闭环作用为 $2-3-5-1-4$。这便是图 d，注意到这个作用并不保持闭环颜色不动。因此我们有 $\sigma\cdot a=d$。同样地，图 b 的两个闭环分别为 $1-2-3-5-4$ 和 $1-3-4-2-5$，那么 σ 在这两个闭环上的作用分别变为 $2-1-3-5-4$ 和 $2-3-4-1-5$，此即为图 c，即有 $\sigma\cdot b=c$。同样我们可以验证 $\sigma\cdot e=f$。于是 σ 在 X 上的作用等同于 S_X 中的元素 $(a\ d)(b\ c)(e\ f)$。对于 S_5 中的其它元素我们同样也能按照上述方法定义它在 X 上的作用，直接验证容易知道这构成一个群作用。由此我们可以得到一个群同态 $S_5\to S_X$。类似地我们可以验证 $(1\ 2\ 3)$ 在 X 上的作用等同于 $(a\ f\ c)(b\ e\ d)$。而 $(1\ 2\ 3\ 4)$ 在 X 上的作用则等同于 $(a\ c\ e\ b)$。

注 3. 上述定理中的映射 $G\to S_X, g\mapsto\sigma_g$ 的核称为该群作用的**核**。特别地，若该同态是单射，那么我们称 G 在 X 上的作用是**忠实的**。容易看出来，元素 g 属于该群作用的核当且仅当对任意 $x\in X$ 均有 $g\cdot x=x$。

定义 2.4.6. 设 G 是 X 上的一个群作用，对任意 $x\in X$，我们称集合 $G_x=\{g\in G\mid g\cdot x=x\}$ 为 x 的**稳定化子**。我们称集合 $\mathrm{orbit}(x)=\{g\cdot x\mid g\in G\}$ 为 G 中包含 x 的**轨道**。若 X 只有一个轨道，那么我们称该作用是**可迁的**。

例 2.4.7. 对于例2.4.2中的例子，我们分别计算它们的轨道。

1. 对于平凡作用而言，X 中的每一个元素均为一个轨道，因此当 X 中元素个数 ≥ 2 时，平凡作用不是可迁的。

2. 对于非零向量 $x,y\in V$ 而言，它们在同一个轨道中，当且仅当存在 $k\in\mathbb{R}^*$ 使得 $x=ky$，即 x,y 线性相关。因此 x 所在的轨道即为所有和 x 线性相关的非零向量组成的集合。从几何上来看即为所有过原点的直线（挖去原点）。而零向量自己构成一个单独的轨道。

3. 对任意非零向量 $\alpha,\beta\in V$，我们知道存在 $\mathcal{A}\in\mathrm{GL}(V)$ 使得 $\mathcal{A}(\alpha)=\beta$。因此 $\mathcal{A}\cdot\overline{\alpha}=\overline{\beta}$。故该作用是可迁的。

4. 对任意 $x,y\in X$，我们取对换 $\sigma=(x\ y)\in S_X$，于是 $\sigma\cdot x=y$。因此该作用是可迁的。

5. 设 $x\in S^{n-1}$ 是一个单位向量，根据高等代数的知识我们知道 x 可扩充为一组标准正交向量组 $x,\alpha_2,\ldots,\alpha_n$，记 $Q=(x,\alpha_2,\ldots,\alpha_n)$，于是 $Q\in\mathrm{SO}(n)$，并且 $Qe_1=x$，其中 $e_1=(1,0,\ldots,0)^T$。因此任意一个单位向量都和 e_1 在同一个轨道中，故该作用是可迁的。

我们可以通过轨道将 A 划分为若干个等价类。

定理 2.4.8. 设 G 是 X 上的一个群作用，对任意 $x, y \in X$，我们定义 $x \sim y$ 当且仅当 $y \in \mathrm{orbit}(x)$，那么这是 X 上的一个等价关系，并且对任意 $x \in X$ 有 $|\mathrm{orbit}(x)| = [G : G_x]$。

证明. 等价关系的三个条件均可从定义直接验证。下面我们证明 G_x 是 G 的一个子群。事实上，对任意 $g, h \in G_x$，由于 $h \cdot x = x$，两边同时乘以 h^{-1} 即得 $h^{-1} \cdot x = x$，故 $(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot x = x$。这表明 $gh^{-1} \in G_x$，由命题2.2.3可知 G_x 是 G 的子群。最后我们构造一个 G_x 的陪集集合到 $\mathrm{orbit}(x)$ 的一个双射。

$$\begin{array}{rccc} \Psi: & \{gG_x \mid g \in G\} & \longrightarrow & \mathrm{orbit}(x) \\ & gG_x & \longmapsto & g \cdot x. \end{array}$$

由于 G_x 中元素作用在 x 上不动，因此 Ψ 是定义良好的。容易看出 Ψ 是满射，因此我们只需证明 Ψ 是单射即可，若存在 $g_1, g_2 \in G$ 使得 $g_1 \cdot x = g_2 \cdot x$，两边同时乘以 g_2^{-1} 可得 $g_2^{-1} g_1 \cdot x = x$，即有 $g_2^{-1} g_1 \in G_x$，因此由引理2.3.10可知 $g_2 G_x = g_1 G_x$，故 Ψ 是单射。所以集合 $\mathrm{orbit}(x)$ 的元素个数等于 $[G : G_x]$。

作为应用，我们可以证明如下 Burnside-Frobenius 定理。

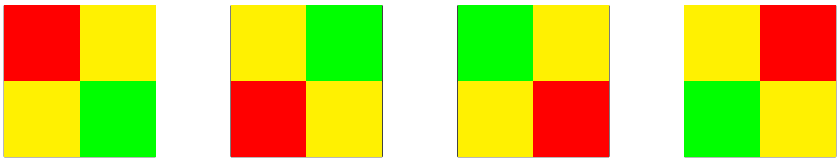
定理 2.4.9 (Burnside-Frobenius)**.** 设 G 是一个有限群，且作用在有限集 X 上。记 r 为 X 中不同的轨道个数，对 $g \in G$，记 $\mathrm{Fix}(g)$ 为 X 中被 g 固定的元素。那么我们有

$$r = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

证明. 我们考虑集合 $S = \{(g, x) \in G \times X \mid gx = x\}$。一方面我们有 $|S| = \sum_{g \in G} |\mathrm{Fix}(g)|$。另一方面，设 $X_1, \ldots, X_r$ 是 X 中不同的轨道，那么我们有

$$|S| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|\mathrm{orbit}(x)|} = |G| \sum_{i=1}^{r} |X_i| \times \frac{1}{|X_i|} = |G| r.$$

该定理的一个经典的应用是组合计数，我们下面举一个例子加以说明。考虑一个 2×2 的方框，每个小方框可以任意染 k 种颜色中的一种，那么共有多少种染色方法？我们这里约定若两种染色是旋转或者镜像对称相同的，那么则认为它们是一种染色，例如下面四个图则被视为同一种染色：



我们需要把问题转化为群论的语言，为简单起见，我们先考虑 $k = 2$ 的情况。令

$$G = D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}.$$

我们用 c_1, c_2 分别代指两种不同的染色，我们用一个四元组（左上角，右上角，右下角，左下角）对应的编号来表示相应方框的颜色。因此总共有 16 个不同的四元组，即为

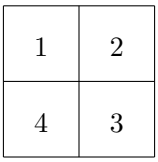
$$(c_1, c_1, c_1, c_1), (c_1, c_1, c_1, c_2), (c_1, c_1, c_2, c_1), (c_1, c_1, c_2, c_2), (c_1, c_2, c_1, c_1), (c_1, c_2, c_1, c_2),$$

$$(c_1,c_2,c_2,c_1),(c_1,c_2,c_2,c_2)(c_2,c_1,c_1,c_1),(c_2,c_1,c_1,c_2),(c_2,c_1,c_2,c_1),(c_2,c_1,c_2,c_2),$$

$$(c_2,c_2,c_1,c_1),(c_2,c_2,c_1,c_2),(c_2,c_2,c_2,c_1),(c_2,c_2,c_2,c_2).$$

我们记这十六个四元组组成的集合为 X，那么 G 在 X 上有一个自然的作用，我们需要计算的而且两种染色被视为相同的当且仅当它们在该作用的同一个轨道中，因此不同的染色个数即为轨道的个数。应用上面的 Burnside-Frobenius 定理可知，我们只需要计算 G 中每个元素的固定数即可，我们依次来进行计算。当 $g=1$ 时，显然每个元素都被 1 固定，因此 $|\mathrm{Fix}(1)|=16$。当 $g=r$ 时，被 g 固定的元素表示的是旋转 90° 不动，因此只有 (c_1,c_1,c_1,c_1) 和 (c_2,c_2,c_2,c_2)，故 $|\mathrm{Fix}(r)|=2$。当 $g=r^2$ 时，被 g 固定的元素表示的是旋转 180° 不动，因此有 $(c_1,c_1,c_1,c_1),(c_1,c_2,c_1,c_2),(c_2,c_1,c_2,c_1),(c_2,c_2,c_2,c_2)$ 这几个元素，故 $|\mathrm{Fix}(r^2)|=4$。类似地计算可知 $|\mathrm{Fix}(r^3)|=2,|\mathrm{Fix}(s)|=4,|\mathrm{Fix}(sr)|=8,|\mathrm{Fix}(sr^2)|=4,|\mathrm{Fix}(sr^3)|=8$。因此根据 Burnside-Frobenius 定理可知其轨道数为 6。

下面我们考虑更一般的情况，我们仍然记 X 为所有可能得染色组成的集合，然而此时集合 X 的大小急剧变大，如果我们仍然按照上面的方法分析将会导致计算量太大。因此我们需要进一步分析来简化计算。我们注意到 G 中元素可以视作四个方框上的一个置换，我们按下图约定每个方框代表的数字：



例如当 $g=r$，它对应的是将正方形逆时针旋转 90°，因此它将 1 作用至 2，2 作用至 3，3 作用至 4，4 作用至 1，这说明它对应的置换为

$$r\longleftrightarrow\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=(1\ 2\ 3\ 4).$$

而这个置换表明如果某个 X 中的元素被 r 固定，那么 1 代表的方框和 2 代表的方框的颜色一定是相同的，同样的，2 代表的方框和 3,4 代表的方框颜色都需要是相同的，总共有 k 种颜色，因此 X 中被 r 固定的元素个数恰好是 k。当 $g=r^2$ 时，和上面的分析一样可知它对应的置换为

$$r^2\longleftrightarrow\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(1\ 3)(2\ 4).$$

这意味着如果某个 X 中的元素被 r^2 固定，那么 1 代表的方框和 3 代表的方框的颜色一定是相同的，而 2 代表的方框和 4 代表的方框的颜色是相同的。因此 X 中被 r^2 固定的元素个数恰好是 k^2。根据这样的分析，我们知道要计算 X 中有多少元素被 g 固定，只需计算 g 对应的置换的轮换分解中轮换的个数即可。我们记 $c(g)$ 为 g 的轮换个数，例如 $c(1)=4,c(r)=1,c(r^2)=2$。同样计算可以得到 $c(r^3)=1,c(s)=2,c(sr)=3,c(sr^2)=2,c(sr^3)=3$ 那么根据 Burnside-Frobenius 定理可知其轨道数目可表示为

$$\frac{1}{|G|}\sum_{g\in G}k^{c(g)}=\frac{1}{8}(k^4+2k^3+3k^2+2k).$$

Burnside-Frobenius 定理另一个简单的应用是 Jordan 引理，可参考练习2.4.11。

2.4.2 左乘作用和 Cayley 定理

这一节我们考虑一类特殊的群作用。设 G 是一个群，$X = G$，我们定义 G 在 G 上的左乘作用为

$$g \cdot x = gx, \qquad \forall g, x \in G.$$

这里 gx 为 G 中的乘法运算。我们这一节主要证明任何一个群都同构于对称群的一个子群。为此，我们先看一个简单的例子。

例 2.4.10. 设 $G = \{1, a, b, c\}$ 为 *Klein* 群。我们将这四个元素分别标号为 $1, 2, 3, 4$，那么在左乘作用下我们考虑 σ_a：

$$a \cdot 1 = a, \quad a \cdot a = 1, \quad a \cdot b = c, \quad a \cdot c = b,$$

因此我们换成标号则有

$$\sigma_a(1) = 2, \quad \sigma_a(2) = 1, \quad \sigma_a(3) = 4, \quad \sigma_a(4) = 3.$$

这意味着我们可以将 σ_a 视作 S_4 中的元素 $(1\ 2)(3\ 4)$。类似地，我们可以将 σ_b 视作 $(1\ 3)(2\ 4)$，将 σ_c 视作 $(1\ 4)(2\ 3)$。这便给出了 $G \to S_4$ 的一个单同态。

更一般地，我们还可以考虑左陪集作用。设 G 是一个群，H 是 G 的一个子群，X 是 H 的左陪集集合。那么我们定义 G 在 X 上的作用为

$$g \cdot xH = gxH, \qquad \forall g \in G, xH \in X.$$

定理 2.4.11. 设 G 是一个群，H 是 G 的一个子群，X 是 H 的左陪集集合。G 在 X 上的作用为左陪集作用。那么

1. G 在 X 上的作用是可迁的；
2. $1H \in X$ 在 G 中的稳定化子是 H；
3. 该作用的核是 $\bigcap_{x \in G} xHx^{-1}$，即为 G 中包含在 H 中的最大正规子群。

证明. 1. 根据定义可知 $g \cdot H = gH$，这表明对任意 $g \in G$，gH 均在 $\mathrm{orbit}(H)$ 中，因此该作用是可迁的。

2. 由引理2.3.10知 $gH = H$ 当且仅当 $g \in H$，因此 $G_H = H$。

3. 记该群作用的核为 K，那么我们知道 $g \in K$ 当且仅当对任意左陪集 xH 均有 $g \cdot xH = xH$，这等价于对任意 $x \in G$ 均有 $g \in xHx^{-1}$。故 $K = \bigcap_{x \in G} xHx^{-1}$。

推论 2.4.12 (Cayley 定理)**.** 任意群都同构于对称群的子群。特别地，若 G 是 n 阶群，那么 G 同构于 S_n 的子群。

证明. 取定理2.4.11中的 H 为 $\{1\}$，那么该左乘作用给出了群同态：$G \to S_G$，根据定理2.4.11知该群同态的核为 $\bigcap_{x \in G} x\{1\}x^{-1} = \{1\}$。因此该群同态是单射，故由第一同构定理可知 G 同构于 S_G 的一个子群。

2.4.3 共轭作用和类方程

这一节我们讨论另一类特殊的群作用–共轭作用。设 G 是一个群，$X = G$。我们定义 G 在 G 上的**共轭作用**为

$$g \cdot x = gxg^{-1} \qquad \forall g, x \in G.$$

我们称 G 在共轭作用下的轨道称为 G 的**共轭类**。

例 2.4.13. *1. 若 G 是交换群，那么 G 在自身的共轭作用是平凡的，它的所有共轭类是 $\{x\}$，$x \in G$；*

2. 设 $G = S_3$，那么它的共轭类有三个：$\{1\}, \{(1\ 2), (1\ 3), (2\ 3)\}, \{(1\ 2\ 3), (1\ 3\ 2)\}$。

3. 设 $G = \mathrm{GL}_n(\mathbb{C})$，那么和 $g \in G$ 共轭的元素即为和 g 相似的矩阵。

利用定理2.4.8，我们可以计算和某个元素共轭的元素个数，即每个共轭类中所含元素个数：

命题 2.4.14. *设 $g \in G$，那么 g 所在的共轭类含有元素个数为 $|G : C_G(g)|$。*

证明. 根据定义可知 $C_G(g)$ 即为 g 在共轭作用下的稳定化子，即有 $C_G(g) = G_g$，故由定理2.4.8有 $\mathrm{orbit}(g) = [G : C_G(g)]$。而 $\mathrm{orbit}(g)$ 即为 g 所在的共轭类。

如果我们将 G 中元素按照共轭类进行划分，便可以得到著名的**类方程**。

定理 2.4.15 (类方程)**.** *设 G 是一个有限群，$g_1, \ldots, g_r$ 是 G 中所有不包含在中心中的共轭类的代表元。那么我们有*

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

证明. G 中每个元素都恰好包含在一个共轭类中，设 $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_m$ 为所有的共轭类，那么我们有

$$|G| = |\mathcal{C}_1| + |\mathcal{C}_2| + \cdots + |\mathcal{C}_m|.$$

若 $g \in Z(G)$，那么 g 和 G 中所有元素交换，因此 g 所在的共轭类只有它自己，反之，若 g 所在的共轭类只有它自己，那么对任意 $h \in G$ 均有 $hgh^{-1} = g$，即 $hg = gh$。故 $g \in Z(G)$。所以我们不妨设后 $|Z(G)|$ 个共轭类均恰好只有一个元素。对 $i = 1, 2, \ldots, m - |Z(G)|$，若 g_i 是 $\mathcal{C}_i$ 中的代表元，那么根据定理2.4.8有 $|\mathcal{C}_i| = |G : C_G(g_i)|$。综上所述，我们得到了

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

例 2.4.16. *设 $G = S_3$，根据之前的计算我们知道 $Z(G) = \{1\}$，并且不在中心中的共轭类有两个，其代表元分别为 $(1\ 2), (1\ 2\ 3)$。直接计算可知 $C_G((1\ 2)) = \langle (1\ 2) \rangle, C_G((1\ 2\ 3)) = \langle (1\ 2\ 3) \rangle$。因此我们有*

$$|Z(G)| + |G : C_G((1\ 2))| + |G : C_G((1\ 2\ 3))| = 1 + 3 + 2 = 6 = |G|.$$

利用类方程我们可以证明一个关于 p-群的结论。设 G 是一个群，p 是一个素数，若 G 的阶是 p 的幂次，则称 G 是 **p-群**。

定理 2.4.17. *p-群中心非平凡。*

证明. 设 G 是一个 p-群，若 $Z(G)$ 是平凡的，那么 $|Z(G)|=1$。设 $g_1,\dots,g_r$ 是 G 中所有不包含在中心中的共轭类的代表元，那么 $C_G(g_i)$ 是 G 的真子群，而 G 的阶是 p^n，因此 p 整除 $[G:C_G(g_i)]$。但是根据类方程可知

$$1=|Z(G)|=|G|-\sum_{i=1}^{r}|G:C_G(g_i)|.$$

但是上式左边被 p 整除，显然矛盾。因此必有 $|Z(G)|=1$。

同样作为类方程的另一个推论，我们可以证明著名的 Cauchy 定理。它部分回答了 Lagrange 定理的逆问题。

定理 2.4.18 (Cauchy)**.** 设 G 是一个群，p 是整除 $|G|$ 的一个素数，那么 G 中有 p 阶元素。

证明. 设 $|G|=n$，我们对 n 进行归纳。当 $n=1,2$ 时，结论显然成立。下面假设 $n>2$，且 p 是 n 的一个素因子。若 $n=p$，结论显然成立。因此不妨设 $n>p$，我们分两种情况讨论：

G 是交换群： 设 $1\neq g\in G$ 的阶为 m，若 $p\mid m$，那么根据命题2.2.11可知 $g^{m/p}$ 的阶即为 p。若 $p\nmid m$，那么群 $G/\langle g\rangle$ 的阶为 $n/m<n$，因此根据归纳假设知 G/H 存在 p 阶元，设为 $x\langle g\rangle$，我们只需证明 p 整除 x 的阶即可。事实上，设 x 的阶为 k，那么 $(x\langle g\rangle)^k=\langle g\rangle$，因此根据命题2.2.10可知 $p\mid k$。于是再次根据命题2.2.11可知 $x^{k/p}$ 的阶为 p。

G 是非交换群： 设 $g_1,\dots,g_r$ 是 G 中所有不包含在中心中的共轭类的代表元。那么根据类方程有

$$|G|=|Z(G)|+\sum_{i=1}^{r}|G:C_G(g_i)|.$$

由于 G 不是交换群，因此 $f\geq 1$，且所有的 $C_G(g_i)$ 是 G 的真子群，若存在某个 i 使得 p 整除 $|C_G(g_i)|$，那么结论得证，否则对所有 i 均有 p 整除 $|G:C_G(g_i)|$。因此根据类方程知 p 整除 $|Z(G)|$。而因此 G 不是交换群，所以 $Z(G)$ 是 G 的真子群，由此结论得证。

更进一步，设 n_p 为 G 中阶为 p 的元素个数，可以证明 $n_p\equiv -1 \pmod p$。

和左乘作用类似，共轭作用不仅能作用在元素上，也能作用在子群上，对此我们仅举一个例子加以说明。

例 2.4.19. 考虑 S_5 的所有五阶子群组成的集合 Y。因为五阶子群只能是五阶循环群，且除了单位元以外，其余元素均为 5-轮换。因为 S_5 中共有 24 个 5-轮换，因此 S_5 共有 6 个五阶子群。我们定义 S_5 在 Y 上的作用为 $H\mapsto \sigma H\sigma^{-1}$。事实上，我们可以将 Y 具体的写出来：

$$Y=\{\langle(1\ 2\ 3\ 4\ 5)\rangle,\langle(1\ 2\ 3\ 5\ 4)\rangle,\langle(1\ 2\ 4\ 5\ 3)\rangle,\langle(1\ 2\ 5\ 4\ 3)\rangle,\langle(1\ 2\ 5\ 3\ 4)\rangle\},\langle(1\ 2\ 4\ 3\ 5)\rangle.$$

我们分别记这六个子群为 H_a,H_b,H_c,H_d,H_e,H_f。考虑 $\sigma=(1\ 2)$ 在 Y 上的作用，直接计算可知

$$\sigma\cdot H_a=\sigma\langle(1\ 2\ 3\ 4\ 5)\rangle\sigma^{-1}=\langle(1\ 3\ 4\ 5\ 2)\rangle=\langle(1\ 2\ 5\ 4\ 3)\rangle=H_d.$$

同样计算可知 $\sigma\cdot H_b=H_c,\sigma\cdot H_e=H_f$，因此 σ 在 Y 上的作用等同于 $(H_a\ H_d)(H_b\ H_c)(H_e\ H_f)$。我们可以发现这个作用和例2.4.5中的作用是非常相似的。事实上，这两个作用是同构的，其中集合 X 和 Y 之间的关系由如下对应给出：假设子群 H 由 c 生成，那么它对应 X 中的两个闭环分别由 $c^{\pm 1}$ 和 $c^{\pm 2}$ 给出。例如 H_a 由 $(1\ 2\ 3\ 4\ 5)$ 生成，那么它的两个闭环分别为 $1-2-3-4-5$ 和 $1-3-5-2-4$，因此它对应的便是 X 中的图 a。容易验证 H_a,H_b,H_c,H_d,H_e,H_f 对应的图分别是 a,b,c,d,e,f。

2.4.4 Sylow 定理

这一节我们证明著名的 Sylow 定理。它在有限群的分类上有重要作用。

定义 2.4.20. 设 p 是一个素数，G 是阶为 $p^k m$ 的群，其中 $p \nmid m$，我们称 G 中阶为 p^k 的子群为 **Sylow p-子群**。我们记 G 中所有 Sylow p-子群组成的集合为 $Syl_p(G)$，记 Sylow p- 子群的个数为 $n_p(G)$。

根据定义容易看出如果 P 是 G 的 Sylow p-子群，那么对任意 $g \in G$，gPg^{-1} 均为 G 的 Sylow p-子群。在给出著名的 Sylow 定理之前，我们先看几个例子。

例 2.4.21. *设 G 是一个群，p 是一个素数。*

1. *若 G 是 p-群，那么 G 只有唯一的 Sylow p-子群，即为 G 自身。*
2. *若 G 是交换群，那么 G 的 Sylow p-子群为 G 中所有阶为 p 的幂次的元素组成的集合。*
3. *S_3 有 3 个 Sylow 2-子群，分别由 $(1\ 2), (1\ 3), (2\ 3)$ 生成。而 S_3 只有一个 Sylow 3-子群，由 $(1\ 2\ 3)$ 生成。*
4. *若 P 是 G 的 Sylow p-子群，那么对任意包含 P 的子群 H，P 也是 H 的 Sylow p-子群。*

下面我们证明如下 Sylow 定理。

定理 2.4.22. *设 p 是一个素数，G 是阶为 $p^k m$ 的群，其中 $p \nmid m$。*

1. *Sylow p-子群存在；*
2. *设 $Q \leq G$ 是一个阶为 p^ℓ 的子群，那么存在 G 的一个 Sylow p-子群 P 使得 $Q \leq P$。特别地，G 中任意两个 Sylow p-子群都是共轭的；*
3. *$n_p \equiv 1 \pmod p$，且 $n_p = [G : N_G(P)]$。特别地，$n_p \mid m$。*

引理 2.4.23. *设 G 是有限群，H 是 G 的一个子群，且素数 p 整除 $|H|$。如果 P 是 G 的一个 Sylow p-子群，那么存在元素 $g \in G$ 使得 $gPg^{-1} \cap H$ 是 H 的 Sylow p-子群。*

证明. 设 $X = \{g_1 P = P, g_2 P, \ldots, g_m P\}$ 是 P 的所有陪集构成的集合。考虑 H 在 X 上的左乘作用，由 Sylow p-子群的定义知 $m = |X| = |G|/|P|$ 和 p 互素。因此根据定理2.4.8可知该左乘作用的所有轨道构成 X 的一个划分，于是一定有一个轨道的元素个数不是 p 的倍数，设为 gP 所在的轨道。gP 在 H 中的稳定化子为

$$H_{gP} = \{h \in H \mid h \cdot gP = gP\} = \{h \in H \mid hg \in gP\} = gPg^{-1} \cap H.$$

再次利用定理2.4.8可知 $|\mathrm{orbit}(gP)| = [H : gPg^{-1} \cap H]$ 和 p 互素。因此 $gPg^{-1} \cap H$ 构成 H 的一个 Sylow p-子群。

定理2.4.22的证明. 我们先用归纳法证明 Sylow p-子群的存在性。当 $|G| = 1, 2, 3$ 时，结论显然成立。下面假设对于阶小于 $|G|$ 的群均成立。我们考虑 G 的类方程：

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

如果 $p \nmid |Z(G)|$，那么一定存在 i 使得 $p \nmid |G : C_G(g_i)|$。因此 $p^k \mid |C_G(g_i)|$。而 $C_G(g_i)$ 是 G 的真子群，故由归纳假设知 $C_G(g_i)$ 存在阶为 p^k 的子群，因此它也是 G 的子群，即为 Sylow p-子群。

若 $p \mid |Z(G)|$，由 Cauchy 定理2.4.18知 $Z(G)$ 存在一个 p 阶元 c，由于 c 在 G 的中心中，因此 $\langle c\rangle$ 是 G 的 p 阶正规子群，根据归纳假设知 $G/\langle c\rangle$ 有一个阶为 p^{k-1} 的子群。根据命题2.3.4可知 $G/\langle c\rangle$ 和 G 中包含 $\langle c\rangle$ 的子群一一对应，即存在 G 的子群 H 使得 $H/\langle c\rangle$ 的阶为 p^{k-1}，故 H 是 G 中阶为 p^k 的子群。

(2) 的证明可由引理2.4.23得到。事实上，设 Q 是 G 的一个 p-子群，P 是 G 的一个 Sylow p-子群，那么根据引理2.4.23可知存在 $g \in G$ 使得 $gPg^{-1} \bigcap Q$ 为 Q 的 Sylow p-子群，但是 Q 本身是 p-群，因此它的 Sylow p-子群即为本身，故 Q 包含在 Sylow p-子群 gPg^{-1} 中。特别地，若 Q 是任意一个 Sylow p-子群，根据前面的证明可知存在 $g \in G$ 使得 $Q \subseteq gPg^{-1}$，但两者的阶相同，因此必有 $Q = gPg^{-1}$，由此可得任意一个 Sylow p-子群均与 P 共轭。

最后我们证明 (3)。我们记 $X = \{P = P_1, P_2, \ldots, P_{n_p}\}$ 为 G 的所有 Sylow p-子群组成的集合。考虑 G 在 X 上的共轭作用，根据前面的证明可知该作用是可迁的。根据定义可知 P 的稳定化子即为正规化子 $N_G(P)$。因此由定理2.4.8可知

$$n_p(G) = |X| = |G|/|N_G(P)|.$$

由于 $P \subseteq N_G(P)$，因此 $|G|/|N_G(P)|$ 整除 m，故有 $n_p(G) \mid m$。

然而为了要得到更细致的 n_p 的信息，仅仅只考虑 G 在 X 上的作用是不够的。下面我们再考虑 $P = P_1$ 在 X 上的共轭作用，此时 P 在 X 上的作用则不一定是可迁的了，我们不妨设该作用的所有轨道为 $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_s$，并且 $P_1, \ldots, P_s$ 分别为轨道 $\mathcal{C}_1, \ldots, \mathcal{C}_s$ 的代表元。下面我们考虑每个轨道的大小。首先注意到 P_i 的稳定化子即为 $N_P(P_i)$，于是由定理2.4.8我们有

$$n_p = |\mathcal{C}_1| + \cdots + |\mathcal{C}_s| = \frac{|P|}{|N_P(P_1)|} + \cdots + \frac{|P|}{|N_P(P_s)|}. \tag{2.3}$$

当 $i = 1$ 时，因为 $P = P_1$，显然有 $N_P(P_1) = P$。下面我们证明当 $i > 1$ 时，必有 $N_P(P_i) \subsetneq P$。若 $N_P(P_i) = P$，那么由于 $N_P(P_i) = N_G(P_i) \cap P$ 可知 $P \subseteq N_G(P_i)$。然而根据例2.3.14的第七条可知 P_i 是 $N_G(P_i)$ 的正规子群，因此 P_i 是 $N_G(P_i)$ 的正规 Sylow p-子群，而上面我们证明了 Sylow p-子群都是共轭的，因此 $N_G(P_i)$ 只有唯一的 Sylow p- 子群。但是 P 和 P_i 都是 $N_G(P_i)$ 的 Sylow p-子群，故 $P = P_i$，这便得到了矛盾。所以 $N_P(P_i)$ 是 P 的真子群。由于 P 是 p-群，这表明当 $i > 1$ 时，$|P|/|N_G(P_i)|$ 均为 p 的倍数，所以由式(2.3)可得 $n_p \equiv 1 \pmod{p}$。

推论 2.4.24. *G 有一个正规的 Sylow p-子群当且仅当 $n_p(G) = 1$。*

Sylow 定理在群分类问题上有着重要作用。下面我们将利用 Sylow 定理给出小阶群的分类。

命题 2.4.25. *设 G 是 pq 阶群，其中 $p < q$ 是两个素数且 $p \nmid q - 1$。那么 $G \simeq \mathbb{Z}/pq\mathbb{Z}$。*

证明. 根据 Sylow 定理，G 有一个 Sylow p-子群 P 和一个 Sylow q-子群 Q。由于 Sylow p-子群的个数满足 $n_p \equiv 1 \pmod{p}$ 且 $n_p \mid pq$。由此可得 $n_p \mid q$。但 q 是素数，所以 $n_p = 1$ 或 q。若 $n_p = q$，则有 $q \equiv 1 \pmod{p}$，与已知条件矛盾。所以可得 $n_p = 1$。同理可得 $n_q = 1$ 或 p。若 $n_q = p$，则有 $p \equiv 1 \pmod{q}$，但 $p < q$，这显然不可能成立。所以我们证明了 P, Q 都是 G 的正规子群。设 $P = \langle x\rangle, Q = \langle y\rangle$。由于 $G/C_G(P)$ 同构于 $\mathrm{Aut}(P)$ 的一个子群，而 $|\mathrm{Aut}(P)| = p - 1$ 和 pq 互素，所以 $C_G(P) = G$，因此 x 和 G 中所有元素均可交换，特别地，$xy = yx$，所以根据命题2.2.12可知 xy 的阶为 pq。因此 $G = \langle xy\rangle$。

习题

练习 2.4.1. 证明下列作用是群作用，判断它们是否是可迁的？是否是忠实的？并计算它们的轨道。

1. $\mathbb{R}$ 在 $\mathbb{R}^2$ 上的作用：$r\cdot(x,y)=(x+ry,y)$。
2. $\mathbb{R}$ 在 $\mathbb{C}$ 上的作用：$\theta\cdot z=\mathrm{e}^{\mathrm{i}\theta}z$。

练习 2.4.2. 证明群 G 在自身上的作用 $g\cdot a=ag^{-1},\forall a,g\in G$ 是一个群作用。若 G 不是交换群，$g\cdot a=ag$ 不是一个群作用。

练习 2.4.3.
1. 构造 S_6 的一个子群使得其同构于 S_3 且在 $\{1,2,3,4,5,6\}$ 上的作用是可迁的。
2. 构造 S_8 的一个子群使得其同构于 Q_8。
3. 证明当 $n<8$ 时，S_n 不存在同构于 Q_8 的子群。

练习 2.4.4. 设 X 是一个非空集合，G 是 S_X 的一个子群。

1. 证明对任意 $\sigma\in G,a\in X$ 均有 $\sigma G_a\sigma^{-1}=G_{\sigma(a)}$。
2. 若 G 在 X 上的作用是可迁的，证明 $\bigcap_{\sigma\in G}\sigma G_a\sigma^{-1}=1$。
3. 假设 G 是可迁的交换群，证明对任意 $1\neq\sigma\in G,a\in X$ 均有 $\sigma(a)\neq a$。由此证明 $|G|=|X|$。
4. 求所有正整数 $n=|X|$ 使得上一问中的 G 在同构意义下是唯一的。

练习 2.4.5.
1. 计算 D_8,D_{10} 的所有共轭类。
2. 设 $n=2k$，计算 D_{2n} 的所有共轭类，并写出 D_{2n} 的类方程。
3. 设 $n=2k+1$，计算 D_{2n} 的所有共轭类，并写出 D_{2n} 的类方程。
4. 写出 D_{12} 的所有 *Sylow* 2-子群和 *Sylow* 3-子群。
5. 设 p 是整除 n 的奇素数，给出 D_{2n} 的一个 *Sylow* p-子群，并证明 D_{2n} 的 *Sylow* p-子群都是循环群且是 D_{2n} 的正规子群。

练习 2.4.6. 设 $g_1,g_2,\ldots,g_r$ 是有限群 G 中所有共轭类的代表元，若它们两两可交换，证明 G 是交换群。

练习 2.4.7. 设 H 是 G 的一个子群，P 是 G 的一个 *Sylow* p-子群且包含在 H 中，证明 P 也是 H 的 *Sylow* p-子群。

练习 2.4.8. 设 p 是一个素数。

1. 构造 $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ 的一个 *Sylow* p-子群；
2. $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ 有多少 *Sylow* p-子群？
3. 计算 $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ 的所有共轭类。

练习 2.4.9. 设 H 是有限群 G 的真子群，证明 $G\neq\bigcup_{g\in G}gHg^{-1}$。举例说明该结论对无限群不成立。

练习 2.4.10. 设群 G 在集合 X 上的作用是可迁的，N 是 G 的一个正规子群。证明 X 在 N 作用下的每个轨道元素个数相同。

练习 2.4.11. 设群 G 在集合 X 上的作用是可迁的，$|X|>1$。证明存在 $g\in G$ 使得对任意 $x\in X$ 均有 $g(x)\neq x$。

练习 2.4.12. *1.* 设 G 是一个有限群。令 $x_1,\dots,x_h$ 为 G 的共轭类的代表元。令 $n_i=|\operatorname{Cent}_G(x_i)|$ 为 x_i 在 G 中中心化子的阶。证明 $1=\sum_{i=1}^{h}\frac{1}{n_i}$；

2. 证明对任意正整数 $h\geq 1$，只存在有限个互不同构的有限群使得其恰有 h 个共轭类；

3. 求所有恰有 3 个共轭类的有限群。

练习 2.4.13. 设 p 是一个素数，n,m 是两个正整数且 m 和 p 互素。设群 G 的阶为 p^nm。

1. 若 $m<p$，证明 G 不是单群。

2. 若 $m<p^2$，且 $n\geq 2$，证明 G 不是单群。

练习 2.4.14. 设 G 是一个有限群，H 是一个指数为 p 的子群，其中 p 是整除 $|G|$ 的最小素因子。证明 H 是正规子群。

练习 2.4.15. *1.* 证明 150 阶群不是单群。

2. 证明 6545 阶群不是单群。

3. 证明 105 阶群有一个正规的 *Sylow* 5-子群和正规的 *Sylow* 7-子群。

4. 证明 200 阶群一定有一个正规的 *Sylow* 5-子群。

练习 2.4.16. 设 p 是 $|G|$ 的最小素因子。若 G 含有一个 p-阶正规子群 H，证明 G 的中心包含 H。

练习 2.4.17. 设 P 是 G 的正规 *Sylow* p-子群，H 是 G 的子群，证明 $P\cap H$ 是 H 唯一的 *Sylow* p-子群。

练习 2.4.18. 设 P 是 G 的 *Sylow* p-子群，H 是 G 的正规子群，证明 $P\cap H$ 是 H 的 *Sylow* p-子群。

练习 2.4.19. 设 G 是非 *Abel* 的有限群，并且 G 的所有真子群都是 *Abel* 的，本题的目标是证明 G 不是单群。下面假设 G 是单群，记 $\mathcal{M}$ 为 G 的所有极大子群组成的集合。

1. 设 A,B 是 G 的两个真子群，证明 $N_G(A\cap B)$ 包含 A 和 B。

2. 证明对任意 $A,B\in\mathcal{M}$，若 $A\neq B$，则有 $A\cap B=\{1\}$。

3. 证明 $(g,A)\mapsto gAg^{-1}$ 是 G 在 $\mathcal{M}$ 上的一个作用。

4. 证明 $A\in\mathcal{M}$ 所在轨道的元素个数等于 $\frac{|G|}{|A|}$。

5. 对 $A\in\mathcal{M}$，我们记 $\mathcal{C}(A)=\bigcup_{g\in G}gAg^{-1}$。证明 $|\mathcal{C}(A)|=1+\frac{|G|}{|A|}(|A|-1)$。由此证明 $1+\frac{|G|}{2}\leq|\mathcal{C}(A)|<|G|$。

6. 对任意 $A,B\in\mathcal{M}$，若 B 不包含在 $\mathcal{C}(A)$ 中，证明 $\mathcal{C}(A)\cap\mathcal{C}(B)=\{1\}$。

7. 证明原结论。

练习 2.4.20. 设 n 是一个正整数。证明下面两个命题是等价的。(提示：利用上一题的结论)

(a) 所有的 n 阶群均是循环群；

(b) n 和欧拉函数 $\varphi(n)$ 互素。

2.5 对称群

这一节我们再深入讨论对称群的一些结论。首先我们讨论 S_n 的生成元。

定义 2.5.1. 我们称只有两个数字的轮换为**对换**。

命题 2.5.2. 所有的对换是 S_n 的一组生成元。

证明. 根据 S_n 中元素的轮换分解知我们只需证明任意一个轮换均可由对换生成即可。事实上，设 $(a_1\ a_2\ \dots\ a_m)$ 是一个 m-轮换，根据定义可直接验证

$$(a_1\ a_2\ \dots\ a_m) = (a_1\ a_m)\cdots(a_1\ a_3)(a_1\ a_2).$$

命题 2.5.3. $(1\ 2), (1\ 2\ \dots\ n)$ 是 S_n 的一组生成元。

证明. 我们记 $(1\ 2), (1\ 2\ \dots\ n)$ 生成的子群为 G。根据命题2.5.2可知，我们只需证明 G 包含所有对换即可。当 $1 \le i \le n-1$ 时，我们有

$$(1\ 2\ \dots\ n)^i(1\ 2)(1\ 2\ \dots\ n)^{-i} = (i+1\ i+2)$$

此时我们约定当 $i = n-1$ 时，等式右端出现的 $n+1$ 为 1。而由 $(2\ 3)(1\ 2)(2\ 3) = (1\ 3)$ 可知 $(1\ 3) \in G$。类似地，由 $(3\ 4)(1\ 3)(3\ 4) = (1\ 4)$ 可知 $(1\ 4) \in G$。依次递推可知对任意 $1 < i \le n$ 有 $(1\ i) \in G$。于是对任意 $2 \le i < j \le n$ 我们有 $(i\ j) = (1\ j)(1\ i)(1\ j) \in G$。故 G 包含所有对换。

接下来我们计算一下 S_n 的共轭类。

命题 2.5.4. S_n 中的两个元素是共轭的当且仅当它们的轮换分解的类型是相同的。

证明. 首先我们证明共轭的两个元素一定有相同的轮换分解类型。设 $\sigma \in S_n$ 的轮换分解为

$$(a_1\ a_2\ \dots\ a_{k_1})(a_{k_1+1}\ a_{k_1+2}\ \dots\ a_{k_1+k_2})\dots,$$

那么对任意 $\tau \in S_n$，我们考虑 $\tau\sigma\tau^{-1}$ 的轮换分解。我们注意到若 $\sigma(i) = j$，那么我们有 $\tau\sigma\tau^{-1}(\tau(i)) = \tau(j)$。因此当 i, j 出现在 σ 的轮换分解的同一个分解中时，$\tau(i), \tau(j)$ 也会出现在 $\tau\sigma\tau^{-1}$ 的轮换分解的同一个分解中。所以 $\tau\sigma\tau^{-1}$ 的轮换分解即为

$$(\tau(a_1)\ \tau(a_2)\ \dots\ \tau(a_{k_1}))(\tau(a_{k_1+1})\ \tau(a_{k_2+2})\ \dots\ \tau(b_{k_1+k_2}))\dots.$$

所以 σ 和 $\tau\sigma\tau^{-1}$ 具有相同的轮换分解类型。反之，若 σ_1,σ_2 具有相同的轮换分解类型，我们将其写成不交的轮换的乘积使得对应位置的轮换长度相等：

$$\sigma_1=(a_1\ a_2\ \dots\ a_{k_1})(a_{k_1+1}\ a_{k_1+2}\ \dots\ a_{k_1+k_2})\dots,\quad \sigma_2=(a_1'\ a_2'\ \dots\ a_{k_1}')(a_{k_1+1}'\ a_{k_1+2}'\ \dots\ a_{k_1+k_2}')\dots,$$

再取 τ 为将对应位置的数字 a_i 映射到 a_i'。根据定义可知 $\tau\in S_n$，再由前面的证明可知 $\tau\sigma_1\tau^{-1}=\sigma_2$。因此 σ_1 和 σ_2 共轭。

例 2.5.5. 设 $\sigma_1=(1)(2\ 5)(3\ 4\ 6\ 7),\sigma_2=(2)(3\ 6)(1\ 7\ 4\ 5)$。于是我们可以取

$$\tau=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&7&6&4&5\end{pmatrix},$$

则有 $\tau\sigma_1\tau^{-1}=\sigma_2$。注意到 τ 的选取并不是唯一的，例如我们取

$$\tau=\begin{pmatrix}1&2&3&4&5&6&7\\2&6&1&7&3&4&5\end{pmatrix},$$

同样也满足条件。

最后我们介绍 S_n 的一个非常重要的子群。给定 $\sigma\in S_n$，我们可以定义 σ 的符号为

$$\operatorname{sign}(\sigma)=\prod_{i<j}\frac{\sigma(j)-\sigma(i)}{j-i}.$$

容易看出 $\operatorname{sign}(\sigma)$ 取值只能是 ±1。并且我们有如下结论

命题 2.5.6. $\operatorname{sign}:S_n\to\mathbb{Z}/2\mathbb{Z}$ 是一个群同态，并且所有对换都取值为 -1。

证明. 设 $\sigma,\tau\in S_n$，我们注意到 $\sigma(1),\sigma(2),\dots,\sigma(n)$ 仍然是 $1,2,\dots,n$ 的一个排列，因此

$$\prod_{i<j}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}=\prod_{i<j}\frac{\tau(j)-\tau(i)}{j-i}=\operatorname{sign}(\tau).$$

所以我们有

$$\operatorname{sign}(\tau\sigma)=\prod_{i<j}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{j-i}=\prod_{i<j}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\cdot\prod_{i<j}\frac{\sigma(j)-\sigma(i)}{j-i}=\operatorname{sign}(\tau)\operatorname{sign}(\sigma).$$

故 sign 是一个群同态。若 σ 是一个对换，不妨设 $\sigma=(1\ 2)$，那么

$$\prod_{i<j}(\sigma(j)-\sigma(i))=(\sigma(2)-\sigma(1))\prod_{j\geq3}(\sigma(j)-\sigma(1))(\sigma(j)-\sigma(2))\prod_{3\leq i<j}(\sigma(j)-\sigma(i))=-\prod_{i<j}(j-i).$$

因此 $\operatorname{sign}(\sigma)=-1$。

我们将上述符号同态的核称为**交错群**，记作 A_n。由于符号同态是满射，因此根据群同构定理可知 A_n 是 S_n 中指数为 2 的正规子群。另一方面，我们可以看出若 $i<j$ 但 $\sigma(i)>\sigma(j)$，那么在 $\operatorname{sign}(\sigma)$ 的定义中便会贡献一个 -1，而这个条件等价于 $(\sigma(i),\sigma(j))$ 构成一个逆序，因此当 σ 的逆序数是奇数时，$\operatorname{sign}(\sigma)=-1$，此时我们称 σ 为**奇置换**；当 σ 的逆序数是偶数时，则 $\operatorname{sign}(\sigma)=1$，此时我们称 σ 为**偶置换**。

推论 2.5.7. *$\sigma \in A_n$ 当且仅当 σ 能分解成偶数个对换的乘积。特别地，m-轮换是偶置换当且仅当 m 是奇数。*

证明. 第一个结论是命题2.5.6的直接推论。至于第二个结论，只需注意到 m-轮换可分解为 $m-1$ 个对换的乘积即可。

由上述结论立刻可以得到所有 3-轮换是 A_n 的生成元。

推论 2.5.8. *所有的 3-轮换可生成 A_n。*

证明. 只需证明两个对换的乘积能被 3-轮换生成即可。设 $\sigma = (a\ b)(c\ d)$。若 $\{a,b\} = \{c,d\}$，则 σ 是单位元。若 $\{a,b\} \cap \{c,d\}$ 含有一个元素，不妨设 $a = c$，于是 $\sigma = (a\ d\ b)$ 即为一个 3-轮换。若 $\{a,b\}$ 和 $\{c,d\}$ 不交，那么我们有

$$\sigma = (a\ b)(a\ c)(a\ c)(c\ d) = (a\ c\ b)(a\ c\ d).$$

因此 σ 同样可由 3-轮换生成。

A_n 中的共轭类的计算则会复杂许多，我们证明如下部分结果，更详细的结论请参考习题2.5.9。

定理 2.5.9. *设 $\mathcal{C} \subseteq A_n$ 是 S_n 中的一个共轭类，那么 $\mathcal{C}$ 要么是 A_n 中的一个共轭类，要么是 A_n 中两个共轭类 $\mathcal{C}_1, \mathcal{C}_2$ 的并集。*

证明. 设 $\sigma \in \mathcal{C}$，并设 $\mathcal{C}_1$ 是 σ 在 A_n 中所在的共轭类，若 $\mathcal{C}_1 = \mathcal{C}$，则结论成立。若 $\mathcal{C}_1 \neq \mathcal{C}$，令 $\mathcal{C}_2 = \mathcal{C} \setminus \mathcal{C}_1$，我们下面证明 $\mathcal{C}_2$ 是 A_n 中的一个共轭类。事实上，对任意 $\tau_1, \tau_2 \in \mathcal{C}_2$，由于它们在 S_n 中均和 σ 共轭，因此存在 σ_1, σ_2 使得 $\tau_i = \sigma_i \sigma \sigma_i^{-1}, i = 1,2$。然而它们在 A_n 中不共轭，这表明 σ_i 必是奇置换，所以 $\sigma_1 \sigma_2^{-1} \in A_n$，因此 τ_1 和 τ_2 在 A_n 中共轭。

特别地，对于 3-轮换，我们有如下结论。

命题 2.5.10. *设 $n \geq 5$，则所有 3-轮换在 A_n 中均共轭。*

证明. 设 $\sigma = (1\ 2\ 3)$，对任意 3-轮换 τ，由命题2.5.4可知，存在 $\tau' \in S_n$ 使得 $\tau = \tau' \sigma \tau'^{-1}$。若 $\tau' \in A_n$ 则命题得证。否则若 τ' 是奇置换，那么 $\tau'(4\ 5)$ 一定是偶置换。因此我们有

$$(\tau'(4\ 5)\sigma(\tau'(4\ 5))^{-1} = \tau'(4\ 5)(1\ 2\ 3)(4\ 5)\tau'^{-1} = \tau'(1\ 2\ 3)\tau'^{-1} = \tau.$$

因此 σ 和 τ 仍然在 A_n 中共轭。

对称群在 Galois 理论中有着至关重要的作用。Galois 正是通过证明 A_n，$n \geq 5$ 是单群来得到五次以上的方程没有根式解的。若群 G 的正规子群只有 $\{1\}$ 和 G 自身，则称 G 为**单群**。上个世纪群论的一个里程碑式的结果便是解决了有限单群的分类问题，该结果散在在上百余篇文章中。

定理 2.5.11. *对任意 $n \geq 5$，A_n 是单群。*

证明. 设 $H \neq \{(1)\}$ 是 A_n 的一个正规子群，根据命题2.5.10及推论2.5.8可知，我们只需证明 H 包含一个 3-轮换即可。

我们先考虑 $n=5$ 的情况。设 $(1)\neq h\in H$，由于 h 是偶置换，根据轮换分解，我们知道 h 要么是一个 3-轮换，要么是一个 5-轮换，要么是两个对换的乘积。若 h 是一个 3-轮换，我们已经证明了所需的结论。若 h 是一个 5-轮换，不妨设 $h=(1\ 2\ 3\ 4\ 5)$，那么 H 包含如下元素

$$h\cdot((3\ 4\ 5)h^{-1}(3\ 4\ 5)^{-1})=(h(3)\ h(4)\ h(5))(3\ 4\ 5)^{-1}=(1\ 4\ 3).$$

若 h 是两个对换的乘积，不妨设 $h=(1\ 2)(3\ 4)$，同样地，H 包含如下元素

$$h\cdot((3\ 4\ 5)h^{-1}(3\ 4\ 5)^{-1})=(h(3)\ h(4)\ h(5))(3\ 4\ 5)^{-1}=(3\ 4\ 5).$$

这便证明了 H 必含有一个 3-轮换。

下面我们考虑一般的情况。由于 h 不是单位元，故取 a 使得 $h(a)\neq a$，令 $b=h(a)$，再取 $c\notin\{a,b,h(b)\}$。令 $\tau=(a\ b\ c)$ 及 $s=h\tau h^{-1}\tau^{-1}$，那么

$$h\cdot(\tau h^{-1}\tau^{-1})=(h\tau h^{-1})\cdot\tau^{-1}=(h(a)\ h(b)\ h(c))(a\ c\ b)\in H.$$

由此可知当 $c\neq h(c)$ 时，$s(a)=c$，而当 $c=h(c)$ 时，$s(a)=h(a)=b$。因此无论是哪种情况，我们都可以得到 $s\neq(1)$。而取 $\{1,2,\dots,n\}$ 的一个五元子集 X 且包含元素 $a,b,c,h(b),h(c)$。注意到这五个元素不一定全都不同，若它们互不相同，那么取 X 是这五个元素组成的集合即可，否则还需要添加其余元素。于是 s 可视作 X 上的一个偶置换。再记

$$G=\{\sigma\in A_n\mid\sigma(x)=x,\forall x\in\{1,2,\dots,n\}\setminus X\}.$$

容易看出 G 同构于 A_5。由于 H 是 A_n 的正规子群，因此 $H\cap G$ 是 G 的正规子群。由于 $(1)\neq s\in H\cap G$，因此根据 $n=5$ 的情况，我们知道 $H\cap G=G$，故 H 包含 3-轮换。

习题

练习 2.5.1. 证明 3-轮换 $\{(i\ i+1\ i+2)\mid 1\leq i\leq n-2\}$ 可生成 A_n。

练习 2.5.2. 证明 $D(S_3)=A_3$，$D(G)$ 的定义见*2.3.23*。更一般地，计算 $D(S_n)$。

注 4. Ore 在这篇文章[1]中证明了 A_n 中的任何元素都是 S_n 中某两个元素的换位子，并且当 $n\geq 5$ 时，A_n 中的任何元素都是 A_n 中某两个元素的换位子。

练习 2.5.3. 证明 n-轮换 $(1\ 2\ \dots\ n)$ 和对换 $(i\ j)$ 可生成 S_n 当且仅当 $i-j$ 和 n 互素。

练习 2.5.4. *1.* 分别计算 $(1\ 2),(1\ 2\ 3),(1\ 2)(3\ 4)$ 在 S_4 中的中心化子。

2. 证明 $|C_{S_n}((1\ 2)(3\ 4))|=8\cdot(n-4)!$，并计算 $(1\ 2)(3\ 4)$ 在 S_n 中的中心化子。

3. 设 $\sigma=(1\ 2\ \dots\ k)$，记 $H=\{\tau\in S_n\mid\tau(m)=m,\ \forall m\leq k\}$。证明 $C_{S_n}(\sigma)\simeq\langle\sigma\rangle\times H$。

练习 2.5.5. 设 $k\geq 1$ 是一个正整数，群 G 在集合 X 上有一个作用且 $|X|\geq k$。若对任意 X 中元素组成的有序 k-元组 $(x_1,\dots,x_k),(y_1,\dots,y_k)$，其中 $x_1,\dots,x_k$ 两两不同，$y_1,\dots,y_k$ 也两两不同，均存在 $g\in G$ 使得对任意 $i=1,\dots,k$ 有 $gx_i=y_i$，那么我们称 G 在 X 上的作用是**k-可迁的**。

[1] O. Ore, Some remarks on commutators, Proc. A. M. S. Vol. 2, 307–314 (1951).

1. 证明 S_n 在 $\{1,2,\dots,n\}$ 上的作用是 n-可迁的。
2. 设 G 是 S_n 的一个子群，且包含一个对换。证明 $G=S_n$ 当且仅当 G 在 $\{1,2,\dots,n\}$ 上的作用是 2-可迁的。
3. 设 V 是 $\mathbb{R}$ 上的线性空间且维数大于 1。证明 $\mathrm{GL}(V)$ 在 $\mathbb{P}(V)$ 上的作用是 2-可迁的。

练习 2.5.6. 设 $n\geq 2$ 是一个正整数。

1. 证明存在唯一的非平凡同态：$S_n\to\{\pm 1\}$。
2. 证明不存在非平凡同态 $A_n\to\{\pm 1\}$。

练习 2.5.7. 设 p 是一个素数，$p\leq n\leq p^2-1$ 是一个正整数。

1. 找出 S_n 的一个 *Sylow* p-子群。

   下面我们构造 S_{p^2} 的 *Sylow* p-子群。我们记 $G=\langle\sigma_0,\dots,\sigma_p\rangle, H=\langle\sigma_0,\dots,\sigma_{p-1}\rangle$，其中当 $0\leq i\leq p-1$ 时，$\sigma_i=(pi+1\ pi+2\ pi+3\ \dots\ pi+p)$，

   $$\sigma_p=(1\ p+1\ \dots\ 1+(p-1)p)(2\ p+2\ \dots\ 2+(p-1)p)\cdots(p\ 2p\ \dots\ p^2).$$

2. 证明 H 同构于 $(\mathbb{Z}/p\mathbb{Z})^p$。
3. 证明 H 是 G 的正规子群。
4. 证明 $[G:H]=p$。
5. 证明 G 是 S_{p^2} 的 *Sylow* p-子群。

练习 2.5.8. 证明 S_n 的所有指数是 n 的子群均同构于 S_{n-1}。

练习 2.5.9. 设 $\sigma\in A_n$，若存在 $\tau\in S_n\setminus A_n$ 使得 $\tau\sigma=\sigma\tau$，那么我们称 σ 是不特殊的，否则称 σ 是特殊的。

1. 证明 σ 是不特殊的当且仅当 σ 的轮换分解类型中有一个偶数或者有两个相同的奇数。
2. 若 σ 是不特殊的，证明 σ 在 S_n 中的共轭类和 σ 在 A_n 中的共轭类相同。
3. 若 σ 是特殊的，$s\in S_n\setminus A_n$。证明 σ 在 A_n 中的共轭类和 $s\sigma s^{-1}$ 在 A_n 中的共轭类不交，并且它们的并集恰好为 σ 在 S_n 中的共轭类。
4. 计算 A_4, A_5 的所有共轭类。

练习 2.5.10. 设 G 是一个有限群，$\pi: G\to S_G$ 是左正则表示。

1. 设 $g\in G$ 的阶为 n，$|G|=mn$。证明 $\pi(g)$ 是 m 个 n-轮换的乘积。
2. $\pi(g)$ 是一个奇置换当且仅当 $|g|$ 是偶数且 $|G|/|g|$ 是奇数。
3. 若 $\pi(G)$ 包含一个奇置换，证明 G 有一个指数为 2 的子群。

4. 设 $|G| = 2k$，其中 k 是一个奇数，证明 G 有一个指数为 2 的子群。

练习 2.5.11. 本题的目标是证明当 $n \neq 6$ 时，$\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$。设 $n \neq 6$ 是一个整数。

(1) 设 $\sigma \in \mathrm{Aut}(G)$，$\mathcal{C}$ 是 G 的一个共轭类，证明 $\sigma(\mathcal{C})$ 也是 G 的一个共轭类；
(2) 设 $\mathcal{C}$ 是 S_n 中由对换组成的共轭类，$\mathcal{C}'$ 是 S_n 的另一个共轭类，并且 $\mathcal{C}'$ 包含一个阶为 2 的非对换元素。证明 $|\mathcal{C}| \neq |\mathcal{C}'|$；
(3) 设 $\sigma \in \mathrm{Aut}(S_n)$，证明存在互不相同的整数 $a, b_2, b_3 \ldots, b_n$ 使得 $\sigma((1\ k)) = (a\ b_k), k = 2, \ldots, n$；
(4) 证明 S_n 可由 $(1\ 2), (1\ 3), \ldots, (1\ n)$ 生成。由此证明 $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$。

练习 2.5.12. 本题的目标是研究 S_6 的自同构群。

1. 证明例2.4.5诱导的映射 $\psi : S_5 \to S_X \simeq S_6$ 是单射。

2. 证明上述映射保持置换的奇偶性，即将奇置换映为奇置换，偶置换映为偶置换。

3. 记 H 为 ψ 的像，并记 Y 为 H 在 S_6 中的左陪集组成的集合，易知 $|Y| = 6$。S_6 在 Y 上的左乘作用给出了群同态 $F : S_6 \to S_6$。证明 F 是单射，从而证明 F 是同构。

4. 通过计算 $F(1\ 2)$ 不是对换证明 F 不是内自同构。

5. 证明 $\mathrm{Aut}(S_6) \simeq \mathrm{Inn}(S_6) \rtimes \langle F \rangle$。(提示：考虑 S_6 中的对换个数以及形如 $(1\ 2)(3\ 4)(5\ 6)$ 的置换个数)

2.6 有限生成的 Abel 群

这一节我们讨论有限生成的交换群的结构问题。我们回忆一下有限生成的群的定义：如果群 G 存在一个有限子集 A 使得 $G = \langle A \rangle$，则称 G 是有限生成的。

例 2.6.1. 1. 循环群都是有限生成的。

2. 有限群都是有限生成的。

3. 更一般地，设 r 是一个正整数，则群 $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ 是有限生成的。我们称之为秩为 r 的**自由 *Abel* 群**。

从上述例子可以看出有限生成的 Abel 群有两类，一类是元素是有限阶的，一类是有无限阶元素的。我们把 G 中所有有限阶元素组成的集合称之为 G 的**挠子群**，记作 G_{tor}。若 G 除了单位元以为没有有限阶的元素，那么我们称 G 为**无挠群**。容易看出 G/G_{tor} 是无挠群。下面我们先考虑挠子群部分。

定理 2.6.2. 设 G 是有限 *Abel* 群，那么存在唯一的一列整数 $n_1, n_2, \ldots, n_s$ 使得

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z},$$

且满足如下条件：

1. $n_i \geq 2$；

2. 对任意 $1 \leq i \leq s-1$ 均有 $n_{i+1} \mid n_i$。

引理 2.6.3. 设 H,K 是 *Abel* 群 G 的两个子群，且 $H\cap K=\{0\}$，那么 $H+K\simeq H\times K$。特别地，若 $|G|=|H||K|$，那么 $G\simeq H\times K$。

证明. 考虑如下映射：

$$H\times K\to G,\qquad (h,k)\mapsto h+k.$$

容易验证该映射是群同态。若 $h+k=0$，那么 $h=-k\in H\cap K$，故只能有 $h=k=0$，因此该映射是单射。根据定义知该映射的像集是 $H+K$，因此有 $H\times K\simeq H+K$。

注 5. 该结论对非 Abel 群也成立，只需假设 H,K 是 G 的正规子群即可。

推论 2.6.4. 设 $n\geq 2$ 是一个正整数，$n=p_1^{k_1}\cdots p_s^{k_s}$ 是 n 的素因数分解。那么我们有如下群同构

$$\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}/p_1^{k_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_s^{k_s}\mathbb{Z}.$$

推论 2.6.5. 设 G 是一个 *Abel* 群，$f:G\to\mathbb{Z}$ 是一个群同态，那么 $G\simeq\operatorname{Im}f\times\ker f$。

证明. 由于 $\mathbb{Z}$ 的子群均形如 $m\mathbb{Z}$，其中 $m\in\mathbb{Z}$，故不妨设 $g\in G$ 使得 $f(g)=m$。当 $m=0$ 时，由于 $\ker f=G$，结论显然成立。当 $m\neq 0$ 时，我们有 $\langle g\rangle\cap\ker f=\{0\}$。下面我们证明 $G=\langle g\rangle+\ker f$。事实上，对任意 $h\in G$，假设 $f(h)=nm$，那么 $h-ng\in\ker f$。因此由引理2.6.3知 $G\simeq\operatorname{Im}f\times\ker f$。

引理 2.6.6. 设 G 是有限 *Abel* 群，$g\in G$ 是 G 中阶最大的元素，其阶为 d。令 $H=\langle g\rangle$，那么对任意 $\bar{h}\in G/H$，存在元素 $h\in G$ 使得 h 和 $\bar{h}$ 的阶相同。

证明. 设 $\bar{h}$ 的阶为 d_1，$h_0\in G$ 是 h 的任意一个原像，其阶为 d_0。由于 $d_0h_0=0\in H$，而 $\bar{h}$ 的阶为 d_1，因此由命题2.2.10可知 $d_1\mid d_0$，不妨设 $d_0=d_1d_1'$。由于 $d_1h_0\in H$，故存在 $k\in\mathbb{Z}$ 使得 $d_1h_0=kg$。故 $d_1d_1'h_0=d_0h=0=kd_1'g$，故再次利用命题2.2.10有 $d\mid kd_1'$。根据命题2.2.13知 $d_0\mid d$。综上有 $d_1\mid k$，设 $k=d_1\ell$，并取 $h=h_0-\ell g$，那么我们有 $d_1h=d_1h_0-d_1\ell g=d_1h_0-kg=0$。由于 $h_0-\ell g$ 仍然是 h 的原像，故其阶不小于 d_1，因此 $h_0-\ell g$ 的阶恰好为 d_1。

定理2.6.2的证明. 我们对 G 的阶数进行归纳。当 $|G|=1,2$ 时，结论显然成立。考虑 $|G|>2$，设 $g_1\in G$ 是 G 中阶最大的元素，其阶为 d_1。于是 $G/\langle g_1\rangle$ 的阶严格小于 G 的阶，因此根据归纳假设可知，存在 $\bar{g}_2,\ldots,\bar{g}_s$ 使得 $G/\langle g_1\rangle\simeq\langle\bar{g}_2\rangle\times\cdots\times\langle\bar{g}_s\rangle$，其中 $\bar{g}_i$ 的阶为 d_i，并且满足 $d_{i+1}\mid d_i$。根据引理2.6.6可知存在元素 $g_i\in G$ 使得 g_i 在 $G/\langle g_1\rangle$ 中的像为 $\bar{g}_i$ 并且 g_i 的阶为 d_i。下面证明

$$\langle g_1\rangle\times\langle g_2\rangle\times\cdots\times\langle g_s\rangle\to G,\qquad (k_1g_1,k_2g_2,\ldots,k_sg_s)\mapsto k_1g_1+k_2g_2+\cdots+k_sg_s$$

是同构。由于 G 是 Abel 群，所以该映射显然是同态。若 $k_1g_1+k_2g_2+\cdots+k_sg_s=0$，那么在 $G/\langle g_1\rangle$ 中有 $(k_2\bar{g}_2,\ldots,k_s\bar{g}_s)=\bar{0}$。但是由于 $G/\langle g_1\rangle\simeq\langle\bar{g}_2\rangle\times\cdots\times\langle\bar{g}_s\rangle$，故必有 $k_2=\cdots=k_s=0$，从而在 G 中有 $k_1g_1=0$，因此 $k_1=0$。所以上述映射是单射，但是等式两边的集合元素个数相等，因此上述映射是同构。

下面我们证明唯一性。设另一列整数 $\delta_1,\ldots,\delta_s$ 也满足定理2.6.2的条件。对任意 $m\in\mathbb{N}$，若 $g\in G$ 的阶为 d，那么根据命题2.2.11 可知 mg 的阶为 $\frac{d}{(m,d)}$。因此 mG 的阶为

$$\prod_{i=1}^{r}\frac{d_i}{(m,d_i)}=\prod_{j=1}^{s}\frac{\delta_j}{(m,\delta_j)}.$$

由于 $|G| = d_1d_2\cdots d_r = \delta_1\delta_2\cdots\delta_s$。由此可知 $\prod_{i=1}^{r}(m,d_i) = \prod_{j=1}^{s}(m,\delta_j)$。特别地，我们取 $m = d_1$，于是

$$\delta_1\delta_2\cdots\delta_s = d_1d_2\cdots d_r = \prod_{i=1}^{r}(d_1,d_i) = \prod_{j=1}^{s}(d_1,\delta_j).$$

由此可知对任意 j 均有 $\delta_j = (m,\delta_j)$。故 $\delta_1 \mid d_1$。由对称性同样可知 $d_1 \mid \delta_1$。故 $d_1 = \delta_1$。由递推便可知 $d_i = \delta_i$。

给定一个正整数 n，利用上述定理我们可以列出所有阶为 n 的有限 Abel 群。因为我们只需要找出所有满足如下条件的有限序列 $n_1, n_2, \ldots, n_s$ 即可。

1. $n_i \geq 2$;
2. $n_{i+1} \mid n_i$;
3. $n_1n_2\cdots n_s = n$。

容易看出所有的 n_i 均为 n 的因子，而 $n_2, \ldots, n_s$ 均为 n_1 的因子。因此若 p 是 n 的一个素因子，那么 p 一定整除 n_1。这意味着如果 p 在 n 中的重数是 1 的话，那么 p 恰好只能整除 n_1，而与 $n_2, \ldots, n_s$ 均互素。下面我们通过例子来给出具体的算法。

例 2.6.7. 假设 $n = 180 = 2^2 \times 3^2 \times 5$。根据上面的分析可知 $2\times3\times5 \mid n_1$，因此 n_1 共有如下四种可能

$$n_1 = 2\times3\times5, \quad 2^2\times3\times5, \quad 2\times3^2\times5, \quad 2^2\times3^2\times5.$$

对于这四种情况，我们需要分别求出 n_2 的可能值，和上面的分析相同，我们可以知道 $\frac{n}{n_1}$ 的素因子一定要整除 n_2，因此前三种情况对应的 n_2 都是唯一的，分别为 $2\times3, 3, 2$，而最后一种情况则不存在 n_2，因为此时已经有 $n_1 = n$。最后我们可以得到 180 阶的 *Abel* 群一定同构于如下四个群之一：

$$\mathbb{Z}/30\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}, \qquad \mathbb{Z}/60\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}, \qquad \mathbb{Z}/90\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}, \qquad \mathbb{Z}/180\mathbb{Z}.$$

设 G 是阶为 n 的有限 Abel 群，其中 $n = p_1^{\ell_1}p_2^{\ell_2}\cdots p_k^{\ell_k}$。根据上面的例子我们可以总结出如下的计算所有互不同构的 Abel 群的方法。

1. 列出所有可能的 n_1，即为 $n_1 = p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}$，其中 $t_i \geq 1$。
2. 列出所有可能的 n_2，此时 n_2 需要满足：(i)，n/n_1 的所有素因子均整除 n_2；(ii)，n_2 整除 n_1。
3. 依次列出所有可能的 n_i 直至 $n = n_1\cdots n_i$，其中 n_i 需要满足：(i)，$n/(n_1\cdots n_{i-1})$ 的所有素因子均整除 n_i；(ii)，n_i 整除 n_{i-1}。

利用推论2.6.4我们可以得到有限 Abel 群的另一种分解：

$$G \simeq \left(\mathbb{Z}/p_1^{k_{11}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_1^{k_{1\ell_1}}\mathbb{Z}\right)\times\cdots\times\left(\mathbb{Z}/p_s^{k_{s1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_s^{k_{s\ell_s}}\mathbb{Z}\right),$$

其中 $k_{i1} \geq k_{i2} \geq \cdots \geq k_{i\ell_i} \geq 1$。这个分解的意义是把 G 中所有阶为 p_i 的幂次的元素放到一起，从这个分解我们容易看出 G 的 Sylow p_i-子群同构于 $\mathbb{Z}/p_i^{k_{i1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_i^{k_{i\ell_i}}\mathbb{Z}$。

我们下面讨论自由 Abel 群。事实上，自由 Abel 群的概念和线性空间的概念是非常类似的，只是把域换成了整数环，一些线性空间中的结论对自由 Abel 群也成立。

定义 2.6.8. 设 G 是一个 Abel 群，$y_1, y_2, \ldots, y_s \in G$，若映射

$$\mathbb{Z}^s \to G, \qquad (n_1, n_2, \ldots, n_s) \mapsto n_1 y_1 + n_2 y_2 + \cdots + n_s y_s,$$

是单射，那么我们称 $y_1, y_2, \ldots, y_s$ 是**自由的**。若该映射是双射，则称 $y_1, y_2, \ldots, y_s$ 是一组基。若 G 有一组 s 个元素组成的基，则称 G 是**秩 r 的自由 Abel 群**。

注 6. 自由 Abel 群的秩是定义良好的，即若 $\mathbb{Z}^n \simeq \mathbb{Z}^m$，则必有 $n = m$。事实上，我们有

$$(\mathbb{Z}/2\mathbb{Z})^n \simeq \mathbb{Z}^n/2\mathbb{Z}^n \simeq \mathbb{Z}^m/2\mathbb{Z}^m \simeq (\mathbb{Z}/2\mathbb{Z})^m.$$

对比两边元素个数即有 $n = m$。

引理 2.6.9. *秩 r 的自由 Abel 群的子群均是自由 Abel 群，且秩不超过 r。*

证明. 当 $r = 0$ 时，结论显然成立；当 $r = 1$ 时，由于 $\mathbb{Z}$ 的子群均形如 $m\mathbb{Z}$，它仍然是自由 Abel 群，并且当 $m = 0$ 时，秩为 0，当 $m \neq 0$ 时，秩为 1。下面我们假设 $r > 1$。设 H 是 $\mathbb{Z}^r$ 的一个非平凡子群。考虑如下投影同态：

$$\pi : \mathbb{Z}^r \to \mathbb{Z}, \qquad (x_1, x_2, \ldots, x_r) \mapsto x_r.$$

显然 $\pi(H)$ 是 $\mathbb{Z}$ 的一个子群。因此存在整数 n_r 使得 $\pi(H) = n_r\mathbb{Z}$，取 $h_r \in H$ 使得 $\pi(h_r) = n_r$。另一方面显然有 $\ker\pi \simeq \mathbb{Z}^{r-1}$。因此 $K = H \cap \ker\pi$ 可视作 $\mathbb{Z}^{r-1}$ 的子群，故根据归纳假设可知 K 是自由 Abel 群，其秩小于等于 $r-1$。由推论2.6.5可知 $H = K \times \mathbb{Z}h_r$ 是自由 Abel 群，其秩小于等于 r。

引理 2.6.10. *设 G 是有限生成的无挠群，那么 G 是有限秩的自由 Abel 群，即存在正整数 r 使得 $G \simeq \mathbb{Z}^r$。*

证明. 设 $x_1, \ldots, x_r$ 是一组生成元，$y_1, \ldots, y_s$ 是 G 中自由的元素数量最多的一组，记 $H = \langle y_1, \ldots, y_s\rangle$。那么对任意 i，$x_i, y_1, \ldots, y_s$ 都不是自由的，故存在 $n_i > 0$ 使得 $n_i x_i \in H$。记 $n = n_1 \cdots n_r$，于是根据定义 nG 是 H 的子群。由于 H 是秩为 s 的自由 Abel 群，故由引理2.6.9知而 nG 也是自由 Abel 群，另一方面由于 $nG \simeq G$，故 G 是自由 Abel 群。

最后我们可以证明如下有限生成 Abel 群的基本定理。

定理 2.6.11. *设 G 是有限生成的 Abel 群，那么存在整数 $r, n_1, n_2, \ldots, n_s$ 使得*

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z},$$

且满足如下条件：

1. *$r \geq 0$ 且 $n_i \geq 2$；*
2. *对任意 $1 \leq i \leq s-1$ 均有 $n_{i+1} \mid n_i$。*

*并且满足上述条件的整数 $r, n_1, n_2, \ldots, n_s$ 是唯一的。其中 r 被称为群 G 的**秩**，$n_1, n_2, \ldots, n_s$ 被称为群 G 的**不变因子**。*

证明. 由于 G/G_{tor} 是无挠的，故由引理 2.6.10 可知 G/G_{tor} 是自由 Abel 群，不妨设 $x_1, \ldots, x_r \in G$ 使得 $G/G_{\text{tor}} \simeq \mathbb{Z}\bar{x_1} \times \cdots \times \mathbb{Z}\bar{x_r}$。设 $H = \langle x_1, \ldots, x_r\rangle$，容易看出 $H \cap G_{\text{tor}} = \{0\}$ 并且 $G = H + G_{\text{tor}}$。因此根据引理2.6.3可知 $G \simeq H \times G_{\text{tor}} \simeq \mathbb{Z}^r \times G_{\text{tor}}$。最后结合定理2.6.2即可完成证明。

习题

练习 2.6.1. 证明群 $\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/90\mathbb{Z}\times\mathbb{Z}/25\mathbb{Z}$ 和群 $\mathbb{Z}/100\mathbb{Z}\times\mathbb{Z}/30\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$ 是同构的。

练习 2.6.2. 在同构意义下写出所有阶为 2025 的 *Abel* 群及其不变因子。

练习 2.6.3. 在同构意义下找出所有的 *Abel* 群 G 使得存在子群 H 满足 $H\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\simeq G/H$。

练习 2.6.4. 证明任意一个非循环的交换群 G 都存在一个子群 H 及素数 p 使得 $H\simeq\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$。

练习 2.6.5. 设 $n\geq 1$ 是一个正整数，构造 $\mathbb{R}$ 的一个子群同构于 $\mathbb{Z}^n$。

练习 2.6.6. 设 $(a,b),(c,d)\in\mathbb{Z}^2$ 并且 $ad-bc\neq 0$。设 G 为由 $(a,b),(c,d)$ 生成的 $\mathbb{Z}^2$ 的子群，证明 $|\mathbb{Z}^2/G|=|ad-bc|$。

练习 2.6.7. 1. 设 $u_1=(2,1),u_2=(1,2)\in\mathbb{Z}^2$，记 M 为 $\mathbb{Z}^2$ 中由 u_1,u_2 生成的子群，计算 $\mathbb{Z}^2/M$。

2. 设 $u_1=(2,1,1),u_2=(1,2,1),u_3=(1,1,2)\in\mathbb{Z}^3$，记 M 为 $\mathbb{Z}^3$ 中由 u_1,u_2,u_3 生成的子群，计算 $\mathbb{Z}^3/M$。

练习 2.6.8. 设 G 是有限 *Abel* 群，证明对于 $|G|$ 的任何因子 d，均存在 G 的子群 H 使得 $|H|=d$。

练习 2.6.9. 设 G 是有限群，且对任意 $g\in G$ 均有 $g^2=1$。证明 G 是 *Abel* 群，并证明存在整数 n 使得 $G\simeq(\mathbb{Z}/2\mathbb{Z})^n$。

练习 2.6.10. 设 p 是一个素数。

1. 若 $p\geq n$，证明对任意 $g\in U_n(\mathbb{Z}/p\mathbb{Z})$ 均有 $g^p=1$，其中 U_n 的定义见2.1.4节。

2. 证明对任意 $p\geq 3$，存在阶为 p^3 的非交换群 G 使得对任意 $g\in G$ 均有 $g^p=1$。

练习 2.6.11. 设 $G=\prod_p\mathbb{Z}/p\mathbb{Z}$，其中乘积遍历所有的素数 p，求 G_{tor}。

练习 2.6.12. 设 $G\subseteq\mathbb{Q}$ 为由 $1/p$ 生成的子群，其中 p 遍历所有的素数。

1. 证明 $G=\{\frac{m}{n}\mid m\in\mathbb{Z},n\in\mathbb{N}_{>0},n\text{ 没有平方因子}\}$。

2. 证明 $G\to G$ 的所有群同态均形如 $x\mapsto kx$，其中 k 是一个整数。

3. 证明 $\mathrm{Aut}(G)\simeq\mathbb{Z}/2\mathbb{Z}$。

练习 2.6.13. 证明 $\mathrm{GL}_n(\mathbb{Q})$ 的有限子群都共轭于 $\mathrm{GL}_n(\mathbb{Z})$ 的子群。(提示：考虑 $\sum_{g\in G}g\cdot\mathbb{Z}^n$。)

练习 2.6.14. 设 G 是一个 *Abel* 群，n 是一个正整数，记 $S(G,n)$ 为 G 中所有指数为 n 的子群组成的集合。

1. 设 $H\in S(G,n)$，证明 $nG\subseteq H$。

2. 证明 $S(G,n)$ 和 $S(G/nG,n)$ 之间存在一个双射。

3. 设 m,N 是两个正整数且 m,n 互素。证明 $S((\mathbb{Z}/mn)^N,mn)$ 和 $S((\mathbb{Z}/m\mathbb{Z})^N,m)\times S((\mathbb{Z}/n\mathbb{Z})^N,n)$ 之间存在一个双射。

4. 证明 $S(\mathbb{Z}^2,2)$ 中恰好有三个元素，并写出这三个元素。

5. 证明 $|S(\mathbb{Z}^2,m)|=\sum_{d|m}d$。(提示：对 m 的每个因子 d，考虑满足 $H\cap(\mathbb{Z}\times 0)=d\mathbb{Z}\times 0\subseteq\mathbb{Z}^2$ 的子群 $H\in S(\mathbb{Z}^2,n)$ 的个数。) 并计算生成级数 $\sum_{r\geq 0}|S(\mathbb{Z}^2,p^r)|T^r$ 及 $\sum_{n\geq 1}|S(\mathbb{Z}^2,n)|n^s$。

练习 2.6.15. 设 G 是一个 *Abel* 群，我们称同态 $G\to\mathbb{C}^*$ 为 G 的**特征**。我们记 G 上所有特征组成的集合为 $\widehat{G}$。在 $\widehat{G}$ 可以定义如下运算：对任意 $\chi,\psi\in\widehat{G}$，$(\chi\psi)(g):=\chi(g)\psi(g)$。

1. 证明在上述运算下 $\widehat{G}$ 构成一个 *Abel* 群，我们称之为群 G 的**特征群**或**对偶群**。

2. 证明 $\widehat{\mathbb{Z}/n\mathbb{Z}}\simeq\mathbb{Z}/n\mathbb{Z}$。

3. 设 G_1,G_2 是两个 *Abel* 群，证明 $\widehat{G_1\times G_2}\simeq\widehat{G_1}\times\widehat{G_2}$。

4. 设 G 是有限 *Abel* 群，证明 $\widehat{G}\simeq G$。

5. 证明下列映射是一个同构：
$$\begin{array}{rccc}\iota_G:& G & \longrightarrow & \widehat{\widehat{G}}\\ & g & \longmapsto & (\chi\mapsto\chi(g)).\end{array}$$

练习 2.6.16 (有限 Fourier 分析)**.** 设 G 是一个有限 *Abel* 群，记 $L^2(G)$ 为所有 G 到 $\mathbb{C}$ 的函数组成的 $\mathbb{C}$-线性空间。我们在 $L^2(G)$ 上定义如下 *Hermitian* 内积：$\langle f,f'\rangle=\frac{1}{|G|}\sum_{g\in G}f(g)\overline{f'(g)}$。

1. 证明 $L^2(G)$ 作为复线性空间的维数等于 $|G|$。

2. 证明 $\widehat{G}$ 构成 $L^2(G)$ 的一组正交基。

3. 对任意 $f\in L^2(G)$，证明 $f=\sum_{\chi\in\widehat{G}}\langle f,\chi\rangle\chi$。

练习 2.6.17. 设 p 是一个素数，我们考虑 $\prod_{n\geq 1}\mathbb{Z}/p^n\mathbb{Z}$ 的子集：
$$\mathbb{Z}_p:=\{(x_n)\in\prod_{n\geq 1}\mathbb{Z}/p^n\mathbb{Z}\mid x_{n+1}\equiv x_n\pmod{p^n}\quad\forall n\geq 1\}.$$
我们称之为p**-进整数**。

1. 证明 $\mathbb{Z}_p$ 是 $\prod_{n\geq 1}\mathbb{Z}/p^n\mathbb{Z}$ 的子群，并且对任意正整数 n，映射 $\mathbb{Z}_p\to\mathbb{Z}/p^n\mathbb{Z}$，$(x_n)\mapsto x_n$ 是满同态。

2. 证明 $\mathbb{Z}_p$ 没有非平凡的有限阶元素。

3. 记 μ_{p^∞} 为练习2.2.20中的 *Prüfer* 群。证明对任意 $\chi\in\widehat{\mu_{p^\infty}}$，均存在唯一的元素 $(x_n)\in\mathbb{Z}_p$ 使得对任意 $n\geq 1$ 有 $\chi(e^{2\pi i/p^n})=e^{2\pi i x_n/p^n}$。

4. 证明 $\widehat{\mu_{p^\infty}}\simeq\mathbb{Z}_p$。

练习 2.6.18 (Cohen-Lenstra 密度问题)**.** 设 p 是素数

1. 设 $n_1\leq\cdots\leq n_r$ 是一列正整数。计算 $\mathrm{Aut}(\mathbb{Z}/p^{n_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p^{n_r}\mathbb{Z})$ 的阶。

2. 记 $(p)_r = \prod_{i=1}^{r}(1-p^{-i})$。证明

$$\sum_{\substack{G \text{ 是 } Abel\ p\text{-群} \\ |G|\le p^r}} \frac{1}{|\operatorname{Aut}(G)|} = \frac{1}{(p)_r}.$$

由此证明

$$\sum_{G \text{ 是 } Abel\ p\text{-群}} \frac{1}{|\operatorname{Aut}(G)|} = \frac{1}{(p)_\infty}.$$

第三章　环

3.1　环的概念及例子

3.1.1　环的概念

定义 3.1.1. 设 R 是一个具有两种二元运算 “$+$” 和 “$\cdot$”（分别称为加法和乘法）的非空集合. 若它满足如下三条性质

1. R 关于加法运算构成一个交换群。
2. R 关于乘法满足结合律，也就是说对任意 $a,b,c\in R$ 均有 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$。
3. R 满足乘法对加法的分配律，也就是说对任意 $a,b,c\in R$，我们有

$$(a+b)\cdot c=a\cdot c+b\cdot c,\qquad c\cdot(a+b)=c\cdot a+c\cdot b.$$

我们则称 R 为一个**环**。若 R 有乘法单位元，则称 R 为**含幺环**。若 R 关于乘法运算是交换的，那么称 R 是**交换环**。若环 R 的非零元关于乘法运算均有逆元，则称 R 为**除环**。若 R 是交换除环，那么称 R 为**域**。

例 3.1.2. *1.* 整数集 $\mathbb{Z}$ 关于通常意义下的加法和乘法构成一个环。

2. 集合

$$\mathbb{Z}[\mathrm{i}]:=\{m+n\mathrm{i}\mid m,n\in\mathbb{Z}\}$$

关于通常意义下的加法和乘法构成一个环。该环被称之为**高斯整数环**。

3. 我们熟知的有理数集，实数集，复数集在通常的加法与乘法下均构成一个域。设 p 是一个素数，那么根据初等数论中的 *Bézout* 定理可知 $\mathbb{Z}/p\mathbb{Z}$ 中的非零元均是可逆的，因此 $\mathbb{Z}/p\mathbb{Z}$ 也是一个域，它被称之为**有限域**。更多关于域的内容将在下一章介绍。

定义 3.1.3. 设 a 是环 R 中的非零元素，若存在非零元素 $b\in R$ 使得 $ab=0$ 或 $ba=0$，那么我们称 a 为**零因子**。若 R 没有零因子，我们则称 R 为**整环**。假设 R 含有乘法单位元，设 $u\in R$，若存在 $v\in R$ 使得 $uv=vu=1$，那么我们称 u 为 R 中的**单位**。我们记 R 中所有单位组成的集合为 R^*。

注意到 R 中的零因子一定不是单位。下面我们给出一些例子。

例 3.1.4. *1.* 设 $R=M_n(\mathbb{C})$ 为矩阵环。那么根据线性代数的知识可知它里面的零因子即为所有秩小于 n 大于 0 的矩阵，而单位则为所有可逆矩阵。

2. 设 $R=\mathbb{Z}/m\mathbb{Z}$，其中 m 是一个正整数，那么 $\bar{0}\neq\bar{a}\in R$ 是零因子当且仅当 $(a,m)>1$，而 $\bar{a}\in R$ 是单位当且仅当 $(a,m)=1$。

在给出更多的例子之前，我们先介绍一些环的基本性质。

命题 3.1.5. 设 R 是一个环。

1. 对任意 $a\in R$ 均有 $0\cdot a=a\cdot 0=0$；
2. 对任意 $a,b\in R$ 均有 $(-a)\cdot b=a\cdot(-b)=-(ab)$，其中 $-a$ 是 a 的加法逆元；
3. 对任意 $a,b\in R$ 均有 $(-a)\cdot(-b)=ab$；
4. 若 R 有单位 1，那么单位是唯一的，并且对任意 $a\in R$，均有 $-a=(-1)\cdot a$。

证明. 我们仅对第一条进行证明，其余的证明均是类似的。因为 $0\cdot a=(0+0)\cdot a=0\cdot a+0\cdot a$，由于加法构成一个群，故两边加上 $0\cdot a$ 的加法逆元可得 $0=0\cdot a$。

注 7. 设 R 是一个环，$a\in R$，n 是一个正整数，和群的情况类似，我们可以记 $na=\underbrace{a+a+\cdots+a}_{n个},0a=0,(-n)a=n(-a)$ 以及 $a^n=\underbrace{aa\cdots a}_{n个}$。我们需要注意到在记号 na 中 n 不一定是环 R 中的元素，所以它表示的不是环 R 中的元素的乘法。该记号和注 2 中所示一样满足乘法和加法的分配率以及指数运算的规则，故不再赘述。只需注意一点当 R 有乘法单位元时，我们才能定义 $a^0=1$，而当 a 有乘法逆元时，我们才能定义 $a^{-n}=(a^{-1})^n$。

3.1.2 多项式环和形式幂级数环

设 R 是一个环，考虑如下以 R 中元素为系数的多项式全体，即

$$R[x]:=\{a_0+a_1x+\cdots+a_nx^n\mid a_0,a_1,\ldots,a_n\in R,n\geq 0\}.$$

若 $a_n\neq 0$，我们称 a_n 为多项式 $f(x)=a_0+a_1x+\cdots+a_nx^n$ 的首项系数，n 为多项式 $f(x)$ 的次数，并记作 $\deg f$。$R[x]$ 上的加法和乘法定义如下：设 $\sum_{i=0}^n a_ix^i,\sum_{i=0}^m b_ix^i\in R[x]$（不妨设 $n\geq m$），其加法定义为

$$\sum_{i=0}^n a_ix^i+\sum_{i=0}^m b_ix^i=(a_0+b_0)+\cdots+(a_m+b_m)x^m+a_{m+1}x^{m+1}+\cdots+a_nx^n.$$

乘法定义为

$$\left(\sum_{i=0}^n a_ix^i\right)\left(\sum_{i=0}^m b_ix^i\right)=\sum_{k=0}^{m+n}\left(\sum_{\substack{i+j=k\\ i\leq n,j\leq m}}a_ib_j\right)x^k.$$

若 R 是整环，根据定义我们容易知道

$$\deg(f+g)\leq\max\{\deg f,\deg g\},\qquad \deg(f\cdot g)=\deg f+\deg g. \tag{3.1}$$

但是要注意到如果 R 不是整环，那么上述结论不一定成立。例如设 $R=\mathbb{Z}/4\mathbb{Z}$，那么 $f(x)=2x+1$ 的次数是 1，但是 $f(x)\cdot f(x)=4x^2+4x+1=1$ 的次数是 0。容易验证 $R[x]$ 构成一个环，因此我们通常称 $R[x]$ 为一元多项式环。

命题 3.1.6. 设 R 是一个整环，那么 $R[x]$ 也是一个整环，$R[x]$ 中的单位即为 R 中的单位。

证明. 设 $f(x)=a_nx^n+\cdots+a_x+a_0, g(x)=b_mx^m+\cdots+b_1x+b_0$ 两个非零多项式，其中 $a_n,b_m\neq 0$。根据多项式的乘法的定义知 $f(x)g(x)$ 的首项系数是 a_nb_m，因为 R 是整环，所以 $a_nb_m\neq 0$，故 $f(x)g(x)$ 也不是零多项式。因此 $R[x]$ 是整环。

设 $f(x)$ 是 $R[x]$ 中的单位，那么存在 $g(x)\in R[x]$ 使得 $f(x)g(x)=1$。根据式(3.1)有 $0=\deg(f\cdot g)=\deg f+\deg g$，因此 f,g 均只能为常数多项式，而 $fg=1$ 表明 f 是 R 中的单位。

更一般地，我们可以定义多元多项式环。设 $x_\lambda,\lambda\in\Lambda$ 是一族未定元。我们定义

$$R[x_\lambda]_{\lambda\in\Lambda}=\{\sum_{\lambda_{i_1},\ldots,\lambda_{i_n}\in\Lambda} a_{\lambda_{i_1},\ldots,\lambda_{i_n}}x_{\lambda_{i_1}}^{k_1}\cdots x_{\lambda_{i_n}}^{k_n}\mid a_{\lambda_{i_1},\ldots,\lambda_{i_n}}\in R,k_1,\ldots,k_n\geq 0\}.$$

$R[x_\lambda]_{\lambda\in\Lambda}$ 上的加法和乘法与一元多项式环类似，逐项相加相乘即可。当 Λ 是 n 元有限集时，我们可以将 n 元多项式环记为 $R[x_1,x_2,\ldots,x_n]$。

设 R 是一个环，考虑如下以 R 中元素为系数的形式幂级数全体，即

$$R[\![x]\!]:=\{a_0+a_1x+a_2x^2\cdots\mid a_0,a_1,a_2\cdots\in R\}.$$

$R[\![x]\!]$ 上的加法和乘法定义如下：设 $\sum_{i\geq 0}a_ix^i,\sum_{i\geq 0}b_ix^i\in R[\![x]\!]$，其加法定义为

$$\sum_{i\geq 0}a_ix^i+\sum_{i\geq 0}b_ix^i=(a_0+b_0)+(a_1+b_1)x+\ldots.$$

乘法定义为

$$\left(\sum_{i\geq 0}a_ix^i\right)\left(\sum_{i\geq 0}b_ix^i\right)=\sum_{k\geq 0}\left(\sum_{i+j=k}a_ib_j\right)x^k.$$

容易验证 $R[\![x]\!]$ 构成一个环，我们称之为形式幂级数环。它与多项式环有着许多不同的性质。例如多项式 $f(x)$ 在 $\mathbb{C}[x]$ 上可逆当且仅当 $f(x)$ 是非零常数多项式。但是绝大部分非常数幂级数都是可逆的，例如

$$(1-x)^{-1}=1+x+x^2+\ldots.$$

更一般地，我们有如下结论：

命题 3.1.7. 设 R 是一个整环，那么 $R[\![x]\!]$ 也是整环，并且 $f(x)\in R[\![x]\!]$ 是单位当且仅当 $f(x)$ 的常数项是 R 中的单位。

证明. 设 $f(x)=a_nx^n+a_{n+1}x^{n+1}+\ldots, g(x)=b_mx^m+b_{m+1}x^{m+1}+\cdots\in R[\![x]\!]$ 是两个非零元素，其中 $a_n,b_m\neq 0$。根据形式幂级数乘法的定义可知 $f(x)g(x)$ 的 x^{n+m} 前的系数为 a_nb_m，由于 R 是整环，故 $a_nb_m\neq 0$。因此 $f(x)g(x)\neq 0$，这便证明了 $R[\![x]\!]$ 是整环。

若 $f(x)=a_nx^n+a_{n+1}x^{n+1}+\cdots\in R[\![x]\!]$ 是一个单位，那么存在 $g(x)=b_mx^m+b_{m+1}x^{m+1}+\cdots\in R[\![x]\!]$ 使得 $f(x)g(x)=1$。对比常数项可知 $f(x)g(x)$ 的常数项等于 1，当且仅当 $n=m=0$ 且 $a_0b_0=1$，即有 $f(x)$ 的常数项是 R 中的单位。反之，若 $f(x)=a_0+a_1x+a_2x^2+\cdots\in R[\![x]\!]$，其中 a_0 是 R 中的单位。利用归纳法容易证明存在元素 $b_0,b_1,\cdots\in R$ 满足如下一系列等式：

$$a_0b_0=1,\quad a_0b_1+a_1b_0=0,\quad \ldots,\quad a_0b_r+a_1b_{r-1}+\cdots+a_rb_0=0,\quad \ldots.$$

事实上，我们取 $b_0=a_0^{-1}$，假设 $b_0,b_1,\ldots,b_{r-1}$ 均已取好，由于 a_0 可逆，因此我们取 $b_r=-a_0^{-1}(a_1b_{r-1}+\cdots+a_rb_0)$ 即可。此时取 $g(x)=b_0+b_1x+b_2x^2+\ldots$，那么根据构造我们有 $f(x)g(x)=1$，因此 $f(x)$ 是 $R[\![x]\!]$ 中的单位。

3.1.3 群环

设 R 是一个含幺环，G 是一个群，我们定义集合

$$R[G] = \{ \sum_{finite} r_g g \mid r_g \in R, g \in G \}.$$

$R[G]$ 中的加法是简单的逐项相加，即 $\sum a_g g + \sum b_g g = \sum (a_g + b_g) g$。乘法的定义则稍微复杂一些，它类似于多项式的 Cauchy 乘积。

$$(a_1 g_1 + \cdots + a_n g_n)(b_1 g_1 + \cdots + b_n g_n) = \sum_g \left(\sum_{g_i g_j = g} a_i b_j \right) g.$$

可以验证 $R[G]$ 在上述两种运算下构成一个环，我们称之为**群环**。

例 3.1.8. 设 $G = D_8 = \langle r, s \mid r^4 = s^2 = 1, rs = sr^{-1} \rangle$ 是 8 阶二面体群，$R = \mathbb{Z}$。考虑 $\alpha = r + r^2 + s, \beta = rs - r \in R[G]$。那么

$$\alpha + \beta = r^2 + s + rs,$$

$$\alpha\beta = (r + r^2 + s)(rs - r) = r^2 s + r^3 s + srs - r^2 - r^3 - sr = r^2 s + r^3 s - r^2 - sr.$$

再设 $\gamma = 1 - r, \delta = 1 + r + r^2 + r^3$，那么我们有

$$\gamma\delta = (1 - r)(1 + r + r^2 + r^3) = 1 - r^4 = 1 - 1 = 0.$$

这表明 $R[G]$ 不是整环。

3.1.4 $\mathbb{Z}[\sqrt{d}]$

在前面的例子中，我们考虑了高斯整数环，更一般地，给定一个非平方数 d，我们可以考虑 $\mathbb{Z}[\sqrt{d}]$。和高斯整数环的例子类似，我们可以证明 $\mathbb{Z}[\sqrt{d}]$ 在通常的加法和乘法下也构成一个环。对任意 $z = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$，我们定义 z 在 $\mathbb{Z}[\sqrt{d}]$ 中的共轭为 $\bar{z} = x - y\sqrt{d}$，以及它的范数为 $N(z) = z\bar{z} = x^2 - dy^2$。注意到当 $d < 0$，z 的范数即为 z 的模长的平方。对于环 $\mathbb{Z}[\sqrt{d}]$ 而言，我们可以用范数来描述它的单位。

引理 3.1.9. 我们有 $(\mathbb{Z}[\sqrt{d}])^* = \{ z \in \mathbb{Z}[\sqrt{d}] \mid N(z) = \pm 1 \}$。

证明. 假设 $a, b \in \mathbb{Z}[\sqrt{d}]$ 且 $ab = 1$，那么有 $N(ab) = N(a)N(b) = 1$，但是根据定义有 $N(a) \in \mathbb{Z}$，因此 $N(a), N(b)$ 只能为 ± 1。反之，若 $a \in \mathbb{Z}[\sqrt{d}]$ 有 $N(a) = \pm 1$，即有 $a\bar{a} = \pm 1$，因此 a 是 $\mathbb{Z}[\sqrt{d}]$ 中的单位。

当 $d < 0$ 时，我们可以直接计算 $\mathbb{Z}[\sqrt{d}]$ 中的单位。

推论 3.1.10. 我们有 $(\mathbb{Z}[\sqrt{-1}])^* = \{ \pm 1, \pm\sqrt{-1} \}$，且当 $d < -1$ 时有 $(\mathbb{Z}[\sqrt{d}])^* = \{ \pm 1 \}$。

证明. 假设 $x + d\sqrt{d} \in (\mathbb{Z}[\sqrt{d}])^*$，那么根据引理3.1.9，有 $x^2 - dy^2 = \pm 1$。当 $d < 0$ 时，只能有 $x^2 - dy^2 = 1$。当 $d = -1$ 时，方程即为 $x^2 + y^2 = 1$，容易看出该方程的整数解只有 $x = \pm 1, y = 0$ 或者 $x = 0, y = \pm 1$，对应的 z 分别为 $\pm 1, \pm\sqrt{-1}$。当 $d < -1$ 时，若 $y \neq 0$，则必有 $1 = x^2 - dy^2 \geq -d$，与假设矛盾。因此只能有 $z = \pm 1$。

然而一般来说当 $d>0$ 时，计算 $\mathbb{Z}[\sqrt{d}]$ 的单位是一件很困难的事，它与数论中的 Pell-方程密切相关。可以证明此时 $(\mathbb{Z}[\sqrt{d}])^*$ 一定是无穷集，参考练习3.1.18。

命题 3.1.11. 设 $d>0$ 是一个非平方数，那么存在一个最小的元素 $\eta_d>1$ 使得 $(\mathbb{Z}[\sqrt{d}])^*=\langle -1,\eta_d\rangle\simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}$。这里的 η_d 被称为**基本单位**。

例 3.1.12. 对于比较小的 d，下图展示了对应的基本单位。

d	2	3	5	6	7	8	10	11	12
η_d	$1+\sqrt{2}$	$2+\sqrt{3}$	$2+\sqrt{5}$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{8}$	$3+\sqrt{10}$	$10+3\sqrt{11}$	$7+2\sqrt{12}$

3.1.5 矩阵环和四元数环

最后我们介绍两个非交换环的例子。设 R 是任意一个环，n 是正整数。记 $M_n(R)$ 为所有系数在 R 中的 n 阶矩阵组成的集合。我们用 $(a_{ij})_{1\le i,j\le n}$（简记为 (a_{ij})）表示 R 中的元素。和通常的矩阵一样，我们定义 $M_n(R)$ 中的加法和乘法为：

$$(a_{ij})+(b_{ij})=(a_{ij}+b_{ij}),$$

而 $(a_{ij})\times(b_{ij})$ 的第 (i,j) 位置元素为 $\sum_{k=1}^n a_{ik}b_{kj}$。直接验证可知 $M_n(R)$ 构成一个环。易知当 $n\ge 2$ 时，$M_n(R)$ 不是交换环，也不是整环。若 R 含有乘法单位元，那么 $M_n(R)$ 也有乘法单位元，即为对角线元素为 1，其余位置为 0 的矩阵。此时 $M_n(R)$ 中的单位即为 n 阶可逆矩阵，我们称之为 R 上的**一般线性群**，记作 $\mathrm{GL}_n(R)$。

另一个例子是四元数环。记 $\mathbb{H}$ 为所有形如 $a+bi+cj+dk$ 的元素组成的集合，其中 $a,b,c,d\in\mathbb{R}$。$\mathbb{H}$ 中的加法定义为：

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k)=(a+a')+(b+b')i+(c+c')j+(d+d')k,$$

其乘法通过分配律以及如下关系定义：

$$i^2=j^2=k^2=-1,\quad ij=-ji=k,\quad jk=-kj=i,\quad ki=-ik=j.$$

例如

$$(1+i+2j)(i+k)=i+k+i^2+ik+2ji+2jk=i+k-1-j-2k+2i=-1+i-j-k.$$

可直接验证 $\mathbb{H}$ 构成一个非交换环，其零元素为 $0=0+0i+0j+0k$，乘法单位元为 $1=1+0i+0j+0k$。而且 $\mathbb{H}$ 的任意非零元均是可逆的，直接计算可知

$$(a+bi+cj+dk)^{-1}=\frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}.$$

四元数的定义看上去并不是很自然，我们将在下一节从矩阵的角度来理解四元数。像四元数环这种非零元素均可逆的环被称为**除环**，交换除环即为域。Wedderburn 小定理表明任何有限除环都是域，相关证明可参考这里。

3.1.6 环的直积

和群的直积类似，我们也可以定义环的直积。从集合的角度来说，环的直积同样也是集合的笛卡尔积，因此我们需要在这个笛卡尔积上赋予环结构。

定义 3.1.13. 设 $(R_i)_{i\in I}$ 是一族环（我们将不同环上的运算均记为 $+,\cdot$）。我们定义其笛卡尔积上的加法运算为 $(r_i)_i+(s_i)_i=(r_i+s_i)_i$，其乘法运算为 $(r_i)_i\cdot(s_i)_i=(r_i\cdot s_i)_i$。我们称具有上述运算的集合为 $R_i, i\in I$ 的**直积**，记作 $\prod_{i\in I}R_i$。特别地，当 I 是有限集时，我们直接记为 $R_1\times R_2\times\cdots\times R_n$。

直接验证可知 $\prod_{i\in I}R_i$ 在上述运算下构成一个环。通常情况下，环的直积都不会是整环。例如我们分别取 R_1,R_2 中的非零元 r_1,r_2，于是 $(a,0),(0,b)$ 都是 $R_1\times R_2$ 中的非零元，但是显然有 $(a,0)\cdot(0,b)=(0,0)$。因此 $(a,0),(0,b)$ 均为零因子。

习题

练习 3.1.1. 设 $\mathcal{C}$ 为从 $[0,1]$ 到 $\mathbb{R}$ 的所有连续函数构成的集合。证明 $\mathcal{C}$ 在函数的加法和乘法下构成一个环，并证明非零函数 $f(x)\in\mathcal{C}$ 是零因子当且仅当存在 $\{a\in[0,1]\mid f(a)=0\}$ 包含一个开区间。

练习 3.1.2. 设 M 是一个加法群，记 $\operatorname{End}M$ 为 M 到自身的全体同态的集合。设 $f,g\in\operatorname{End}M$，定义其加法为 $(f+g)(x)=f(x)+g(x)$，$\forall x\in M$。$\operatorname{End}M$ 上的乘法定义为映射的复合。验证 $\operatorname{End}M$ 在这两种运算下够成一个环。

练习 3.1.3. 设 X 是一个非空集合，记 $\mathcal{P}(X)$ 为 X 的所有子集组成的集合。我们在 $\mathcal{P}(X)$ 上定义如下加法和乘法：

$$A+B=(A-B)\cup(B-A),\quad A\times B=A\cap B.$$

这里 $A-B:=\{a\mid a\in A,a\notin B\}$。证明 $\mathcal{P}(X)$ 是一个含幺交换环。

练习 3.1.4. 设 $d\in\mathbb{Z}$ 是非平方数且 $d\equiv 1\pmod 4$。记 $\tau_d=\frac{1+\sqrt{d}}{2}$ 及

$$A_d=\mathbb{Z}+\mathbb{Z}\tau_d=\{n+m\tau_d\mid m,n\in\mathbb{Z}\}.$$

1. 证明 A_d 在通常的加法与乘法下构成一个环。
2. 计算 A_{-3}^*。
3. 证明当 $d<-3$ 时 $A_d^*=\{\pm1\}$。

练习 3.1.5. 设 R 是一个含幺整环，证明 R 中的幂等元只有 0 和 1，这里我们称满足 $a^2=a$ 的元素为**幂等元**。

练习 3.1.6. 设 R 是一个环，若对任意 $x\in R$ 均有 $x^2=x$，证明 R 是交换环。这类环被称为**布尔环**，例如练习*3.1.3*中的 $\mathcal{P}(X)$ 便是一个布尔环。

练习 3.1.7. 证明唯一的布尔整环是 $\mathbb{Z}/2\mathbb{Z}$。

练习 3.1.8. 设 R 是一个含幺环，设 $a,b\in R$，若 $1-ab$ 是可逆元，证明 $1-ba$ 也是可逆元。

练习 3.1.9. 证明任意有限交换整环一定是域。

练习 3.1.10. 设 $a \in R$，若存在正整数 n 使得 $a^n = 0$，则称 a 为**幂零元**。若 a 是幂零元，证明 $1+a$ 是 R 中的单位。

练习 3.1.11. 设 R 是一个含幺交换环，$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$。

1. 证明 f 是幂零元当且仅当 $a_0, a_1, \ldots, a_n$ 是幂零元。
2. 证明 f 是一个单位当且仅当 a_0 是单位，$a_1, \ldots, a_n$ 是幂零元。

练习 3.1.12. 设 R 是一个含幺交换环，证明 $f(x) \in R[x]$ 是零因子当且仅当存在非零元 $a \in R$ 使得 $af(x) = 0$。

练习 3.1.13. 设 $\alpha = 3(1\ 2) - 5(2\ 3) + (1\ 2\ 3), \beta = 2(1) + (2\ 3) - 3(1\ 3\ 2) \in \mathbb{Z}S_3$，计算 $2\alpha + 3\beta, \alpha\beta, \beta\alpha, \alpha^2$。

练习 3.1.14. 设 $\alpha = 3(1\ 2) - 5(2\ 3) + (1\ 2\ 3), \beta = 2(1) + (2\ 3) - 3(1\ 3\ 2) \in \mathbb{Z}/3\mathbb{Z}S_3$，计算 $2\alpha + 3\beta, \alpha\beta, \beta\alpha, \alpha^2$。

练习 3.1.15. 设 K 是一个域，若映射 $\nu : K^* \to \mathbb{Z}$ 满足如下条件：

1. ν 是一个群同态；
2. ν 是满射；
3. 对任意 $x, y \in K^*$ 且 $x + y \neq 0$ 均有 $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$。

我们则称 ν 是 K 上的一个**离散赋值**。我们称 $R = \{x \in K^* \mid \nu(x) \geq 0\} \cup \{0\}$ 为 ν 的**赋值环**。证明对任意 $x \in K^*$，若 $x \notin R$，则 $x^{-1} \in R$，并且 x 是 R 中的单位当且仅当 $\nu(x) = 0$。

练习 3.1.16. 设 p 是一个素数，对任意 $\frac{a}{b} \in \mathbb{Q}$，我们记 $\frac{a}{b} = p^n \frac{c}{d}$ 其中 $p \nmid cd$。我们定义 $\nu_p : \mathbb{Q}^* \to \mathbb{Z}$ 为 $\nu_p(a/b) = n$。证明 ν_p 是 $\mathbb{Q}$ 上的一个离散赋值，并计算其赋值环。证明这是 $\mathbb{Q}$ 上的所有离散赋值。

练习 3.1.17.
1. 设 $(a,b), (c,d) \in \mathbb{Z}^2$ 并且 $ad - bc \neq 0$。设 G 为由 $(a,b), (c,d)$ 生成的 $\mathbb{Z}^2$ 的子群，证明 $|\mathbb{Z}/G| = |ad - bc|$。
2. 设 $d > 0$ 是一个非平方的整数，$0 \neq \mathbb{Z}[\sqrt{d}]$。证明加法群 $\mathbb{Z}[\sqrt{d}]/z\mathbb{Z}[\sqrt{d}]$ 是有限群且元素个数等于 $|N(z)|$。

练习 3.1.18. 设 $d > 0$ 是一个非平方的整数。

1. 证明对任意 $\alpha \in \mathbb{R}$ 及任意整数 $M \geq 1$，存在 $p \in \mathbb{Z}$ 及 $1 \leq q \leq M$ 使得 $|q - q\alpha| < \frac{1}{M}$。
2. 证明存在一列非零数 $z_n \in \mathbb{Z}[\sqrt{d}]$ 使得 $z_n \to 0$ 且 $\{N(z_n)\}$ 是有界的。
3. 证明上面的数列中存在一个子列 $\{z_{n_k}\}$ 及整数 $m \in \mathbb{Z}$ 使得对任意 $k, \ell > 1$ 均有 $N(z_{n_k}) = m$ 且 $z_{n_k}\overline{z_{n_\ell}} \in m\mathbb{Z}[\sqrt{d}]$。
4. 证明 $\mathbb{Z}[\sqrt{d}]$ 中有无穷多个单位。

3.2 理想与商环

为方便起见，本节均假设环 R 为含幺环。

3.2.1 理想

定义 3.2.1. 设 R 是一个环，S 是 R 的非空子集。若 S 关于 R 的两种运算也构成一个环，那么称 S 为 R 的**子环**。

类似于群论中的商群，我们同样可以定义商环。和群的情况类似，仅仅只有子环结构，我们无法在等价类上定义一个自然的环结构，因为无法保证 R 和 S 中的元素的乘法封闭性，为此我们需要给出理想的概念。

定义 3.2.2. 设 R 是一个环，I 是 R 的一个子环，并且对任意 $a \in I$ 及 $r \in R$ 均有 $ra \in I$ $(ar \in I)$，则称 I 为 R 的**左（右）理想**。若 I 既是左理想又是右理想，则称 I 为**双边理想**，简称**理想**。

注意到对于交换环而言，左理想，右理想和双边理想是相同的。

例 3.2.3. *1.* 任意环 R 均有两个平凡理想 0 和 R。

2. 对任意正整数 m，$m\mathbb{Z}$ 都是 $\mathbb{Z}$ 的理想。

3. $\mathbb{Z}$ 是 $\mathbb{Z}$[i] 的子环，但不是理想。

4. 设 $R[x]$ 为环 R 上的多项式环，I 为所有常数项等于 0 的多项式的集合，那么 I 是 $R[x]$ 的一个理想。

5. 更一般地，设 $f(x) \in R[x]$，记 $(f(x)) = \{f(x)g(x) \mid g(x) \in R[x]\}$，那么 $(f(x))$ 也是 $R[x]$ 的理想。

和群的情况类似，我们也可以考虑用部分元素来生成环 R 的理想。

定义 3.2.4. 设 A 是环 R 的一个子集，我们记 (A) 为 R 中包含 A 的最小理想。我们称 (A) 为由 A **生成的理想**。若 A 只有一个元素，则称该理想为**主理想**，若 A 只有有限个元素，则称 A 是**有限生成的理想**。

我们下面介绍理想的一些基本性质。

命题 3.2.5. 设 $\{I_\lambda\}_{\lambda\in\Lambda}$ 是环 R 中的一族理想，那么 $\bigcap I_\lambda$ 也是 R 的理想。特别地，设 A 是 R 的一个子集，那么

$$(A) = \bigcap_{A\subseteq I} I,$$

这里 I 遍历 R 中所有包含 A 的理想。

证明. 直接验证即可。

命题 3.2.6. 设 I, J 是环 R 的两个理想，定义理想的和与乘积分别为

$$I + J = \{a + b \mid a \in I, b \in J\}, \quad IJ = \{a_1b_1 + \cdots + a_nb_n \mid a_1, \ldots, a_n \in I, b_1, \ldots, b_n \in J\}.$$

那么 $I + J$ 和 IJ 都是 R 中的理想。

证明. 直接验证即可。

命题 3.2.7. 设 I 是环 R 的一个理想，那么

1. $I = R$ 当且仅当 I 包含一个单位；

2. 若 R 是交换环，那么 R 是一个域当且仅当 R 只有 0 和 R 两个理想。

证明. 若 $I = R$，那么 $I = (1)$。反之，若 $I = (u)$，其中 u 是一个单位，那么对任意 $a \in R$ 均有 $a = au^{-1} \cdot u \in I$，所以 $I = R$。

假设 R 是一个域，显然它只有平凡的理想。反之，对任意 $0 \neq a \in R$，(a) 不是零理想，因此根据假设知 $(a) = R$，所以存在 $b \in R$ 使得 $ab = 1$，所以 a 可逆，这表明 R 是一个域。

3.2.2 环同态和商环

和群同态类似，我们也可以定义环之间的同态关系。

定义 3.2.8. 设 R, S 是两个环，若映射 $\varphi : R \to S$ 满足对任意 $a, b \in R$ 有 $\varphi(ab) = \varphi(a)\varphi(b)$，$\varphi(a + b) = \varphi(a) + \varphi(b)$，则称 φ 为**环同态**。我们称集合 $\ker\varphi = \{a \in R \mid \varphi(a) = 0\}$ 为 φ 的**核**，称集合 $\mathrm{Im}\,\varphi = \{\varphi(a) \mid a \in R\}$ 为 φ 的像。如果 φ 还是双射，则称 φ 是**环同构**。

同样地我们要注意到 R 中元素的加法和乘法与 S 中的加法与乘法不一定相同，在不会引起混淆的情况下，我们均用 $a + b$ 与 ab 表示。在群论中，我们需要正规子群才能定义商群，而在环论中，前面定义的理想便取代了正规子群的地位。设 I 是环 R 的一个理想，我们记

$$R/I := \{r + I \mid r \in R\}.$$

我们可以在集合 R/I 上定义两种运算：对任意 $r, s \in R$，我们定义

$$(r + I) + (s + I) := (r + s) + I, \qquad (r + I)(s + I) := rs + I.$$

定理 3.2.9. 集合 R/I 在这两种运算下构成一个环，我们称其为**商环**，并且我们有自然同态

$$\begin{array}{rccc} \pi : & R & \longrightarrow & R/I \\ & r & \longmapsto & r + I. \end{array}$$

证明. 直接验证即可。

商环同样有如下泛性质：

命题 3.2.10. 设 R, S 是两个环，I 是 R 的理想，对任意环同态 $f : R \to S$，若 $I \subseteq \ker f$，那么存在唯一的环同态 $\bar{f} : R/I \to S$ 使得 $f = \bar{f} \circ \pi$，即有如下交换图表：

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle\pi}\downarrow & \nearrow_{\bar{f}} & \\ R/I & & \end{array}$$

证明. 证明和命题2.3.16类似，我们略去不表。

例 3.2.11. 1. 设 R 是一个环，那么我们有同构

$$\begin{array}{ccc} R[x]/(x) & \longrightarrow & R \\ \bar{f}(x) & \longmapsto & f(0). \end{array}$$

2. 设 R 是一个环，我们有环同构 $R[x_1,x_2,\ldots,x_n]\to R[x_1,x_2,\ldots,x_{n-1}][x_n]$，该映射即为将多元多项式 $f(x_1,x_2,\ldots,x_n)$ 视作关于 x_n 的多项式，其系数在 $R[x_1,x_2,\ldots,x_{n-1}]$ 中。

3. 设 R 是一个环，G 是一个有限群，那么如下映射是一个群同态：
$$\begin{array}{ccc} RG & \longrightarrow & R \\ \sum_{i=1} r_i g_i & \longmapsto & \sum_{i=1}^n r_i. \end{array}$$

4. 设 I 是环 R 的一个理想，记 $(I)=I[x]$ 为 $R[x]$ 中 I 生成的理想，那么我们有环同构 $R[x]/(I)\simeq (R/I)[x]$。

5. 设 $I=(2,x)\subseteq\mathbb{Z}[x]$，考虑如下同态：
$$\begin{array}{ccc} \mathbb{Z}[x]/I & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ \bar{f}(x) & \longmapsto & f(0). \end{array}$$
可以验证这是一个环同构。

6. 设 $R=\mathbb{C}[x,y]/(x^2,xy,y^2)$，并假设 $\bar{x},\bar{y}$ 分别为 x,y 所在的类。那么 R 中的任意元素均可表示成 $a+b\bar{x}+c\bar{y}$。这是因为 $\bar{x}^2,\bar{x}\bar{y},\bar{y}^2$ 在 R 中均等于 $\bar{0}$。此时 $a+b\bar{x}+c\bar{y}$ 在 R 中可逆当且仅当 $a\neq 0$。当 $a\neq 0$ 时，不妨设 $a=1$，那么 $1+b\bar{x}+c\bar{y}$ 的逆即为 $1-b\bar{x}-c\bar{y}$，这是因为
$$(1+b\bar{x}+c\bar{y})(1-b\bar{x}-c\bar{y})=1-(b\bar{x}+c\bar{y})^2=1.$$

7. 设 $R=\mathbb{Q}[x,y,z]/(x-xyz)$，并假设 $\bar{x},\bar{y},\bar{z}$ 分别为 x,y,z 所在的类。那么 R 不是一个整环，并且有 $(\bar{x})=(\bar{x}\bar{y})$。事实上，在 R 中，我们有 $\bar{x}(1-\bar{y}\bar{z})=0$，但是容易验证 $\bar{x}$ 和 $1-\bar{y}\bar{z}$ 在 R 中均不是零元素。因此 R 不是整环。一方面，我们显然有 $(\bar{x}\bar{y})\subseteq(\bar{x})$。另一方面，由于 $\bar{x}=\bar{x}\bar{y}\bar{z}\subseteq(\bar{x}\bar{y})$。因此我们有 $(\bar{x})=(\bar{x}\bar{y})$。

8. 设 R_i 均为环，并且有如下同态链条：
$$\cdots\to R_{i-1}\xrightarrow{f_i} R_i\xrightarrow{f_{i+1}} R_{i+1}\to\ldots,$$
若这些同态均满足 $\operatorname{Im} f_i=\ker f_{i+1}$，那么则称该同态链条为**正合列**。容易验证
$$0\to R'\xrightarrow{f} R \text{ 是正合列} \iff f \text{ 是单射};$$
$$R\xrightarrow{g} R''\to 0 \text{ 是正合列} \iff g \text{ 是满射}.$$
而 $0\to R'\xrightarrow{f} R\xrightarrow{g} R''\to 0$ 是正合列当且仅当 f 是单射，g 是满射且 g 诱导了同构 $R/f(R')\simeq R''$。像这样的正合列被称之为**短正合列**。例如我们有短正合列：$0\to\mathbb{Z}\xrightarrow{\times n}\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\to 0$。

9. 在3.1.5节中定义的除环看上去并不是特别地自然，我们可以用矩阵的语言重新定义除环。首先我们注意到复数 $a+b\mathrm{i}$ 可以对应于一个 2×2 的实矩阵 $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$。同时该对应给出了复数域到矩阵环的子环 $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\mid a,b\in\mathbb{R}\right\}$ 直接的一个环同构。类似地，考虑如下复矩阵集
$$\mathbb{M}=\left\{\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}\mid \alpha,\beta\in\mathbb{R}\right\}.$$

我们可以定义映射：

$$\begin{array}{ccc} \mathbb{H} & \longrightarrow & \mathbb{M} \\ a+bi+cj+dk & \longmapsto & \begin{pmatrix} a+b\sqrt{-1} & c+d\sqrt{-1} \\ -c+d\sqrt{-1} & a-b\sqrt{-1} \end{pmatrix}. \end{array}$$

可以验证这是一个环同构。特别地，我们有

$$i \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

和群同构定理类似，我们也有如下的环同构定理。其证明和群同构定理类似，故我们略去不表。

定理 3.2.12 (第一同构定理)**.** 设 $\varphi : R \to S$ 是一个环同态，那么 $\ker\varphi$ 是 R 的一个理想，并且有同构 $R/\ker\varphi \simeq \varphi(R)$。

定理 3.2.13 (第二同构定理)**.** 设 A 是环 R 的子环，B 是环 R 的理想。设 $A+B = \{a+b \mid a \in A, b \in B\}$。那么 $A+B$ 是 R 的子环，$A \cap B$ 是 A 的理想，并且有同构 $(A+B)/B \simeq A/(A \cap B)$。

定理 3.2.14 (第三同构定理)**.** 设 I, J 是环 R 的理想，且 $I \subseteq J$。那么 J/I 是 R/I 的理想，且 $(R/I)/(J/I) \simeq R/J$。

3.2.3 中国剩余定理

这一节我们讨论中国剩余定理。设 I, J 是环 R 的两个理想，若存在 $r \in I, s \in J$ 使得 $r+s = 1$，我们则称 I, J **互素**。首先我们给出互素的理想的一些基本性质。

命题 3.2.15. 设 $I_1, I_2, \ldots, I_n$ 是 R 中两两互素的理想，那么 I_1 和 $I_2 \cap \cdots \cap I_n$ 也互素。

证明. 由于 I_1 和 I_i，$i = 2, \ldots, n$ 互素，因此存在 $r_i \in I_1$ 和 $s_i \in I_i$ 使得 $r_i + s_i = 1$，累乘即得 $(r_2+s_2)\cdots(r_n+s_n) = 1$。将其展开可得

$$r_2(r_3+s_3)\cdots(r_n+s_n) + s_2r_3(r_4+s_4)\cdots(r_n+s_n) + \cdots + s_2s_3\cdots s_{n-1}r_n + s_2s_3\cdots s_n = 1.$$

根据理想的定义可知上式左边除了最后一项均属于 I_1，而 $s_2s_3\cdots s_n \in I_2 \cap \cdots \cap I_n$，因此根据定义可知 I_1 和 $I_2 \cap \cdots \cap I_n$ 互素。

定理 3.2.16 (中国剩余定理)**.** 设 $I_1, \ldots, I_n$ 是环 R 的两两互素的理想，那么我们有环同构

$$R/I_1 \cap \cdots \cap I_n \simeq R/I_1 \times \cdots \times R/I_n.$$

证明. 考虑自然映射

$$\begin{array}{rccc} \psi : & R & \longrightarrow & R/I_1 \times \cdots \times R/I_n \\ & r & \longmapsto & (r+I_1, \ldots, r+I_n). \end{array}$$

根据定义容易得知 $\ker\psi = I_1 \cap \cdots \cap I_n$，因此根据环同态基本定理，我们只需证明 ψ 是满射即可。首先我们证明 $(1+I_1, 0+I_2, \ldots, 0+I_n)$ 在 $\mathrm{Im}\,\psi$ 中。根据性质3.2.15可知存在 $s \in I_1$ 及 $r_1 \in I_2 \cap \cdots \cap I_n$ 使得 $r_1 + s = 1$。因此根据定义可知 $\psi(r_1) = (1+I_1, 0+I_2, \ldots, 0+I_n)$。同理可证存在 $r_2, \ldots, r_n$ 使得

$\psi(r_i) = (0 + I_1, \ldots, 1 + I_i, \ldots, 0 + I_n)$。最后对任意 $(a_1 + I_1, \ldots, a_n + I_n) \in R/I_1 \times \cdots \times R/I_n$，根据环同态的定义可知

$$\psi(a_1 r_1 + \cdots + a_n r_n) = (a_1 + I_1, \ldots, a_n + I_n).$$

因此 ψ 是满射。

作为推论，我们可以得到整数版本的中国剩余定理。

推论 3.2.17. 设 $n_1, n_2, \ldots, n_k$ 是两两互素的正整数，记 $n = n_1 n_2 \cdots n_k$，那么我们有如下同构

$$\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}).$$

特别地，如果我们取两边的单位群，那么我们有如下群同构

$$(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/n_1\mathbb{Z})^* \times (\mathbb{Z}/n_2\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})^*.$$

习题

练习 3.2.1. 判断下面哪些集合是 $\mathbb{Z}[x]$ 的理想。

1. 所有常数项是 3 的倍数的多项式组成的集合。
2. 所有奇数项系数为 0 的多项式组成的集合。
3. 所有系数和为 0 的多项式组成的集合。

练习 3.2.2. 设 $\mathcal{C}$ 为从 $[0,1]$ 到 $\mathbb{R}$ 的所有连续函数构成的集合，I 是 $\mathcal{C}$ 的一个非平凡理想。证明存在 $a \in [0,1]$ 使得对任意 $f(x) \in I$ 均有 $f(a) = 0$。

练习 3.2.3. 设 $\mathcal{P}(X)$ 是练习*3.1.3*中定义的环，设 $A \subseteq X$ 是 X 的一个子集，求 A 在 $\mathcal{P}(X)$ 中生成的理想。

练习 3.2.4. 设 I 是环 R 的理想，记 $r(I) = \{a \in R \mid ax = 0 \quad \forall x \in I\}$。证明 $r(I)$ 也是一个理想。

练习 3.2.5. 设 I, J, K 是环 R 的理想。下列关于理想的结合律和分配律是否成立。

1. $(IJ)K = I(JK)$？
2. $I(J + K) = IJ + IK$？

练习 3.2.6. 设 $I_1 \subseteq I_2 \subseteq$ 是 R 中的一列理想，证明 $\cup_{n \geq 1} I_n$ 也是 R 中的理想。

练习 3.2.7. 证明 $\mathbb{Z}/m\mathbb{Z}$ 中存在非零的幂零元当且仅当 m 有平方因子，即存在素数 p 使得 p^2 整除 m。

练习 3.2.8. 设 R 是一个环，I 是一个理想。我们称集合 $\sqrt{I} := \{a \in R \mid$ 存在正整数 n 使得$a^n \in I\}$ 为 I 的**根**。

1. 证明 $\sqrt{I}$ 是一个理想。
2. 设 $R = \mathbb{Z}, I = N\mathbb{Z}$，计算 $\sqrt{I}$。

练习 3.2.9. 设 R 是一个交换环，若 R 的理想均是有限生成的，那么我们称 R 为**诺特环**。证明下列命题是等价的。

1. R 是诺特环。
2. 设 $(I_m)_{m\geq 1}$ 是 R 中的一列递增的理想，即对任意 $m \geq 1$ 有 $I_m \subseteq I_{m+1}$，那么存在 M 使得对任意 $m > M$ 均有 $I_m = I_{m+1}$。
3. R 的任意一族理想在包含关系下均有极大元。

练习 3.2.10. 若复数 $z \in \mathbb{C}$ 满足一个首一整系数的多项式，我们则称 z 是一个**代数整数**，我们记所有代数整数组成的集合为 $\overline{\mathbb{Z}}$。

1. 证明 $\overline{\mathbb{Z}}$ 构成一个环。
2. 证明 $\overline{\mathbb{Z}}$ 不是诺特环。

练习 3.2.11. 判断下列命题是否正确。

1. 诺特环的子环都是诺特环。
2. 诺特环的商环都是诺特环。
3. 有限个诺特环的直积是诺特环。
4. 对任意 $\alpha \in \mathbb{C}$，环 $\mathbb{Z}[\alpha]$ 均是诺特环。

练习 3.2.12. 设 R 是一个诺特环，$f : R \to R$ 是一个环同态。

1. 证明存在整数 $n \geq 1$ 使得 $\ker(f^n) = \ker(f^{n+1})$。由此证明 $f : \mathrm{Im}(f^n) \to \mathrm{Im}(f^{n+1})$ 是单射。
2. 证明若 f 满射，那么它是双射。
3. 请找一个反例说明上一问中由 f 是单射推不出 f 是双射。
4. 请找一个反例说明若 R 不是诺特环，则 f 是满射也推不出 f 是双射。

练习 3.2.13. 设 d 是一个非平方的整数，$R = \mathbb{Z}[\sqrt{d}]$。

1. 设 I 是 R 的一个非零理想，证明 I 包含一个正整数。
2. 对于给定的一个正整数 n，证明至多存在有限个包含 n 的理想。
3. 证明 R 是诺特环，且任意非零理想在 R 中的指数是有限的。
4. 对于给定的一个正整数 n，证明 R 只有有限个主理想 (z) 使得 $N(z) = n$。

练习 3.2.14. 判断下列映射哪些是从 $M_2(\mathbb{Z})$ 到 $\mathbb{Z}$ 的环同态。

1. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a$

2. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a+d$

3. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad-bc$

练习 3.2.15. 设 $f_1 : R_1 \to R_2$，$f_2 : R_2 \to R_3$ 是环同态，证明 $f_2 f_1 : R_1 \to R_3$ 也是环同态。

练习 3.2.16. 设 $f : R \to S$ 是一个环同态，a 是 R 中的幂零元，证明 $f(a)$ 是 S 中的幂零元。

练习 3.2.17. 1. 证明 $\mathbb{Q}$ 上的环同构只有恒等映射。

2. 证明实数域上的环同构也只有恒等映射。

练习 3.2.18. 计算商环 $\mathbb{Z}/12\mathbb{Z}$ 的所有理想。

练习 3.2.19. 设 m, n 是互素的正整数，证明 $\mathbb{Z}/m\mathbb{Z}$ 到 $\mathbb{Z}/n\mathbb{Z}$ 的环同态只有零同态。

练习 3.2.20. 设 X 是一个非空集合，$\mathcal{P}(X)$ 是习题3.1.3中定义的环。记 R 为所有从 X 到 $\mathbb{Z}/2\mathbb{Z}$ 上函数组成的环。对任意 $A \in \mathcal{P}(X)$，定义 $\chi_A : X \to \mathbb{Z}/2\mathbb{Z}$，其中当 $x \in A$ 时，$\chi_A(x) = 1$，当 $x \notin A$ 时，$\chi_A(x) = 0$。证明映射

$$\begin{array}{ccc} \mathcal{P}(X) & \longrightarrow & R \\ A & \longmapsto & \chi_A \end{array}$$

是一个环同态。

练习 3.2.21. 设 R 是一个环，$f(x) \in R[x]$ 为次数 $n \geq 1$ 的首一多项式。我们记 $\overline{g(x)}$ 为 $p(x) \in R[x]$ 在 $R[x]/(f(x))$ 中的像。

1. 证明 $R[x]/(f(x))$ 中的元素均形如 $\overline{g(x)}$，其中 $g(x)$ 是次数小于 n 的多项式。

2. 设 a 是 R 中的幂零元，$f(x) = x^n - a$。证明 $\bar{x}$ 是 $R[x]/(f(x))$ 中的幂零元。

3. 设 p 是一个素数，$R = \mathbb{Z}/p\mathbb{Z}$，$f(x) = x^p - a$，其中 $a \in \mathbb{Z}/p\mathbb{Z}$。证明 $\overline{x-a}$ 是 $R[x]/(f(x))$ 中的幂零元。

练习 3.2.22. 设 G 是 n 阶交换群，$\hat{G}$ 记为从 G 到 $\mathbb{C}^*$ 的全体群同态。对任意 $\chi \in \hat{G}$，记

$$e_\chi = \frac{1}{n} \sum_{g \in G} \chi(g) g^{-1} \in \mathbb{C}[G].$$

证明 $e_\chi^2 = e_\chi$，$e_\chi g = \chi(g) e_\chi$，$\sum_{\chi \in \hat{G}} e_\chi = 1$，及对任意 $\chi \neq \chi'$ 均有 $e_\chi \cdot e_{\chi'} = 0$。

3.3 素理想和极大理想

这一节我们介绍两类特殊的理想，它们在环论中具有重要的作用。

3.3.1 极大理想

定义 3.3.1. 设 $\mathfrak{m}$ 是环 R 中的一个理想，若严格包含 $\mathfrak{m}$ 的理想只有 R 本身，那么则称 $\mathfrak{m}$ 是**极大理想**。

一般而言，环不一定会有极大理想，但是对于含幺环而言，极大理想是存在的。和许多存在性问题类似，极大理想的存在性也依赖于 Zorn 引理。

定理 3.3.2. *设 R 是一个含幺环，那么 R 的任意真理想均包含在一个极大理想中。*

证明. 设 I 是 R 的一个真理想，设 $\mathcal{S}$ 是 R 中所有包含 I 的真理想组成的集合。显然 $\mathcal{S}$ 非空，且在包含关系下构成一个偏序集。假设 $\mathcal{C}$ 是 $\mathcal{S}$ 中的一条链，我们定义

$$J = \bigcup_{A\in\mathcal{C}} A.$$

首先我们证明 J 是 R 的一个理想。显然 J 是非空的。对任意 $a,b\in J$，不妨设 $a\in A, b\in B$，由于 $\mathcal{C}$ 是全序集，因此不妨设 $A\subseteq B$，于是 $a,b\in B$，因此 $a+b\in B\subseteq J$。对任意 $r\in R, a\in J$，不妨设 $a\in A$，于是 $ra\in A\subseteq J$，由此可得 J 是一个理想。

下面再证明 J 是真理想，否则假设 $1\in J$，那么存在 $A\in\mathcal{C}$ 使得 $1\in A$，这与 A 是真理想矛盾。这表明 $\mathcal{S}$ 中的任意一条链都在 $\mathcal{S}$ 中有上界，因此根据 Zorn 引理可知 $\mathcal{S}$ 中有极大元，此即为包含 I 的极大理想。

注 8. 对于没有乘法单位元的环，我们可以构造一个没有极大理想的例子。取 $R=\mathbb{Q}$，加法是通常意义下的加法，乘法定义为 $ab=0, \forall a,b\in R$。在这种情况下，R 的理想即为 $\mathbb{Q}$ 的加法子群，然而根据练习2.3.22可知 $\mathbb{Q}$ 没有极大子群。

从定义来说，要验证一个理想是否是极大理想并不是一个简单的事。但是对于交换环而言，极大理想有一个更加简单的刻画。

命题 3.3.3. *设 R 是一个交换环，那么 $\mathfrak{m}$ 是 R 的极大理想当且仅当 $R/\mathfrak{m}$ 是域。*

证明. 设 $\mathfrak{m}$ 是一个极大理想，设 $a\in R\setminus\mathfrak{m}$，那么 $(a)+\mathfrak{m}$ 是严格包含 $\mathfrak{m}$ 的理想，由 $\mathfrak{m}$ 的极大性可知 $(a)+\mathfrak{m}=R$。所以存在 $r\in R$ 及 $b\in\mathfrak{m}$ 使得 $ar+b=1$，于是 $\bar{a}\cdot\bar{r}=\bar{1}$，这表明 $\bar{a}$ 在 $R/\mathfrak{m}$ 中可逆，由 a 的任意性可知 $R/\mathfrak{m}$ 是一个域。

反之，若 $R/\mathfrak{m}$ 是一个域，若 $\mathfrak{m}$ 不是极大理想，那么存在 $a\in R\setminus\mathfrak{m}$ 使得 $(a)+\mathfrak{m}$ 是 R 的真理想。但由于 $\bar{a}$ 在 $R/\mathfrak{m}$ 中可逆，所以存在 $r\in R$ 使得 $ar-1\in\mathfrak{m}$，即有 $1\in(a)+\mathfrak{m}$，这与 $(a)+\mathfrak{m}$ 是真理想矛盾。

例 3.3.4.

1. $\mathbb{Z}$ 的理想 $(n)=n\mathbb{Z}$ 是极大理想当且仅当 n 是素数。事实上，若 n 不是素数，设 p 是 n 的一个素因子，那么显然有 $(n)\subsetneq(p)$，故 (n) 不是极大理想。反之，若 p 是素数，根据例3.1.2我们知道 $\mathbb{Z}/(p)$ 是域，因此 (n) 是极大理想。

2. 由例3.2.11第一个例子可知 (x) 是 $R[x]$ 的极大理想当且仅当 R 是域。

3. 由于 $\mathbb{Z}/2\mathbb{Z}$ 是一个域，因此由例3.2.11可知 $(2,x)$ 是 $\mathbb{Z}[x]$ 的一个极大理想。

3.3.2 素理想

定义 3.3.5. 设 R 是一个交换环，$\mathfrak{p}$ 是 R 的一个真理想，若对任意 $a,b\in R\setminus\mathfrak{p}$，均有 $ab\notin\mathfrak{p}$，那么我们称 $\mathfrak{p}$ 为素理想。

和极大理想的定义不同，素理想的定义似乎有些奇怪。事实上，它是对素数的一种推广。我们假设 $R=\mathbb{Z}$，$\mathfrak{p}=n\mathbb{Z}$ 其中 n 是一个正整数，这时候如果 $\mathfrak{p}$ 是一个素理想，那么对任意整数 a,b，若 ab 是 n 的倍数，那么 a 和 b 至少有一个是 n 的倍数，这便是素数的一个刻画，即 $\mathfrak{p}$ 是素理想当且仅当 n 是素数。当然我们注意到 (0) 也是 $\mathbb{Z}$ 的一个素理想。事实上，一般而言，(0) 是环 R 的素理想当且仅当 R 是整环。和极大理想类似，我们对素理想也有一个简单的刻画。

命题 3.3.6. 设 R 是一个交换环，那么 $\mathfrak{p}$ 是 R 的素理想当且仅当 $R/\mathfrak{p}$ 是整环。由此可知极大理想一定是素理想。

证明. 设 $\mathfrak{p}$ 是一个素理想，若 $R/\mathfrak{p}$ 不是整环，则存在 $a,b\in R\setminus\mathfrak{p}$ 使得 $\bar{a}\cdot\bar{b}=\bar{0}$，这等价于 $ab\in\mathfrak{p}$，但这与 $\mathfrak{p}$ 是素理想矛盾。

反之，假设 $R/\mathfrak{p}$ 是整环，那么对任意 $a,b\in R$，若 $ab\in\mathfrak{p}$，则 $\bar{0}=\overline{ab}=\bar{a}\cdot\bar{b}$，因此 $\bar{a}=\bar{0}$ 或者 $\bar{b}=\bar{0}$。这表明 $a\in\mathfrak{p}$ 或者 $b\in\mathfrak{p}$，所以 $\mathfrak{p}$ 是素理想。

例 3.3.7. *1.* $\mathbb{Z}$ 的所有素理想为 (0) 和素数生成的理想，并且素数生成的理想均是极大理想。

2. $\mathbb{Q}[x]$ 的所有素理想为 (0) 和不可约多项式生成的理想，而不可约多项式生成的理想均为极大理想。

3. 由例*3.2.11*第一个例子可知 (x) 是 $R[x]$ 的素理想当且仅当 R 是整环。因此虽然 (x) 不在 $\mathbb{Z}[x]$ 中的极大理想，但是是素理想。

4. $\mathbb{Z}[x]$ 中的素理想除了 (0)，不可约多项式生成的理想之外还有许多素理想，例如 $(2,x)$。如前所述此时素理想 (x) 则不再是极大理想了，$(2,x)$ 是包含 (x) 的极大理想。刻画 $\mathbb{Z}[x]$ 中的所有素理想则是一件比较困难的事，可参考练习*3.5.12*。

5. 在 $\mathbb{Z}[\sqrt{-1}]$ 中，$(1+\sqrt{-1})$ 是素理想，同时也是极大理想。事实上我们可以证明 $\mathbb{Z}[\sqrt{-1}]/(1+\sqrt{-1})\simeq\mathbb{Z}/2\mathbb{Z}$，因为对任意 $a+b\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}]$，当 $a+b$ 是偶数时，在 $\mathbb{Z}[\sqrt{-1}]/(1+\sqrt{-1})$ 中有 $\overline{a+b\sqrt{-1}}=\bar{0}$；当 $a+b$ 是奇数时有 $\overline{a+b\sqrt{-1}}=\bar{1}$。更一般地，设 p 是一个奇素数，可以证明当 $p\equiv 3\pmod 4$ 时，(p) 是 $\mathbb{Z}[\sqrt{-1}]$ 中的素理想，当 $p\equiv 1\pmod 4$，则存在整数 a,b 使得 $p=a^2+b^2$，此时 $(a\pm b\sqrt{-1})$ 均是素理想。

6. 下面我们计算 $\mathbb{Z}[\sqrt{-5}]$ 中的几个素理想。首先注意到在 $\sqrt{-5}$ 处的赋值诱导了如下同构：

$$\begin{array}{ccc}\mathbb{Z}[X]/(X^2+5) & \longrightarrow & A=\mathbb{Z}[\sqrt{-5}]\\ g(X) & \longmapsto & g(\sqrt{-5}).\end{array}$$

由此我们有如下同构：

$$\begin{aligned}A/3A&\simeq\mathbb{Z}[X]/(3,X^2+5)\simeq\mathbb{Z}/3\mathbb{Z}[X]/(X^2+5)\simeq\mathbb{Z}/3\mathbb{Z}[X]/(X^2-1)\\&\simeq\mathbb{Z}/3\mathbb{Z}[X]/((X-1)(X+1))\simeq\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z},\end{aligned}$$

其中最后一个同构由赋值映射 $X \mapsto 1$ 和 $X \mapsto -1$ 诱导。由于 $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ 不是整环，故 (3) 不是 A 的素理想。考虑该映射到两个分量的投影可以得到如下两个满同态：

$$\alpha_1 : A \xrightarrow{\sim} \mathbb{Z}[X]/(X^2+5) \to \mathbb{Z}[X]/(3, X^2+5) \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \xrightarrow{\mathrm{Pr}_1} \mathbb{Z}/3\mathbb{Z},$$

$$\alpha_2 : A \xrightarrow{\sim} \mathbb{Z}[X]/(X^2+5) \to \mathbb{Z}[X]/(3, X^2+5) \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \xrightarrow{\mathrm{Pr}_2} \mathbb{Z}/3\mathbb{Z}.$$

其具体表达式是由下面的公式给出：

$$\alpha_1 : a + b\sqrt{-5} \mapsto a + b \pmod 3,$$

$$\alpha_2 : a + b\sqrt{-5} \mapsto a - b \pmod 3.$$

因此我们可以直接计算这两个同态的核为

$$\mathfrak{p}_1 := \ker \alpha_1 = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}, 3 \mid a + b\} = (3, 1 - \sqrt{-5}),$$

$$\mathfrak{p}_2 := \ker \alpha_2 = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}, 3 \mid a - b\} = (3, 1 + \sqrt{-5}).$$

由同态基本定理可知 $A/\mathfrak{p}_i \simeq \mathbb{Z}/3\mathbb{Z}$，因此 $\mathfrak{p}_1.\mathfrak{p}_2$ 既是素理想也是极大理想。同时直接计算可知

$$\mathfrak{p}_1\mathfrak{p}_2 = (3, 1 - \sqrt{-5})(3, 1 + \sqrt{-5}) = (9, 3 - 3\sqrt{-5}, 3 + 3\sqrt{-5}, 6) = (3).$$

类似的计算我们可以得到

$$(7) = (7, 3 + \sqrt{-5})(7, 3 - \sqrt{-5}).$$

更一般地，我们可以证明 A 中每一个非零素理想均能唯一分解为有限个素理想的乘积，像这样的环我们称之为 ***Dedekind* 环**。

习题

练习 3.3.1. 求下列环的极大理想：

(1) $\mathbb{R} \times \mathbb{R}$; (2) $\mathbb{R}[x]/(x^2)$; (3) $\mathbb{R}[x]/(x^2 - 1)$.

练习 3.3.2. 设 $\mathfrak{p}$ 是 R 中的素理想，证明 $\sqrt{\mathfrak{p}} = \mathfrak{p}$，其中 $\sqrt{\mathfrak{p}}$ 的定义见练习 *3.2.8*。

练习 3.3.3. 设 p 是一个素数，记 $\mathbb{Z}[\zeta_p] = \{f(\zeta_p) \mid f(x) \in \mathbb{Z}[x]\}$，其中 $\zeta_p = \mathrm{e}^{\frac{2\pi \mathrm{i}}{p}}$。

1. 证明 $\mathbb{Z}[\zeta_p]$ 在通常的加法和乘法下构成一个环。
2. 证明 $(1 - \zeta_p)$ 是 $\mathbb{Z}[\zeta_p]$ 中的素理想。
3. 证明 $(p) = (1 - \zeta_p)^{p-1}$。

练习 3.3.4. 1. 设 $R = \mathbb{C}[x, y]$，判断 $(x^2 + y^2 - 1)$ 是否是素理想，是否是极大理想？

2. 设 $R = \mathbb{R}[x, y]$，判断 $(x^2 + y^2 - 1)$ 是否是素理想，是否是极大理想？

练习 3.3.5. 设 R 是一个含幺交换环。$\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ 均为 R 的素理想。$I, I_1, \ldots, I_n$ 均是 R 中的理想。

1. 若 $I_1 I_2 \subseteq \mathfrak{p}$，证明 $I_1 \subseteq \mathfrak{p}$ 或 $I_2 \subseteq \mathfrak{p}$。

2. 若 $I_1I_2\cdots I_n$ 包含 $\mathfrak{p}$，证明存在一个 k 使得 I_k 包含 $\mathfrak{p}$。

3. 若 I 包含在 $\bigcup_{i=1}^n \mathfrak{p}_i$ 中，证明存在一个 k 使得 $\mathfrak{p}_k$ 包含 I。

练习 3.3.6. 设 R 是一个含幺交换环，证明多项式环 $R[x]$ 中的理想 (x) 是素理想当且仅当 R 是整环，(x) 是极大理想当且仅当 R 是域。

练习 3.3.7. 设 R 是一个含幺交换环，若 R 只有唯一的极大理想，则称 R 为**局部环**。

1. 证明 R 是局部环当且仅当 $R\setminus R^*$ 是一个理想。

2. 若 $\mathfrak{m}$ 是 R 的一个极大理想，且对任意 $x\in\mathfrak{m}$，$1+x$ 均为 R 中的单位，证明 R 是局部环。

3. 若 $\mathfrak{m}$ 是 R 的一个极大理想且满足 $\mathfrak{m}^2=0$，证明 R 是局部环。

练习 3.3.8. 设 $\mathcal{C}$ 为从 $[0,1]$ 到 $\mathbb{R}$ 的所有连续函数构成的集合。对每个 $x\in[0,1]$，记 $I_x:=\{f\in\mathcal{C}\mid f(x)=0\}$。

1. 证明 I_x 是 $\mathcal{C}$ 的极大理想。

2. 若 I 是 $\mathcal{C}$ 的极大理想，证明存在 $x\in[0,1]$ 使得 $I=I_x$。

3. 记 $I=\{f\in\mathcal{C}\mid \lim_{x\to 0}\frac{f(x)}{x^m}=0,\forall m\in\mathbb{N}\}$，证明 $I=\sqrt{I}$。

4. 构造 $\mathcal{C}$ 中一个不是极大理想的素理想。

练习 3.3.9. 设 R 是一个含幺交换环，I 是其一个理想。若 $\mathfrak{p}$ 是包含 I 的素理想，那么 $\mathfrak{p}/I$ 是 R/I 的素理想。反之，设 $\mathfrak{p}$ 是包含 I 的理想，若 $\mathfrak{p}/I$ 是 R/I 的素理想，那么 $\mathfrak{p}$ 是 R 的素理想。

练习 3.3.10. 设 R 是一个含幺交换环，

1. 假设 R 是整环且只有有限个理想，证明 R 是域。

2. 假设 R 只有有限个理想，证明 R 所有的素理想都是极大理想。

3. 假设 R 的所有理想都是素理想，证明 R 是域。

练习 3.3.11. 设 R 是一个含幺交换环且对任意 $x\in R$ 有 $x^2=x$。证明

1. 对任意 $x\in R$ 有 $2x=0$。

2. R 中的所有素理想均是极大理想。

3. R 的所有有限生成的理想均是主理想。

练习 3.3.12. 设 R 是一个含幺交换环，若对任意 $a\in R$ 均存在正整数 $n\geq 2$ 使得 $a^n=a$。证明 R 的所有素理想均是极大理想。

练习 3.3.13. 设 R 是一个含幺交换环，

1. 证明 R 的素理想在包含关系下存在极小元。(提示：*Zorn* 引理)

2. 证明 $\sqrt{(0)}$ 等于 R 的所有素理想的交。

3. 设 I 是 R 的一个理想，证明 $\sqrt{I}$ 是 R 中所有包含 I 的素理想的交。

练习 3.3.14. 设 R 是局部环，$\mathfrak{m}$ 是极大理想，且 $\mathfrak{m}=(a)$ 是主理想。

1. 假设 $\bigcap_{n>0}\mathfrak{m}^n=0$。
   (a) 证明 R 中任意非零元素 x 均能写成 ua^n 的形式，其中 u 是 R 中的单位，$n\in\mathbb{N}$，并且若 R 是整环，那么该表示是唯一的。
   (b) 证明任意理想 I 都形如 (a^n)。
2. 假设 R 是诺特环。
   (a) 设 I 是一个理想使得 $\mathfrak{m}\cdot I=I$，证明 $I=0$。(提示：假设 I 由一组最小数量生成元 $x_1,\dots,x_n$ 生成。)
   (b) 证明 $\bigcap_{n>0}\mathfrak{m}^n=0$。

练习 3.3.15. 设 R 是一个含幺交换环，X 是 R 中所有素理想组成的集合。对 A 的任意子集 E，我们记 $V(E)$ 为 A 中所有包含 E 的素理想组成的集合。

1. 记 I 为 E 生成的理想，证明 $V(E)=V(I)=V(\sqrt{I})$；
2. 证明 $V(0)=X, V(1)=\emptyset$；
3. 设 (E_i) 是 R 的一个子集族，证明 $V(\cup E_i)=\cap V(E_i)$；
4. 设 I,J 是 R 的任意两个理想，证明 $V(I\cap J)=V(IJ)=V(I)\cup V(J)$。

上述结论表明 $V(E)$ 满足闭集公理，由此可以给出集合 X 上的一个拓扑结构，该拓扑被称为 ***Zariski* 拓扑**。拓扑空间 X 也被称为 R 的**素谱**，记作 $\operatorname{Spec}(R)$。

练习 3.3.16. 计算 $\operatorname{Spec}\mathbb{Z}, \operatorname{Spec}\mathbb{R}, \operatorname{Spec}\mathbb{Z}[x], \operatorname{Spec}\mathbb{R}[x]$。

练习 3.3.17. 设 X 是一个有限集，计算 $\operatorname{Spec}\mathcal{P}(X)$，这里 $\mathcal{P}(X)$ 在题3.1.3中定义。

练习 3.3.18. 对任意 $f\in R$，我们记 X_f 为 $V(f)$ 在 $X=\operatorname{Spec}(R)$ 中的补集。

1. 证明 $\{X_f\}_{f\in R}$ 构成 *Zariski* 拓扑的一组开集基；
2. $X_f\cap X_g=X_{fg}$；
3. $X_f=\emptyset \iff f$ 是幂零的；
4. $X_f=X \iff f$ 是单位；
5. $X_f=X_g \iff \sqrt{(f)}=\sqrt{(g)}$；
6. X 是紧集。

练习 3.3.19. 1. 集合 $\{\mathfrak{p}\}$ 是闭集 $\iff \mathfrak{p}$ 是极大理想；
2. $\{\mathfrak{p}\}$ 的闭包是 $V(\mathfrak{p})$；
3. $\mathfrak{p}_1$ 包含在 $\mathfrak{p}$ 的闭包中当且仅当 $\mathfrak{p}\subseteq\mathfrak{p}_1$。

3.4 分式环

这一节我们假设 R 是含幺交换整环，我们的目标是定义 R 的分式环，分式环的一个特例可以得到任意一个整环 R 都能嵌入到域中。若 R 不是整环，它的分式环的构造可参考练习3.4.3。分式环的构造过程和从整数出发构造有理数是一模一样的。首先我们来回顾一下有理数的构造。任何一个有理数都来自于两个整数的商，但是不同的整数的商有可能代表同一个有理数，例如：$\frac{1}{2}=\frac{2}{4}=\frac{3}{6}=\dots$。更一般地，

$$\frac{a}{b}=\frac{c}{d} \iff ad=bc.$$

因此每个有理数 $\frac{a}{b}$ 实际上是有序整数对在等价关系 "$(a,b)\sim(c,d) \iff ad=bc$" 下的等价类。由此我们便可以给出一般的整环上的分式环的构造。

设 D 是 R 中不含 0 的乘法封闭子集，即对任意 $a,b\in D$ 均有 $ab\in D$。那么我们可以构造一个包含 R 的环 Q 使得 D 中元素在 Q 中都是单位。考虑集合

$$\mathcal{S}=\{(a,b)\mid a\in R, b\in D\}.$$

我们在 $\mathcal{S}$ 上定义如下关系：

$$(a,b)\sim(c,d) \iff ad=bc.$$

容易验证该关系满足反身性和对称性。我们下面验证它满足传递性。若 $(a,b)\sim(c,d)$ 且 $(c,d)\sim(e,f)$，那么 $ad=bc, de=cf$。由此可得 $cd(ae-bf)=0$，由于 R 是整环，且 $c,d\neq 0$，因此 $ae=bf$，即 $(a,b)\sim(e,f)$。这意味着上述关系是等价关系。我们记 $Q=\mathcal{S}/\sim$。为了和有理数的记号统一，我们记 $\frac{a}{b}$ 为 (a,b) 所在的等价类。到目前为止，我们已经从集合的角度定义了我们所需要的，接下来我们还需要在这个集合上定义一个环结构，即在 Q 上定义一个加法和乘法，这两个运算的定义也是自然的。设 $\frac{a}{b},\frac{c}{d}\in Q$，我们定义

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\qquad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}. \tag{3.2}$$

定理 3.4.1. *集合 Q 在上述两种运算下构成一个含幺交换环，并且有自然的单同态：*

$$\begin{aligned}\iota:\ R &\longrightarrow Q\\ r &\longmapsto \tfrac{rd}{d},\end{aligned}$$

*其中 d 是 D 中任意一个元素。我们称 Q 为 R 在 D 处的***分式环***，记作 $D^{-1}R$。*

证明. 我们先证明 Q 上的两个运算是定义良好的。若 $\frac{a}{b}\sim\frac{a'}{b'},\frac{c}{d}\sim\frac{c'}{d'}$，我们需要验证

$$\frac{ad+bc}{bd}\sim\frac{a'd'+b'c'}{b'd'}.$$

根据定义有 $ab'=a'b, cd'=c'd$。因此

$$b'd'(ad+bc)-bd(a'd'+b'c')=dd'(ab'-a'b)+bb'(cd'-c'd)=0.$$

由此可得 $\frac{ad+bc}{bd}\sim\frac{a'd'+b'c'}{b'd'}$。乘法的验证也是类似的，我们不再赘叙。容易验证 $\frac{0}{d}$ 是 Q 中的零元，$\frac{d}{d}$ 是 Q 中的单位元。Q 的可交换性来源于 R 的可交换性。因此 Q 是一个定义良好的含幺交换环。

下面我们再证明 φ 是一个定义良好的环同态。对任意 $d_0,d_1\in D$，由于 $\frac{rd_0}{d_0}\sim\frac{rd_1}{d_1}$，因此该映射和 d_0 的选取无关。对任意 $r,s\in R$，我们有 $\frac{rsd_0}{d_0}\sim\frac{rd_0}{d_0}\cdot\frac{sd_0}{d_0}$，即有 $\varphi(rs)=\varphi(r)\varphi(s)$。

最后我们我们证明 φ 是单射。若存在 $r\in R$ 使得 $\frac{rd_0}{d_0}=\frac{0\cdot d_0}{d_0}$，即有 $d(rd_0-0\cdot d_0)=0$，由于 R 是整环，且 $d_0\neq 0$，故必有 $r=0$。因此 φ 是单射。

定理 3.4.2 (分式环的泛性质)**.** 设 $\varphi : R \to S$ 是一个单同态，并且对任意 $d \in D$，$\varphi(d)$ 是 S 中的单位。那么存在单同态 $\Phi : Q \to S$ 使得 $\Phi \circ \iota = \varphi$，即有如下交换图表

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle\iota}\downarrow & \nearrow_{\Phi} & \\ Q & & \end{array}$$

证明. 对任意 $\frac{a}{b} \in Q$，由于 $\varphi(b)$ 是 S 中的单位，因此我们定义 $\Phi(a/b) = \varphi(a)\varphi(b)^{-1}$。我们先验证该定义和代表元 $\frac{a}{b}$ 的选取无关，若 $\frac{a}{b} \sim \frac{c}{d}$，则有 $ad = bc$，因此有

$$\varphi(a)\varphi(d) = \varphi(ad) = \varphi(bc) = \varphi(b)\varphi(c).$$

由于 $\varphi(b), \varphi(d)$ 在 S 中均可逆，因此有 $\Phi(a/b) = \Phi(c/d)$。这便证明了 Φ 是定义良好的。

下面我们再证明 Φ 是一个单同态。对任意 $\frac{a}{b}, \frac{c}{d} \in Q$，我们有

$$\Phi(\frac{a}{b} \cdot \frac{c}{d}) = \Phi(\frac{ac}{bd}) = \varphi(ac)\varphi(bd)^{-1} = \varphi(a)\varphi(c)\varphi(b)^{-1}\varphi(d)^{-1} = \Phi(\frac{a}{b})\Phi(\frac{c}{d}).$$

故 Φ 是一个同态。若存在 $\frac{a}{b} \in Q$ 使得 $\Phi(\frac{a}{b}) = 0$，则有 $\varphi(a) = 0$，由于 φ 是单射，因此 $a = 0$，故 Φ 也是单射。

然后我们再验证 $\Phi \circ \iota = \varphi$。事实上，对任意 $r \in R$，我们有

$$(\Phi \circ \iota)(r) = \Phi(\frac{rd_0}{d_0}) = \varphi(rd_0)\varphi(d_0)^{-1} = \varphi(r).$$

因此有 $\Phi \circ \iota = \varphi$。

推论 3.4.3. 设 R 是一个交换整环，若 $D = R \setminus \{0\}$，那么 $D^{-1}R$ 是一个域，称之为 R 的**分式域**。

证明. 因为 D 中元素在 $D^{-1}R$ 中均可逆，因此 $D^{-1}R$ 中的非零元均是可逆的，故 $D^{-1}R$ 是域。

例 3.4.4. *1.* 若 R 是一个域，那么它的分式域就是 R 自己。

2. $\mathbb{Z}$ 的分式域即为有理数域，而 $\mathbb{Z}[\sqrt{d}]$ 的分式域则为 $\mathbb{Q}(\sqrt{d})$。

3. 有理数域上的多项式环 $\mathbb{Q}[x]$ 的分式域为有理函数域 $\mathbb{Q}(x)$。$\mathbb{Z}[x]$ 的分式域同样也是 $\mathbb{Q}(x)$。

4. 设 $D = \{1, p, p^2, \dots\}$，其中 p 是一个素数，于是 $D^{-1}\mathbb{Z} = \{r = \frac{a}{b} \mid b \text{ 是 } p \text{ 的幂}\}$。

5. $\mathbb{Z}[\sqrt{d}]$ 的分式域为 $\mathbb{Q}(\sqrt{d})$。

6. 设 $\mathfrak{p}$ 是环 R 的一个素理想，那么 $D = R \setminus \mathfrak{p}$ 是一个乘法封闭集，我们记 $R_{\mathfrak{p}} = D^{-1}R$。我们称 $R_{\mathfrak{p}}$ 为 R 在 $\mathfrak{p}$ 处的**局部化**。$R_{\mathfrak{p}}$ 是局部环，$\mathfrak{p}R_{\mathfrak{p}}$ 是 $R_{\mathfrak{p}}$ 唯一的极大理想。特别地，若 $R = \mathbb{Z}$，$\mathfrak{p} = (p)$，其中 p 是素数，那么 $\mathbb{Z}_{\mathfrak{p}}$ 可等同于集合 $\{\frac{n}{m} \mid (m, p) = 1\}$。

7. 设 $R = \mathbb{C}[x]$，那么 $\mathfrak{p} = (x - a)$ 是 R 中的一个素理想。R 在 $\mathfrak{p}$ 处的局部化为

$$R_{\mathfrak{p}} = \left\{ \frac{f(x)}{g(x)} \mid f, g \in R, g(a) \neq 0 \right\}.$$

容易看出，$R_{\mathfrak{p}}$ 即为在点 a 处有定义的有理函数的集合。从几何上来说，$R = \mathbb{C}[x]$ 是在全局都有定义的有理函数，而 $R_{\mathfrak{p}}$ 则只需要在 a 处有定义即可，因此局部化更方便研究函数在某个点处的性质。

最后我们讨论一下分式环中的理想。

定理 3.4.5. 设 R 是一个含幺交换整环，D 是其一个乘法封闭集。

1. $D^{-1}R$ 中的理想均形如 $I(D^{-1}R)$，其中 I 是 R 的理想；
2. $D^{-1}R$ 中的素理想均形如 $\mathfrak{p}(D^{-1}R)$，其中 $\mathfrak{p}$ 是 R 中和 D 不交的素理想。

证明. (1). 若 J 是 $D^{-1}R$ 中的理想，记 $I = J \cap R$。对任意 $x = a/d \in J$，我们有 $a = d \cdot a/d \in J$，故 $a \in J \cap R = I$。因此 $x = a \cdot 1/d \in I(D^{-1}R)$。另一方面显然有 $I(D^{-1}R) \subseteq J$，故 $I(D^{-1}R) = J$。(2). 设 P 是 $D^{-1}R$ 的一个素理想，记 $\mathfrak{p} = P \cap R$。根据定义容易验证 $\mathfrak{p}$ 是素理想。由上面的证明可知 $P = \mathfrak{p}(D^{-1}R)$。由于 P 不含单位元，故 $\mathfrak{p}$ 和 D 不交。反之，若 $\mathfrak{p}$ 是一个和 D 不交的素理想，那么对任意 $\frac{a}{d}, \frac{a'}{d'} \in D^{-1}R$，若有 $\frac{a}{d} \cdot \frac{a'}{d'} \in \mathfrak{p}(D^{-1}R)$，则有

$$aa' = (dd') \cdot \frac{a}{d} \cdot \frac{a'}{d'} \in \mathfrak{p}(D^{-1}R) \cap R = \mathfrak{p}.$$

故 $a \in \mathfrak{p}$ 或 $a' \in \mathfrak{p}$，因此 $a/d \in \mathfrak{p}(D^{-1}R)$ 或 $a'/d' \in \mathfrak{p}(D^{-1}R)$。因此 $\mathfrak{p}(D^{-1}R)$ 是 $D^{-1}R$ 的素理想。

习题

练习 3.4.1. 设 D, S 是环 R 中的两个乘法封闭集且有 $S \subseteq D$。记 $\bar{D}$ 为 D 在 $S^{-1}R$ 中的像，证明 $\bar{D}^{-1}(S^{-1}R) = D^{-1}R$。

练习 3.4.2. 证明局部化可以和商交换顺序。即：设 R 是一个环，D 是 R 的一个乘法封闭集，I 是 R 的一个理想，$\bar{D}$ 是 D 在 R/I 中的像，那么我们有

$$D^{-1}R/I(D^{-1}R) \simeq \bar{D}^{-1}(R/I).$$

练习 3.4.3. 设 R 是任意一个含幺交换环，D 是一个不含 0 的乘法封闭集。下面我们定义它的分式环。我们定义 $R \times D$ 上的关系为

$$(a, b) \sim (c, d) \iff \text{存在 } u \in D \text{ 使得 } (ad - bc)u = 0.$$

1. 证明上述关系是一个等价关系。

   我们定义 $D^{-1}R := (R \times D)/\sim$，我们将 $D^{-1}R$ 中的元素记为 $\frac{a}{b}$，并按照运算(3.2)来定义 $D^{-1}R$ 上的加法与乘法。

2. 证明上述加法与乘法的定义不依赖于代表元的选取，并证明在这两个运算下 $D^{-1}R$ 构成一个含幺交换环。

3. 证明 $D^{-1}R$ 满足定理3.4.2所述的泛性质。

练习 3.4.4. 设 $R = \mathbb{Z}/60\mathbb{Z}$，$\mathfrak{p} = 2R$。计算 $R_{\mathfrak{p}}$ 所含元素个数。

练习 3.4.5. 设 R 是整环，证明 $R = \cap R_{\mathfrak{m}}$，这里交集取 R 的所有极大理想 $\mathfrak{m}$。

练习 3.4.6. 设 R 是一个诺特环，D 是 R 的一个乘法封闭集，证明 $D^{-1}R$ 也是诺特环，诺特环的定义见练习3.2.9。

练习 3.4.7. 设 R 是一个整环，K 是其分式域。若对任意 $x \in K$ 但 $x \notin R$，均有 $x^{-1} \in R$，则称 R 为**赋值环**。若 I, J 赋值环 R 的两个理想，那么我们有 $I \subseteq J$ 或 $J \subseteq I$。由此证明 R 是局部环。

练习 3.4.8. 设 R 是一个赋值环，K 是其分式域。环 R' 满足 $R \subseteq R' \subseteq K$ 且 $R \neq R'$。设 $\mathfrak{m}$ 是 R 的极大理想，$\mathfrak{p}$ 是 R' 的素理想。证明

1. $\mathfrak{p} \subseteq \mathfrak{m} \subseteq R \subseteq R'$ 且 $\mathfrak{m} \neq \mathfrak{p}$；
2. $\mathfrak{p}$ 是 R 的素理想且 $R' = R_{\mathfrak{p}}$。

练习 3.4.9. 设 K 是一个域，R 是一个局部环且满足 $K[x] \subseteq R \subsetneq K(x)$。证明存在不可约多项式 $f(x) \in K[x]$ 使得 $R = K[x]_{(f(x))}$。

3.5 主理想整环

这一节我们均假设环是交换环。

定义 3.5.1. 设 R 是一个整环，若 R 的所有理想都是主理想，那么我们称 R 为**主理想整环**，简记为 PID（Principal ideal domain）。

例 3.5.2. $\mathbb{Z}, \mathbb{Z}[\sqrt{-1}]$ 都是主理想整环，但是 $\mathbb{Z}[\sqrt{-5}]$ 则不是主理想整环，因为 $(3, 1+\sqrt{-5})$ 不是主理想。事实上，若 $(3, 1+\sqrt{-5})$ 是主理想，不妨设 $(3, 1+\sqrt{-5}) = (a+b\sqrt{-5})$。由于 $3 \in (a+b\sqrt{-5})$，故存在 $m+n\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ 使得 $3 = (m+n\sqrt{-5})(a+b\sqrt{-5})$。两边取模长可得 $9 = (m^2+5n^2)(a^2+5b^2)$。由此可得 $m^2+5n^2 = 1, 3$ 或 9，此时可解得 $m = \pm 1$ 或 ± 3，对应的有 $a+b\sqrt{-5} = \pm 3$ 或 ± 1。若 $a+b\sqrt{-5} = \pm 3$，那么我们有 $1+\sqrt{-5} \in (3)$，然而这显然不成立。若 $a+b\sqrt{-5} = \pm 1$，即有 $(3, 1+\sqrt{-5}) = (1)$。但是根据例*3.3.7*中的第六个例子可知 $\mathbb{Z}[\sqrt{-5}]/(3, 1+\sqrt{-5}) \simeq \mathbb{Z}/3\mathbb{Z}$，因此 $(3, 1+\sqrt{-5}) \neq (1)$。故 $(3, 1+\sqrt{-5})$ 不是主理想。

我们可以类似于整数一样定义元素的因子和倍数。

定义 3.5.3. 设 R 是一个交换整环，$a, b \in R$ 且 $b \neq 0$。若存在 $c \in R$ 使得 $a = bc$，那么我们称 a 为 b 的**倍数**，且 b 整除 a，记作 $b \mid a$。若存在元素 $d \in R$ 使得 $d \mid a, d \mid b$ 且对任意同时整除 a, b 的元素 d' 均有 $d' \mid d$，那么我们称 d 为 a, b 的**最大公因子**，记作 $\gcd(a, b)$。

从理想的角度来理解的话，$b \mid a$ 当且仅当 $(a) \subseteq (b)$。若 d 是 a, b 的最大公因子则说明由 a, b 生成的理想 I 一定包含于 (d) 中，且任意包含 I 的主理想均包含 (d)。但是注意到一般而言 I 不一定是主理想的，因此 I 不一定等于 (d)。但是对于主理想整环而言，一切都变得简单了，这使得我们可以像操作数字一样操作理想。

命题 3.5.4. 设 R 是一个主理想整环，$a, b \in R$ 是非零元素。设 $d = \gcd(a, b)$。那么

1. $(d) = (a, b)$；
2. 存在 $x, y \in R$ 使得 $d = ax + by$；
3. d 在相乘 R 的一个单位下是唯一的。

证明. 记 $I=(a,b)$。由于 R 是主理想的，那么存在 $d'\in R$ 使得 $I=(d')$。下面我们证明 d' 是 a,b 的最大公约数。首先由于 $a,b\in I=(d')$，因此 d' 整除 a 和 b。反之，若 d'' 整除 a 和 b，那么 $(d')=I\subseteq(d'')$，即有 d'' 整除 d'。因此根据定义知 d' 是最大公约数。由此证明了 (1)。(2),(3) 由定义可立即得到。

我们前面证明了极大理想都是素理想，通常来说反过来往往都不对，但是对于主理想整环而言反过来也是对的。

命题 3.5.5. 主理想整环的非零素理想均是极大理想。

证明. 设 $I=(a)$ 是 R 的非零素理想，根据定理3.3.2可知存在极大理想 J 包含 I。由于 R 的理想均是主理想，因此不妨设 $J=(b)$。由于 $a\in J$，因此存在 $r\in R$ 使得 $a=br\in I$。由于 I 是素理想，因此比有 $b\in I$ 或者 $r\in I$，若 $b\in I$，那么 $J\subseteq I$，所以 $I=J$ 是极大理想。若 $r\in I$，那么存在 $r'\in R$ 使得 $r=ar'$，所以有 $a=abr'$。由于 R 是整环，所以 $br'=1$，即有 b 是单位，这与 J 是极大理想矛盾。

一般而言，要判断一个具体的环是否是主理想整环并不是一件容易的事，但是有一类环可以比较容易判定是主理想整环，这类环被称为欧几里得整环。

定义 3.5.6. 设 R 是一个交换环，若存在函数 $\varphi:A\setminus\{0\}\to\mathbb{N}$ 使得对任意 $a,b\in R\setminus\{0\}$ 均存在 $q,r\in R$ 使得 $a=bq+r$ 并且要么 $r=0$ 要么 $\varphi(r)<\varphi(b)$，那么我们称 R 是**欧几里得环**。

可以看出欧几里得环中的条件其实就是我们熟知的带余除法的推广，因此我们熟知的一些环均是欧几里得环。

例 3.5.7. *1.* 域显然是一个欧几里得环，对应的函数 φ 取常值函数 1 即可。

2. 整数环是欧几里得环，其对应的函数为 $\varphi(n)=|n|$；

3. 设 F 是一个域，那么 $F[x]$ 是欧几里得环，其对应的函数是 $\varphi(f)=\deg f$。对此，我们可以对 $n=\deg f$ 进行归纳，我们记 $\deg g=m$。当 $n=0$ 时，若 $m=0$，那么取 $q(x)=f(x)/g(x),r(x)=0$ 即可，若 $m>0$，那么取 $q(x)=0,r(x)=f(x)$ 即可。下面假设 $n>0$，若 $m>n$，那么同样取 $q(x)=0,r(x)=f(x)$ 即可。若 $m\leq n$，不妨设 $f(x),g(x)$ 的首项系数分别为 a,b，再设 $h(x)=f(x)-\frac{a}{b}x^{n-m}g(x)$，那么 $\deg h<\deg f$，根据归纳假设知存在 $q_1(x),r_1(x)$ 使得 $h(x)=q_1(x)g(x)+r_1(x)$，并且 $r_1(x)=0$ 或 $\deg r_1<m$。于是取 $q(x)=\frac{a}{b}x^{n-m}+q_1(x),r(x)=r_1(x)$，根据定义知 $f(x)=q(x)g(x)+r(x)$。

4. 设设 F 是一个域，对于 $f(x)\in F[\![x]\!]$，我们设 n 是使得 $f(x)$ 中 x^n 前系数不为 0 的最小整数，记作 $\mathrm{ord}(f)$。那么 $F[\![x]\!]$ 是欧几里得环，其对应的函数为 $\mathrm{ord}(f)$。事实上，我们可以证明一个更强的结论：对任意 $f(x),g(x)\in F[\![x]\!]$，$\mathrm{ord}(f)\leq\mathrm{ord}(g)$ 当且仅当 f 整除 g。不妨设 $\mathrm{ord}(f)=n\leq\mathrm{ord}(g)=m$，那么存在常数项不是 0 的形式幂级数 $f_1(x),g_1(x)$ 使得 $f(x)=x^nf_1(x),g(x)=x^mg_1(x)$。根据命题3.1.7可知 f_1,g_1 均为 $F[\![x]\!]$ 中的单位。因此

$$g(x)=f(x)\left(x^{m-n}f_1(x)^{-1}g_1(x)\right).$$

故 $f(x)$ 整除 $g(x)$。反之若 $f(x)$ 整除 $g(x)$，那么存在 $h(x)\in F[\![x]\!]$ 使得 $g(x)=f(x)h(x)$。根据定义可以直接得到 $\mathrm{ord}(g)=\mathrm{ord}(f)+\mathrm{ord}(h)\geq\mathrm{ord}(f)$。

5. 对于 $d=-1,\pm 2$，环 $\mathbb{Z}[\sqrt{d}]$ 均为欧几里得环，其对应的函数为 $\varphi(m+n\sqrt{d})=|N(m+n\sqrt{d})|=|m^2-dn^2|$。我们首先证明对任意 $t\in\mathbb{Q}(\sqrt{d})$，均存在 $q\in\mathbb{Z}[\sqrt{d}]$ 使得 $|N(t-q)|<1$。设 $t=x+y\sqrt{d}$，其中 $x,y\in\mathbb{Q}$。易知存在整数 u,v 使得 $|u-x|,|v-y|\leq\frac{1}{2}$。取 $q=u+v\sqrt{d}\in\mathbb{Z}[\sqrt{d}]$，于是我们有

$$|N(t-q)|\leq(x-u)^2+|d|(y-v)^2\leq\frac{1+|d|}{4}<1.$$

因此对任意 $a,b\in\mathbb{Z}[\sqrt{d}]$ 且 $a,b\neq 0$，令 $t=\frac{a}{b}$，根据前面的证明可知存在 $q\in\mathbb{Z}[\sqrt{d}]$ 使得 $|N(a/b-q)|<1$，即有 $|N(a-bq)|<N(b)$，我们取 $r=a-bq$ 即满足条件。

更一般地，可以证明对于上述的函数 φ，$\mathbb{Z}[\sqrt{d}]$ 是欧几里得环当且仅当 $d=-2,-1,2,3,6,7,11,19$。但是是否存在其它的函数使得 d 取其它数时仍然时欧几里得环呢？答案是未知的！一个猜想是存在无穷个正整数 d 使得 $\mathbb{Z}[\sqrt{d}]$ 是欧几里得环。*Harper*[1]证明了 $\mathbb{Z}[\sqrt{14}]$ 是欧几里得环。

命题 3.5.8. 欧几里得整环都是主理想整环。

证明. 我们只需证明 R 的任意一个非零理想 I 是主理想即可。假设 φ 是使得 R 成为欧几里得环的函数。由于 $\varphi(I\setminus\{0\})$ 是 $\mathbb{N}$ 的非空子集，取 $b\in I\setminus\{0\}$ 使得 $\varphi(b)$ 最小，显然有 $(b)\subseteq I$。反之，对任意 $a\in I$，存在 $q,r\in R$ 使得 $a=bq+r$ 且 $\varphi(r)<\varphi(b)$ 或者 $r=0$。但是由于 $r=a-bq\in I$，由 $\varphi(b)$ 的最小性可知必有 $r=0$，即有 $a=bq\in(b)$。故 $I=(b)$ 是主理想。

根据前面的讨论立刻可以得到如下结论。

推论 3.5.9. 环 $\mathbb{Z},\mathbb{Z}[\sqrt{-1}],\mathbb{Z}[\sqrt{-2}],\mathbb{Z}[\sqrt{2}],F[x],F[\![x]\!]$ 都是主理想整环，其中 F 是一个域。

注 9.

1. 可以证明当 $d<-2$ 时，$\mathbb{Z}[\sqrt{d}]$ 均不是主理想整环，见练习3.6.6。另一方面，当 $d>0$ 时，确定 $\mathbb{Z}[\sqrt{d}]$ 是否是主理想整环则是一个公开问题。可以证明当 $d=2,3,6,7,11,14,19,22,23,31$ 等数时，$\mathbb{Z}[\sqrt{d}]$ 都是主理想的。更多的例子可见这里[2]。

2. 若 R 是一个交换环，那么 $R[x]$ 是主理想整环当且仅当 R 是一个域。事实上，由于 $R[x]$ 是主理想整环，R 必定是整环。另一方面注意到 (x) 是 $R[x]$ 的非平凡的素理想，由命题3.5.5可知 (x) 是极大理想，所以 $R\simeq R[x]/(x)$ 是一个域。

习题

练习 3.5.1. 在环 $\mathbb{Z}[\sqrt{-1}]$ 中求最大公约数。

$$(1).\ 11+7\sqrt{-1},4+7\sqrt{-1}\qquad\qquad(2).\ 3+4\sqrt{-1},18-\sqrt{-1}.$$

练习 3.5.2. 设 R 是 PID，$\mathfrak{p}$ 是 R 的素理想。证明 $R/\mathfrak{p}$ 也是 PID。

练习 3.5.3. 设 R 是 PID，D 是 R 的一个乘法封闭集，证明 $D^{-1}R$ 也是 PID。

练习 3.5.4. 设 $R=\{x\in\mathbb{Q}\mid$ 存在 $n\in\mathbb{Z}$ 使得 $10^nx\in\mathbb{Z}\}$。证明 R 是主理想整环。

练习 3.5.5. 设 $R=\mathbb{Z}[\sqrt{-5}]$，记 $I_2=(2,1+\sqrt{-5})$，$I_3=(3,2+\sqrt{-5})$，$I_3'=(3,2-\sqrt{-5})$。

[1] M. Harper, $\mathbb{Z}[\sqrt{-14}]$ *is Euclidean*, Canad. J. Math. Vol. 56 (1), 2004 pp. 55–70.

[2] https://oeis.org/A003172.

1. 证明 I_2, I_3, I_3' 都不是 R 的主理想。
2. 证明 $I_2^2 = (2)$。
3. 证明 $I_2 I_3 = (1-\sqrt{-5}), I_2 I_3' = (1+\sqrt{-5})$。
4. 证明 I_2, I_3, I_3' 都是素理想。

练习 3.5.6. 证明 A_{-3}, A_{-7}, A_{-11} 均为欧几里得整环，对应的函数为

$$N(m+n\tau_d) = (m+n\tau_d)(m+n\overline{\tau_d}) = m^2 + mn + \frac{1-d}{4}n^2,$$

其中 A_d 的定义见练习3.1.4。

练习 3.5.7. 设 R 是一个整环，且 R 的所有素理想均是主理想。本题的目标是证明 R 是主理想整环。

1. 记 R 中所有不是主理想的理想组成的集合为 S，假设 S 非空，利用 *Zorn* 引理证明在包含关系下 S 存在极大元。
2. 设 $I \in S$ 是一个极大元。根据假设知 I 不是素理想，因此不妨设 $a, b \in R$ 使得 $ab \in I$ 但 $a, b \notin I$。记 I_a 为由 I 和 a 生成的理想，I_b 为由 I 和 b 生成的理想。记 $J = \{r \in R \mid rI_a \subseteq I\}$。证明 $I_a = (\alpha), J = (\beta)$ 均为主理想，且 $I \subsetneq I_b \subseteq J$ 及 $I_a J = (\alpha\beta) \subseteq I$。
3. 设 $x \in I$ 证明存在 $s \in J$ 使得 $x = \alpha s$。由此证明 $I = I_a J$ 是主理想。

练习 3.5.8. 证明赋值环中有限生成的理想都是主理想。(赋值环的定义见习题3.4.7)

练习 3.5.9. 设 R 是一个含幺交换整环，对任意非零理想 $I, J \subset R$，若存在非零元素 $a, b \in R$ 使得 $aI = bJ$，则称 I 和 J 等价，记作 $I \sim J$。

1. 证明上述关系在全体非零理想的集合上定义了一个等价关系。我们记其商集为 $\mathrm{Cl}(R)$。
2. 证明非零理想 I 是主理想当且仅当它和 R 等价。
3. 证明 A 是主理想整环当且仅当 $|\mathrm{Cl}(R)| = 1$。

练习 3.5.10. 设 $R = \mathbb{Z}[\sqrt{d}]$，其中 $-7 \leq d \leq -3$。

1. 设 $0 < t < 1 + \sqrt{3}$。证明对任意 $z \in \mathbb{C}$ 存在 $v \in \mathbb{Z} + \mathbb{Z}it$ 使得 $|z - v| < 1$ 成立或者 $|z - v/2| < 1/2$ 成立。
2. 证明对任意 $a, b \in R$，$b \neq 0$，存在 $q, r \in R$ 且 $N(r) < N(b)$ 使得 $a = qb + r$ 成立或者 $2a = qb + r$ 成立。
3. 证明 R 的任意非零理想均和一个包含 $2R$ 的理想等价。
4. 证明 R 中包含 $2R$ 的理想只有 $2R, J, R$ 三个，其中 $J = (2, \alpha)$，当 d 是偶数时，$\alpha = \sqrt{d}$，当 d 是奇数时，$\alpha = 1 + \sqrt{d}$。
5. 证明 $\mathrm{Cl}(R) = \{[R], [J]\}$ 并且 J 和 R 不等价。

练习 3.5.11. 本题的目标是证明当 $d < -11$ 时，A_d 不是欧几里得整环。

1. 假设 R 是欧几里得整环但不是域，证明存在不是单位的非零元 $x \in R$ 使得自然映射 $R^* \cup \{0\} \to R/xR$ 是满射。
2. 证明当 $d < -11$ 时，A_d 中不存在元素 z 使得 $N(z) = 2$ 或 3。
3. 证明原结论。

练习 3.5.12. 设 R 是一个主理想整环，K 是其分式域。本题的目标是刻画 $R[x]$ 的所有素理想和极大理想。设 I 是 $R[x]$ 的一个非零素理想。

1. 证明当 $I \cap R \neq 0$ 时，$I \cap R$ 是 R 的极大理想。
2. 我们先假设 $I \cap R = 0$。
   (a) 设 J 是 $K[x]$ 中由 I 生成的理想。证明 $I = J \cap R[x]$。
   (b) 证明 I 是主理想，并且由一个次数大于 1 的本原不可约多项式生成。
3. 下面我们假设 $I \cap R$ 是非零的。记 $k = R/(I \cap R)$。证明 I 要么是由 $I \cap R$ 生成的，要么是由 $I \cap R$ 及某个多项式 $P(x) \in R[x]$ 生成，其中 $P(x)$ 在 $k[x]$ 中的像是不可约的。
4. 确定上述素理想中哪些是极大理想。

练习 3.5.13. 设 R 是一个交换环。我们通过如下递推方式定义 R 的一个子集列 $\{R_n\}_{n\geq 0}$：$R_0 = \emptyset$，$R_{n+1} = \{a \in R \mid aR + R'_n = R\}$，其中 $R'_n = R_n \bigcup \{0\}$。考虑如下映射：

$$\begin{array}{rccc} \phi\colon & \bigcup_{n\geq 0} R_n & \longrightarrow & \mathbb{N} \\ & a & \longmapsto & \min\{k \geq 0 \mid a \in R_{k+1}\}. \end{array}$$

1. 证明 $R_1 = R^*$ 并且 $R_1 \subseteq R_2 \subseteq R_3 \subseteq \ldots$。
2. 假设 R 在函数 φ 下构成欧几里得环，证明对任意 $a \in R$ 有 $\phi(a) \leq \varphi(a)$ 且 $\bigcup R'_n = R$。
3. 若 $\bigcup R'_n = R$，证明 R 在函数 ϕ 下构成一个欧几里得环。

3.6 唯一分解整环

我们知道整数都能唯一分解成若干个素数的乘积。我们可以将这个性质抽象出来得到所谓的唯一分解整环。为此我们需要引入不可约元和素元的概念。

定义 3.6.1. 设 R 是一个整环，$0 \neq r \in R$ 不是单位元。若存在两个非单位元 $a, b \in R$ 使得 $r = ab$，那么我们称 r 是**可约的**，否则称 r 是**不可约的**。设 $0 \neq p \in R$，若 (p) 是 R 中的素理想，那么则称 p 为**素元**。

命题 3.6.2. 在整环中，素元一定是不可约的。

证明. 设 $p \in R$ 是素元，若 p 是可约的，那么存在非单位元 $a, b \in R$ 使得 $ab = p \in (p)$。由于 (p) 是素理想，故 a, b 之一必属于 (p)，不妨设 $a \in (p)$，那么存在 $r \in R$ 使得 $a = pr$，由此我们有 $p = ab = pbr$，由于 R 是整环，故 $br = 1$，这与 b 不是单位矛盾。

然而上述结论的逆命题却不一定是对的。例如 $R=\mathbb{Z}[\sqrt{-5}]$，元素 3 在 R 中是不可约的，但 (3) 却不是素理想，因为 $(2+\sqrt{-5})(2-\sqrt{-5})=9\in(3)$，但 $2\pm\sqrt{-5}\notin(3)$。但是对于特殊的环，我们可以证明两者是等价的。

命题 3.6.3. *设 R 是 PID，那么非零元素 $a\in R$ 是素元当且仅当它是不可约的。*

证明. 我们只需证明不可约元是素元即可。假设 p 是不可约的，但不是素元，那么存在 a,b 使得 p 整除 ab，且 p 不整除 a 和 b。设 d 为 p 和 a 的最大公约数，于是存在 $q\in R$ 使得 $p=dq$，根据假设可知 d 和 q 有一个是单位，若 q 是单位，那么 d 整除 a 意味着 p 整除 a，与假设矛盾。因此 d 是单位。根据命题3.5.4可知存在 $r,s\in R$ 使得 $1=ar+ps$。两边同时乘以 b 可得 $b=abr+pbs$。由 p 整除 ab 可知 p 整除 $abr+pbs=b$，这与假设矛盾。所以 p 是素元。

定义 3.6.4. 设 R 是一个整环，若对任意 $r\in R$ 均存在不可约元 $p_1,\dots,p_n$ 及单位 u 使得 $r=up_1\cdots p_n$，并且若 $r=vq_1\cdots q_m$ 是另一个不可约分解，那么一定有 $n=m$，且存在单位 u_i 使得在某个顺序下有 $p_i=u_iq_i$，那么我们称 R 为**唯一分解整环**，简称为 UFD（Unique Factorization Domain）。

下面我们证明本节最重要的一个结论，即 PID 一定是 UFD。这意味着对 PID 中的元素求最大公因子均可采用上述方法。

定理 3.6.5. *主理想整环一定是唯一分解整环。*

证明. 首先我们需要证明分解的存在性，如果 x 是单位或者素元，那么结论自然成立了。下面我们假设 x 既不是单位也不是素元，根据引理3.6.3可知存在非单位元 a,b 使得 $x=ab$。同样地，如果 a,b 是素元，则不需要继续分解，否则的话再次利用引理3.6.3可知它们能分解成两个非单位元的乘积。我们需要证明这个过程一定会在有限步后停止，即有限步之后均只能得到素元，从而不能再继续分解。否则我们假设有这样一个严格的理想升链

$$(x)\subset(a_1)\subset(a_2)\subset\dots,$$

首先注意到 $I=\cup(a_i)$ 仍是一个理想。由于 R 是主理想整环，故存在 $a\in R$ 使得 $I=(a)$。特别地，存在整数 n 使得 $a\in(a_n)$。所以 $I\subset(a_n)$，但根据定义显然有 $(a_n)\subset I$，因此必有 $I=(a_n)$。从而有 $(a_n)=(a_{n+1})=\dots$，这与上述理想升链是严格的矛盾。因此 x 必然能分解成有限个素元的乘积。

结合推论3.5.9立刻可以得到如下结论。

推论 3.6.6. *环 $\mathbb{Z},\mathbb{Z}[\sqrt{-1}],\mathbb{Z}[\sqrt{-2}],\mathbb{Z}[\sqrt{2}],F[x],F[\![x]\!]$ 都是唯一分解整环，其中 F 是一个域。*

和整数的情况类似，对于主理想整环中的两个元素，我们可以通过将它们分解为不可约元的乘积来计算它们的最大公约数。

推论 3.6.7. *设 ,b 是唯一分解整环 R 中的两个非零元素，并假设*

$$a=up_1^{k_1}\cdots p_n^{k_n},\qquad b=vp_1^{s_1}\cdots p_n^{s_n},$$

其中 u,v 是 R 中的单位，p_i 是 R 中互不相同的不可约元。那么

$$d=(a,b)=p_1^{\min(k_1,s_1)}\cdots p_n^{\min(k_n,s_n)}.$$

证明. 根据定义显然有 $d \mid a$ 及 $d \mid b$。反之，若 d' 同时整除 a, b，不妨设 $d' = u' p_1^{t_1} \cdots p_n^{t_n}$，设 $c \in R$ 且 $a = d'c$，再设 $c = v' p_1^{\ell_1} \cdots p_n^{\ell_n}$。由于 a 的分解唯一，因此我们有 $k_i = t_i + \ell_i$。特别地有 $t_i \leq k_i$。同理有 $t_i \leq s_i$。于是有 $t_i \leq \min(k_i, s_i)$。因此 d' 整除 d。故 d 是 a, b 的最大公约数。

一般而言，在 UFD 中将元素分解为不可约元的乘积并不是一件简单的事，例如在环 $\mathbb{C}[x]$ 中分解等价于求多项式的所有根，而在 $\mathbb{Q}[x]$ 中分解则需要计算多项式在有理数域上的不可约因子，其计算量通常都比较大，因此利用唯一分解来计算两个元素的最大公约数只是理论上的结果，实际操作我们需要其它更加有效的方法。另外注意到定理3.6.5的逆命题是不对的，一个经典的例子是 $\mathbb{Z}[x]$。

例 3.6.8. 根据高等代数中的结论我们知道 $\mathbb{Z}[x]$ 是唯一分解整环，但是根据注 *9* 可知 $\mathbb{Z}[x]$ 不是主理想整环。更具体地，我们可以证明理想 $I = (2, x)$ 不是主理想。事实上，若 $(2, x)$ 是主理想，不妨设它由 $f(x)$ 生成。由于 $2 \in (2, x) = (f(x))$，因此存在多项式 $g(x)$ 使得 $2 = f(x)g(x)$。两边对比次数可知必有 $\deg f = \deg g = 0$，即 $f(x), g(x)$ 均为常数多项式。由于 $f(x), g(x)$ 均是整系数的，故 $f(x)$ 只能为 $\pm 1, \pm 2$。若 $f(x) = \pm 1$，由于 $f(x) \in (2, x)$，因此存在多项式 $h_1(x), h_2(x) \in \mathbb{Z}[x]$ 使得 $\pm 1 = f(x) = 2h_1(x) + xh_2(x)$。对比等式两边的常数项可知不成立。若 $f(x) = \pm 2$，由于 $x \in (2, x) = (f(x))$，因此存在 $r(x) \in \mathbb{Z}[x]$ 使得 $x = f(x)r(x) = \pm 2r(x)$。对比等式两边 x 前的系数可知不成立。因此 $(2, x)$ 不是主理想。

例 3.6.9. 不是 *UFD* 的最经典的例子是 $R = \mathbb{Z}[\sqrt{-5}]$。因为在 R 中有 $6 = 2 \times 3 = (1 + \sqrt{-5}) \times (1 - \sqrt{-5})$，而 $2, 3, 1 \pm \sqrt{-5}$ 在 R 中均为不可约元。环 $R' = \mathbb{C}[x, y, z, w]/(xy - zw)$ 同样也不是 *UFD*，因为在 R' 中有 $xy = zw$。

最后我们指出命题3.6.3对 UFD 也成立。

命题 3.6.10. 设 R 是 *UFD*，那么 $0 \neq p \in R$ 是素元当且仅当 p 是不可约元。

证明. 若 $p \neq 0$ 是素元，根据命题3.6.2可知 p 一定是不可约元。反之，设 p 是不可约元，若存在 $a, b \in R$ 使得 $ab \in (p)$，则不妨设 $c \in R$ 使得 $ab = pc$。将 a, b 写成不可约元的乘积，$a = p_1 \cdots p_s, b = q_1 \cdots q_t$，由于 p 是不可约元并且 ab 的分解是唯一的，于是存在某个整除 a 或 b 的不可约元，使得它和 p 相差一个单位的倍数，不妨设为 p_1，再设 $u \in R^*$ 使得 $p_1 = up$。这意味着 $a = p \cdot up_2 \cdots p_s \in (p)$，即有 p 是素元。

习题

练习 3.6.1. 将 $10, 7 + \sqrt{-1}, 6 + 9\sqrt{-1}$ 在环 $\mathbb{Z}[\sqrt{-1}]$ 中分解为不可约元的乘积。

练习 3.6.2. 设 $R = \mathbb{Z}[\sqrt{-5}]$，证明 $2, 3, 1 + \sqrt{-5}$ 和 $1 - \sqrt{-5}$ 是 R 中的不可约元。

练习 3.6.3. 设 R 是 *UFD*，D 是 R 的一个乘法封闭集，证明 $D^{-1}R$ 也是 *UFD*。

练习 3.6.4. *1.* 找一个元素 $f(X) \in \mathbb{Z}[X]$ 使得它在 $\mathbb{Z}[X]$ 中可约，但是在 $\mathbb{Z}[\![X]\!]$ 中不可约；

2. 找一个元素 $f(X) \in \mathbb{Z}[X]$ 使得它在 $\mathbb{Z}[X]$ 中不可约，但是在 $\mathbb{Z}[\![X]\!]$ 中可约；

练习 3.6.5. 证明 $R = \mathbb{R}[x, y]/(x^2 + y^2 - 1)$ 不是 *UFD*，但 $S = \mathbb{C}[x, y]/(x^2 + y^2 - 1)$ 是 *PID*。(提示：证明 x 是 R 中的不可约元，但不是素元。)

练习 3.6.6. 本题的目标是证明当 $d<-2$ 时，环 $\mathbb{Z}[\sqrt{d}]=\mathbb{Z}+\mathbb{Z}\sqrt{d}$ 都不是 *PID*。

1. 当 $d=-3$ 或 -4 时，通过找一个不是唯一分解的元素来证明 $\mathbb{Z}[\sqrt{d}]$ 不是 *PID*。
   下面当 d 是偶数时，假设 $\alpha=\sqrt{d}$，当 d 是奇数时，设 $\alpha=1+\sqrt{d}$。
2. 当 $d<-4$ 时，列举出所有元素 $z\in\mathbb{Z}[\sqrt{d}]$ 使得 $|z|^2$ 整除 4。
3. 证明 $(2,\alpha)=2\mathbb{Z}+\alpha\mathbb{Z}$。
4. 证明 $(2,\alpha)$ 不是主理想。

练习 3.6.7. 设 $\rho=\mathrm{e}^{\frac{2\pi i}{3}}$，并记 $\mathbb{Z}[\rho]=\{a+b\rho\mid a,b\in\mathbb{Z}\}$。

1. 证明 $\mathbb{Z}[\rho]$ 在通常的加法与乘法下构成一个环。
2. 证明 $(\mathbb{Z}[\rho])^*=\{\pm1,\pm\rho,\pm\rho^2\}$。
3. 证明 $\mathbb{Z}[\rho]$ 是欧几里得环，其对应的函数为 $\varphi(z)=|z|^2$。
4. 设 p 是模 3 余 1 的素数，
   (a) 证明存在 $\mathbb{Z}[\rho]$ 中的不可约元 r 及 $\bar{r}$ 使得 $p=r\bar{r}$。
   (b) 证明恰好存在 12 对整数 $(a,b)\in\mathbb{Z}^2$ 使得 $p=a^2+ab+b^2$。
   (c) 证明存在唯一的正整数对 $(a,b)\in\mathbb{N}^2$ 使得 $p=a^2+3b^2$。

练习 3.6.8. 本题的目标是证明 $R=\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ 是主理想整环但不是欧几里得环。

1. 证明对任意 $z\in R$，均有 $|z|^2\in\mathbb{Z}$。
2. 列出所有满足 $|z|^2\leq 9$ 的元素。由此给出 R 中的单位，并证明 2 和 3 都是不可约元。
3. 证明 R 不是欧几里得环。
4. 下面均设 I 是 R 的一个非零理想，且 w 是 I 中范数最小的元素。设 $z\in I$。证明存在 $b\in R$ 使得 $z/w-b$ 的虚部的绝对值小于 $\frac{\sqrt{19}}{4}$。
5. 若 $z/w-b$ 的虚部的绝对值小于 $\frac{\sqrt{3}}{2}$，证明 $z/w-b$ 到某个整数的距离严格小于 1，由此证明 $z\in(w)$。
6. 若 $z/w-b$ 的虚部的绝对值不小于 $\frac{\sqrt{3}}{2}$，证明 z 或 $2z$ 在 (w) 中。由此证明 I 是主理想。

练习 3.6.9. 设 R 是一个整环。若存在函数 $f:R\setminus\{0\}\to\mathbb{N}$ 使得对任意 $a,b\in R\setminus\{0\}$，要么有 $b\mid a$ 要么存在 $c\in aR+bR$ 使得 $f(c)<f(a)$，我们则称 R 是**几乎欧几里得整环**。

1. 证明若 R 是几乎欧几里得整环，那么 R 是主理想整环。
2. 假设 R 是主理想整环，记 $f:R\setminus\{0\}\to\mathbb{N}$ 为元素 r 的素因子个数。证明 R 是几乎欧几里得整环。

练习 3.6.10. 设 R 是一个唯一分解整环，且对任意非零元 $a\in R$，R/aR 均是有限集。

1. 证明 R 是诺特环。

2. 若 $a \in R$ 是素元，证明 aR 是极大理想。

3. 设 I 是 R 的一个极大理想，证明存在素元 $a \in R$ 使得 $I = aR$。

4. 设 $a \in R$ 既不是零元也不是单位，I 是 R 的一个非零理想，证明 $aI \subsetneq I$。

5. 证明 R 是主理想整环。

3.7 多项式环

这一节我们继续探讨关于多项式环的相关结论。如前所示，域上的多项式环性质很好，它们均是主理想整环。而一般环上的多项式环则不会有如此性质。对于 UFD 和诺特环，我们有如下结论。

定理 3.7.1. *R 是 UFD 当且仅当 $R[x]$ 是 UFD。*

该定理的证明和域的情况类似，我们先证明如下 Gauss 引理：

引理 3.7.2. *设 R 是 UFD，其分式域为 F。设 $f(x) \in R[x]$，若 $f(x)$ 作为 F 上的多项式是可约的，那么 $f(x)$ 在 R 上也可约。*

证明. 假设在 F 上 $f(x)$ 可分解为 $f(x) = g(x)h(x)$。我们不妨设 $a, b \in R$ 使得 $ag(x), bh(x) \in R[x]$。若 ab 是 R 中的单位，那么 a, b 均为 R 中的单位，故 $g(x), h(x) \in R[x]$。若 ab 不是单位，那么将其分解为不可约元的乘积 $ab = p_1 p_2 \cdots p_s$。由于 p_1 是不可约元，因此由命题3.6.10可知 (p_1) 是素理想。由例3.2.11知 $R[x]/p_1R[x] \simeq (R/(p_1))[x]$，而后者是整环。因此 $p1R[x]$ 是 $R[x]$ 中的素理想，我们对 $abf(x) = (ag(x))(bh(x))$ 两边取模 p_1 可知在整环 $(R/(p1))[x]$ 中有等式 $0 = \overline{ag(x)bh(x)}$。故 $\overline{ag(x)}, \overline{bh(x)}$ 中至少有一个是零多项式，不妨设为 $\overline{ag(x)}$。而 $\{olag(x)$ 是零多项式当且仅当其系数在 $R/(p_1)$ 中均为 0，即 $ag(x)$ 的系数均是 p_1 的倍数。因此 $\frac{a}{p_1}g(x)$ 仍是 $R[x]$ 中的多项式。由此我们得到 $p_2 \cdots p_s f(x) = \frac{a}{p_1}g(x)bh(x)$。我们依次对 $p_2, \ldots, p_s$ 进行上述操作便可以证明 $p(x)$ 能写成 $R[x]$ 中两个多项式的乘积，因此 $f(x)$ 在 $R[x]$ 中也是可约的。

设 $f(x) \in R[x]$，若不存在素元 p 使得 p 整除 $f(x)$ 的所有系数，那么我们称 $f(x)$ 是**本原的**。

定理3.7.1的证明. 设 $f(x) \in R[x]$，我们先证明 $f(x)$ 能分解为不可约多项式的乘积。首先我们假设 $f(x)$ 的系数的最大公因数是 1。若 $\deg f = 0$，那么 $f(x)$ 即为 R 中的单位，结论成立。下面假设 $\deg f > 0$，我们先假设 $f(x)$ 是本原的。设 F 是 R 的分式域，由推论3.6.6知 $F[x]$ 是 UFD，因此存在不可约多项式 $f_1(x), \ldots, f_s(x) \in F[x]$ 使得 $f(x) = f_1(x) \cdots f_s(x)$。根据 Gauss 引理知 $f(x)$ 在 R 上也能分解为若干个不可约多项式的乘积。

下面证明唯一性。假设

$$f(x) = f_1(x) \cdots f_s(x) = g_1(x) \cdots g_t(x),$$

其中 f_i, g_i 都是 $R[x]$ 中的不可约元。由于 $f(x)$ 是本原的，容易知道 f_i, g_i 都是本原的。将 f, f_i, g_i 视作 $F[x]$ 中的元素，由 Gauss 引理知 f_i, g_i 在 $F[x]$ 也是不可约的。由于 $F[x]$ 是 UFD，因此我们必有 $s = t$，并且在调整一定的顺序后，$f_i(x)$ 和 $g_i(x)$ 只相差 F 中的一个常数。设 $f_i(x) = \frac{b_i}{a_i}g_i(x)$，其中 $a_i, b_i \in R$，并且 a_i, b_i 互素。由于 f_i 和 g_i 都是本原的，因此容易知道 a_i, b_i 只能是 R 中的单位。这表明 $f(x)$ 在 $R[x]$ 中是唯一分解的。

最后若 $f(x)$ 不是本原的，不妨设 a 是其所有系数的最大公约数，那么 $f(x)/a$ 是本原的。根据上面的证明知 $f(x)/a$ 是唯一分解的。而 R 是 UFD，因此 a 能唯一分解为有限个不可约元的乘积。综上可知 $f(x)$ 可唯一分解为 $R[x]$ 中有限个不可约元的乘积。

最后我们证明著名的 Hilbert 基定理。它表明从一个诺特环出发，我们可以不断的构造出新的诺特环，关于诺特环的定义见练习3.2.9。

定理 3.7.3. *设 R 是一个诺特环，那么 $R[x]$ 也是诺特环。*

证明. 设 I 是 $R[x]$ 中的一个理想，再设 J 为 I 中元素的首项系数组成的集合。我们先证明 J 是 R 的一个理想。由于 I 包含零多项式，因此 $0 \in J$。对任意 $a, b \in J$ 及 $r \in R$，不妨设 a, b 分别是 $f(x), g(x) \in I$ 的首项系数，并设 $\deg f = n, \deg g = m$，由于 I 是 $R[x]$ 中的理想，因此 $f(x) \cdot (rx^m) - g(x) \cdot (x^n) \in I$，而直接计算可知当 $ar - b \neq 0$ 时，$ar - b$ 恰好是多项式 $f(x) \cdot (rx^m) - g(x) \cdot (x^n)$ 的首项系数，因此根据定义有 $ar - b \in J$。故 J 是 R 的理想。

根据假设条件知 J 是有限生成的，不妨设 $J = (a_1, a_2, \ldots, a_s)$。设 a_i 是 I 中多项式 f_i 的首项系数，f_i 的次数为 n_i。记 $N = \max\{n_1, \ldots, n_s\}$，对每一个 $0 \leq d \leq N$，记 J_d 为 I 中所有次数为 d 的多项式的首项系数和 0 的并。同样可以证明 J_d 是 R 的一个理想，因此它也是有限生成的，不妨设 $J_d = (a_{d1}, \ldots, a_{ds_d})$。设 $f_{d,i}$ 是 I 中首项系数等于 a_{di} 的元素。记 I' 为由 $\{f_j, f_{d,i} \mid 1 \leq j \leq s, 0 \leq d \leq N, 1 \leq i \leq s_d\}$ 生成的理想。下面我们证明 $I = I'$

若 $I \neq I'$，那么我们取 $f \in I \setminus I'$ 使得 f 的次数最低，再记 f 的首项系数为 a。若 $\deg f \geq N$，那么由 J 的定义可知存在 $r_i \in R$ 使得 $a = a_1 r_1 + \cdots + a_s r_s$，于是 $f - r_1 x^{N-n_1} f_1 - \cdots - r_s x^{N-n_s} f_s$ 仍然不在 I' 中，并且次数比 f 低，这与 $\deg f$ 的最小性矛盾。

若 $\deg f < N$，设 $\deg f = d$，那么根据 J_d 的定义知存在 $r_i \in R$ 使得 $a = a_{d1} r_1 + \cdots + a_{ds_d} r_{s_d}$，同上可考虑 $f - r_1 f_{d,1} - \cdots - r_{s_d} f_{d,s_d}$，该多项式同样不属于 I' 并且次数严格小于 d，因此与 $\deg f$ 的最小性矛盾。

习题

练习 3.7.1. *设 R 是 UFD，F 是其分式域。设 $f(x)$ 是 $R[x]$ 中的首一多项式，若 $g(x) \in F[x]$ 是首一多项式且在 $F[x]$ 中整除 $f(x)$，证明 $g(x) \in R[x]$。*

练习 3.7.2. *证明整系数多项式 $f(x), g(x)$ 在 $\mathbb{Q}$ 上互素的充要条件是除有限个素数外，对其余素数 p，$f(x)$ 和 $g(x)$ 在 $\mathbb{Z}/p\mathbb{Z}$ 上互素。*

练习 3.7.3. *证明 Hilbert 基定理的逆定理，即证明若 $R[x]$ 是诺特环，那么 R 也是诺特环。*

练习 3.7.4. *设 R 是诺特环，证明 $R[\![x]\!]$ 也是诺特环。*

第四章　域

4.1　域扩张

4.1.1　域扩张

定义 4.1.1. 设 F 是一个域，若存在正整数 n 使得 $n\cdot 1=0$，那么我们称满足条件的最小正整数为域 F 的**特征**，若不存在这样的正整数，那么我们定义 F 的特征为 0。

命题 4.1.2. *任意域的特征要么是 0，要么是一个素数。*

证明. 假设 F 的特征是 n，若 n 是合数，不妨设 $n=n_1n_2$，其中 $n_1,n_2\neq 1$。根据分配律我们有 $(n_1\cdot 1)\cdot(n_2\cdot 1)=0$，因为 F 是整环，所以比有 $n_1\cdot 1=0$ 或者 $n_2\cdot 1=0$，这与 n 的最小性矛盾。

例 4.1.3. *像我们熟知的一些域 $\mathbb{Q}.\mathbb{R},\mathbb{C}$ 的特征均是 0。而 $\mathbb{Z}/p\mathbb{Z}$ 的特征则是 p。*

定义 4.1.4. 设 F,K 是两个域，且 $F\subseteq K$，那么我们称 K 是 F 的一个**域扩张**，记作 K/F。若将 K 视作 F 上的线性空间，那么我们称 K 在 F 上的维数为**扩张次数**，记作 $[K:F]$。若 $[K:F]$ 是有限的，则称该扩张是有限扩张，否则是无限扩张。

例 4.1.5. *$\mathbb{C}/\mathbb{Q},\mathbb{R}/\mathbb{Q}$ 都是无限扩张，但 $\mathbb{C}/\mathbb{R}$ 是有限扩张，扩张次数等于 2。*

和环同态相比，域之间的同态的性质会简单很多。

命题 4.1.6. *设 F,K 是两个域，$\phi:F\to K$ 是一个环同态，那么 ϕ 要么是零映射，要么是单射。*

证明. 由于 $\ker\phi$ 是 F 的理想，而根据命题3.2.7可知 F 的理想只有 0 和 F 自身。若 $\ker\phi=0$，那么 ϕ 是单射，若 $\ker\phi=F$，那么 ϕ 是零映射。

上述命题表明对于任意域之间的非平凡同态 $\phi:F\to K$，我们可以直接将 F 等同于 $\phi(F)$，从而只需要研究域扩张 $K/\phi(F)$。

4.1.2　代数扩张

定义 4.1.7. 设 K/F 是一个域扩张，$\alpha\in K$。若存在非零多项式 $f(x)\in F[x]$ 使得 $f(\alpha)=0$，那么我们称 α 在 F 上是**代数的**，否则称为**超越的**。若 K 中每个元素在 F 上都是代数的，那么则称 K/F 是**代数扩张**。

例 4.1.8. 容易看出诸如 $\sqrt{2},\sqrt{3},\sqrt[3]{5}$ 这些数在 $\mathbb{Q}$ 上均是代数的。然而要具体的构造一个在 $\mathbb{Q}$ 上是超越的复数并不是容易的事，第一个给出具体构造的是 *Liouville*，他证明了 $\sum_{n\geq 1}\frac{1}{10^{k!}}$ 在 $\mathbb{Q}$ 是超越的，见习题*4.1.18*。*Lindemann*证明了 π 和 e 在 $\mathbb{Q}$ 上是超越的。另一方面，*Cantor* 证明了所有 $\mathbb{Q}$ 上的代数数是可数的，而复数集是不可数的，所以几乎所有复数都是超越的。

命题 4.1.9. 设 α 在 F 上是代数的，那么存在唯一的首一不可约多项式 $m_{\alpha,F}(x)\in F[x]$，使得 $m_{\alpha,F}(\alpha)=0$。并且任意满足 $f(\alpha)=0$ 的多项式 $f(x)\in F[x]$ 均是 $m_{\alpha,F}(x)$ 的倍数。

证明. 记 $I=\{f(x)\in F[x]\mid f(\alpha)=0\}$，显然 I 非空，于是 I 中存在次数最小的首一多项式，设为 $m_{\alpha,F}(x)$。若 $m_{\alpha,F}(x)$ 可约，那么不妨设 $m_{\alpha,F}(x)=f_1(x)f_2(x)$，于是一定有 $f_1(\alpha)=0$ 或者 $f_2(\alpha)=0$，这与 $m_{\alpha,F}(x)$ 的次数最小矛盾。若还存在另一个次数相同的首一多项式 $m'(x)$ 满足条件，那么 $m_{\alpha,F}(x)-m'(x)\in I$ 并且它的次数小于 $m_{\alpha,F}(x)$，这意味着 $m_{\alpha,F}(x)=m'(x)$。最后由于 $F[x]$ 是主理想整环，所以 I 中每个元素均是 $m_{\alpha,F}(x)$ 的倍数。

设 α 在域 F 上是代数的，我们称命题4.1.9中的多项式 $m_{\alpha,F}$ 为 α 在 F 上的**极小多项式**，$\deg m_{\alpha,F}$ 称之为 α 在 F 上的**次数**。

命题 4.1.10. 设 α 在 F 上是代数的，那么我们有同构：

$$F(\alpha)\simeq F[x]/(m_{\alpha,F}(x)).$$

特别地，我们有 $[F(\alpha):F]=\deg m_{\alpha,F}(x)$。

证明. 我们考虑环同态

$$\begin{array}{rccc}\varphi: & F[x] & \longrightarrow & F(\alpha)\\ & f(x) & \longmapsto & f(\alpha).\end{array}$$

根据命题4.1.9的证明可知 $\ker\varphi$ 是由 $m_{\alpha,F}(x)$ 生成的理想。显然映射 φ 是满射，因此根据环同构定理可知 $F(\alpha)\simeq F[x]/(m_{\alpha,F}(x))$。

例 4.1.11. 对任意正整数 $n>1$，多项式 x^n-2 在 $\mathbb{Q}$ 上都是不可约的，记其中一个根为 $\sqrt[n]{2}$，那么 $[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}]=n$。

命题 4.1.12. α 在 F 上是代数的当且仅当 $F(\alpha)/F$ 是有限扩张。特别地，若 K/F 是有限扩张，那么 K/F 一定是代数扩张。

证明. 若 α 在 F 上是代数的，那么根据命题4.1.10可知 $F(\alpha)/F$ 是有限扩张。反之，我们证明更一般地结论，若 K/F 是有限扩张，那么 K/F 是代数扩张，事实上，设 $[K:F]=n$，那么对任意 $0\neq\beta\in K$，$1,\beta,\beta^2,\ldots,\beta^n$ 在 F 上一定是线性相关的，所以存在不全为 0 的元素 $a_i\in F$ 使得 $a_0+a_1\beta+\cdots+a_n\beta^n=0$。所以 β 在 F 上是代数的。

命题 4.1.13. 设 $F\subseteq K\subseteq L$ 是三个域，那么 $[L:F]=[L:K][K:F]$。

证明. 不妨假设 $L/K,K/F$ 均是有限扩张。设 $\alpha_1,\ldots,\alpha_n\in K$ 是 K 在 F 上的一组基，$\beta_1,\ldots,\beta_m$ 是 L 在 K 上的一组基。下面证明 $\alpha_i\beta_j$ 是 L 在 F 上的一组基。首先对任意 $x\in L$，存在 $b_i\in K$ 使得 $x=b_1\beta_1+\cdots+b_m\beta_m$，同样地，存在 $a_{ij}\in F$ 使得对任意 $1\leq i\leq m$ 均有 $b_i=a_{i1}\alpha_1+\cdots+a_{in}\alpha_n$。由

此可以证明 x 可被 $\alpha_i\beta_j$ 线性表出。最后证明 $\alpha_i\beta_j$ 线性无关，假设 $\sum_{i,j} a_{ij}\alpha_i\beta_j = 0$，由 $\beta_1, \dots, \beta_m$ 线性无关可知对任意 $1 \le j \le m$ 均有 $\sum_i a_{ij}\alpha_i = 0$。同样由于 $\alpha_1, \dots, \alpha_n$ 是线性无关的，因此对任意 i, j 均有 $a_{ij} = 0$。这表明 $\alpha_i\beta_j$ 是线性无关的。

由此可以得到代数扩张具有传递性。

定理 4.1.14. *若 $K/F, L/K$ 均是代数扩张，那么 L/F 也是代数扩张。*

证明. 对任意 $\alpha \in L$，因为 L/K 是代数的，因此存在多项式 $f(x) \in K[x]$ 使得 $f(\alpha) = 0$，不妨设 $f(x) = a_n x^n + \cdots + a_0$，由于 K/F 上也是代数的，记 $K' = F(a_0, \dots, a_n)$，所以 K'/F 是有限扩张。而 $F(\alpha) \subseteq K'(\alpha)$，因此由命题4.1.13可知 $K'(\alpha)/F$ 是有限扩张，所以 α 在 F 上是代数的，故 L/F 是代数扩张。

定义 4.1.15. 设域 K_1, K_2 是包含在域 K 中的两个域，我们称 K 中同时包含 K_1, K_2 最小的域为 K_1, K_2 的**复合**，记为 K_1K_2。同样对于 K 的一族子域，我们也可以定义它们的复合为 K 中包含它们的最小子域。

例 4.1.16. *设 $K_1 = \mathbb{Q}(\sqrt{2}), K_2 = \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$。那么 $K_1K_2 = \mathbb{Q}(\sqrt[6]{2})$。更一般地，设 $K_1 = F(\alpha_1, \dots, \alpha_n), K_2 = F(\beta_1, \dots, \beta_m) \subseteq K$，那么*

$$K_1K_2 = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m).$$

对于复合域的扩张次数，我们有如下结论。

命题 4.1.17. *设 K_1, K_2 是 F 上包含在域 K 中的两个域扩张，那么我们有*

$$[K_1K_2 : K_1] \le [K_2 : K_1 \cap K_2].$$

特别地，我们有 $[K_1K_2 : F] \le [K_1 : F][K_2 : F]$。

证明. 设 $\alpha_1, \dots, \alpha_n$ 是 K_1 在 $K_1 \cap K_2$ 上的一组基，$\beta_1, \dots, \beta_m$ 是 K_2 在 $K_1 \cap K_2$ 上的一组基。容易看出 K_1K_2 作为 K_1 上的线性空间可由 $\beta_1, \dots, \beta_m$ 张成。因此 $[K_1K_2 : K_1] \le m$。故由命题4.1.13可知 $[K_1K_2 : K_1 \cap K_2] = [K_1K_2 : K_1][K_1 : K_1 \cap K_2] \le [K_2 : K_1 \cap K_2][K_1 : K_1 \cap K_2]$。特别地，$K_1 \cap K_2$ 是 F 上的扩张，故有

$$\begin{aligned}[K_1K_2 : F] &= [K_1K_2 : K_1 \cap K_2][K_1 \cap K_2 : F] \\ &\le [K_2 : K_1 \cap K_2][K_1 : K_1 \cap K_2][K_1 \cap K_2 : F] \le [K_1 : F][K_2 : F].\end{aligned}$$

习题

练习 4.1.1. *计算 $\sqrt{2} + \sqrt[3]{2}$ 和 $1 + \sqrt[3]{2} + \sqrt[3]{4}$ 在 $\mathbb{Q}$ 上的极小多项式。*

练习 4.1.2. *设 θ 是 $x^3 + x + 1$ 的一个根，求 $1 + \theta$ 在 $\mathbb{Q}(\theta)$ 中的逆元。*

练习 4.1.3. *证明 $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 并计算 $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$ 的扩张次数。。*

练习 4.1.4. *$\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{-2})$ 是否同构？*

练习 4.1.5. 设 F 是一个域，$d_1, d_2 \in F$ 不是 F 中的平方元，即不存在 $\alpha \in F$ 使得 $\alpha^2 = d_1$。求 $F(\sqrt{d_1}, \sqrt{d_2})/F$ 的扩张次数。

练习 4.1.6. 设 K 是一个特征不等于 2 的域。设 $a, b \in K$ 且 b 不是平方元，求 $K(\sqrt{a+\sqrt{b}})/K$ 的扩张次数。

练习 4.1.7. 假设 K/F 的扩张次数是素数 p，证明 K 中任何包含 F 的子域要么是 K 要么是 F。

练习 4.1.8. 设 K/F 是有限扩张，$f(x) \in F[x]$ 是 k 次不可约多项式。若存在 $a \in K$ 使得 $f(a) = 0$，证明 k 整除 $[K : F]$。

练习 4.1.9. 若 $[F(a) : F]$ 是奇数，证明 $F(a) = F(a^2)$。

练习 4.1.10. 设 K_1, K_2 是 F 上包含在域 K 中的两个域扩张。假设 $[K_1 : F]$ 和 $[K_2 : F]$ 互素。证明 $[K_1K_2 : F] = [K_1 : F][K_2 : F]$。

练习 4.1.11. 证明 $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3}\ldots, \sqrt{n})$。

练习 4.1.12. 设 K/F 是一个域扩张，对于 $a \in K$，我们定义映射 $L_a : K \to K, b \mapsto ab$。容易看出这是 F-线性映射。我们称 L_a 的迹为 a 的**迹**，记作 $\mathrm{Tr}_{K/F}(a)$，称 L_a 的行列式为 a 的**范数**，记作 $N_{K/F}(a)$。

1. 设 $F = \mathbb{Q}, K = \mathbb{Q}(\sqrt[3]{2})$，计算 $\mathrm{Tr}_{K/F}(\sqrt[3]{2})$ 和 $N(\sqrt[3]{2})$。
2. 证明对任意 $a \in K$ 均有 $\mathrm{Tr}_{K/F}(a), N_{K/F}(a) \in F$。特别地，若 $a \in F$，则有 $\mathrm{Tr}_{K/F}(a) = na, N_{K/F}(a) = a^n$。
3. 设 $[K : F] = n$，$a \in K$ 在 F 上的极小多项式为 $p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$，那么 $\mathrm{Tr}_{K/F}(a) = -\frac{n}{m}a_{m-1}, N_{K/F}(a) = (-1)^n a_0^{\frac{n}{m}}$。

练习 4.1.13. 设 F 是一个特征不为 2 的域，K/F 是一个二次扩张。

1. 证明存在 $x \in K \setminus F$ 使得 $K = F(x)$ 且 $x^2 \in F$。
2. 证明 $(K^*)^2 \cap F^* = (F^*)^2 \sqcup x^2(F^*)^2$。

练习 4.1.14. 设 F 是一个特征不为 2 的域。设 $a, b \in F^*$ 且 $b \notin (F^*)^2$。记 $K = F(\sqrt{b}), L = K(\alpha)$ 其中 $\alpha^2 = a + \sqrt{b}$。

1. 证明 $L = K$ 当且仅当存在 $d \in F^*$ 使得 $a^2 - b = d^2$ 且 $2(a + d) \in (F^*)^2$。
2. 证明存在 $\beta \in L^*$ 使得 $\beta^2 = a - \sqrt{b}$ 当且仅当 $a^2 - b \in (F^*)^2 \sqcup b(F^*)^2$。
3. 计算 $F^* \cap (L^*)^2$。
4. 证明存在 $c \in F^*$ 使得 $L = F(\sqrt{b}, \sqrt{c})$ 当且仅当 $a^2 - b \in (F^*)^2$。

练习 4.1.15. 设 F 是一个域，K 为 F 的代数扩域且包含在 $F(X)$ 中，证明 $F = K$。

练习 4.1.16. 设 K/F 是一个有限扩张。设 $a, b \in K$ 在 F 上的极小多项式分别为 f_a, f_b，证明 f_a 在 $F(b)$ 上不可约当且仅当 f_b 在 $F(a)$ 上不可约。

练习 4.1.17. 设 K_1, K_2 是 K 的两个子域，且 $K/K_1, K/K_2$ 均是代数扩张，$K/(K_1 \cap K_2)$ 是否一定是代数扩张？(提示：考虑 $K = \mathbb{Q}(x), K_1 = \mathbb{Q}(x^2), K_2 = \mathbb{Q}(x^2 - x)$。)

练习 4.1.18 (Liouville 定理)**.** 设 α 是次数为 $n \geq 2$ 的代数数，$f(x)$ 是其极小多项式。

1. 设 $|\alpha - \frac{p}{q}| < 1$，证明存在只依赖于 α 的常数 M 使得 $|f(\frac{p}{q}) - f(\alpha)| < M|\alpha - \frac{p}{q}|$；
2. 对任意有理数 $\frac{p}{q}$ 均有 $|f(\frac{p}{q}) - f(\alpha)| \geq \frac{1}{q^n}$；
3. 证明存在常数 $c > 0$ 使得对任意有理数 $\frac{p}{q}$ 均有 $|\alpha - \frac{p}{q}| \geq \frac{c}{q^n}$。
4. 证明 $\sum_{n\geq 1} \frac{1}{10^{n!}}$ 不是代数数。

练习 4.1.19. 设 $K(x)$ 是域 K 上的有理函数域。

1. 计算 x 在域 $K(x^2+1)$ 上的极小多项式，并计算 $[K(x) : K(x^2+1)]$。
2. 记 $t = \frac{f(x)}{g(x)} \in K(x)$，其中 $f(x)$ 和 $g(x)$ 是 $K[x]$ 中互素的多项式。证明 $f(X) - tg(X)$ 作为域 $K(t)$ 上的多项式是不可约的，并且 x 是其一个根。由此计算 $[K(x) : K(t)]$。

4.2 尺规作图

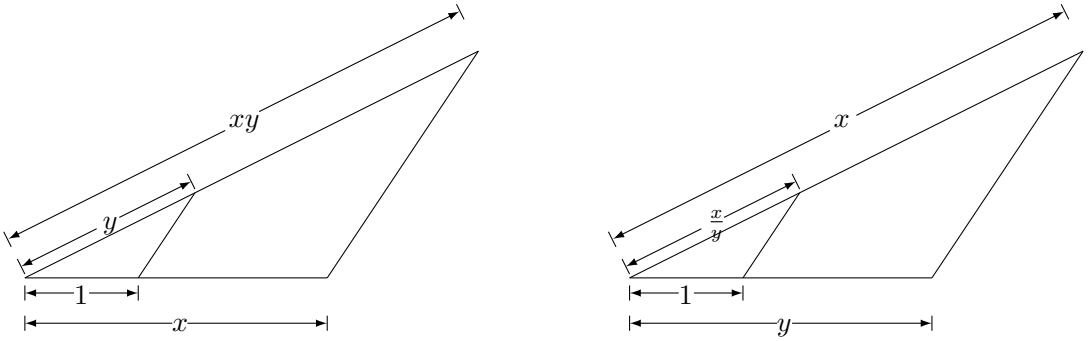
这一节我们应用域论来解决古希腊的三大几何作图难题，

1. 三等分角问题：能否通过尺规作图将任意给定角三等分?
2. 倍立方体问题：能否通过尺规作图给出是给定立方体体积两倍的立方体?
3. 化圆为方问题：能否通过尺规作图作出正方形使得其面积是给定圆的面积。

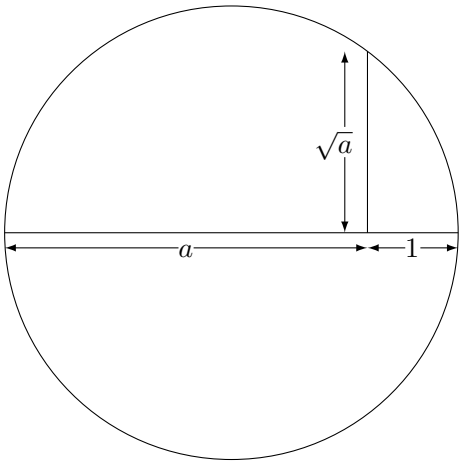
为了解决这些问题，我们需要将尺规作图的过程转化为代数语言。

我们先假定一个单位长度 '1'，再记所有可以通过给定的单位长度和尺规作图得到的长度的集合为 F，F 中的点我们称为是可构造的。因为 $x + y\sqrt{-1}$ 是可构造的当且仅当 x, y 是可构造的，因此我们只需考虑可构造的实数即可。

首先我们说明 F 构成一个域。若 $x, y \in F$，那么显然有 $x \pm y \in F$。根据下面这两个图示我们可以证明 $xy, x/y \in F$。



更进一步，根据下图我们还知道若 $a \in F$，那么 $\sqrt{a} \in F$。



那么是否这便能做出 F 中所有的数呢？我们先来分析尺规作图可以做什么？利用直尺可以做出过任意两个确定点的直线，利用圆规可以做出以任意已知点为圆心，已知长度为半径的圆。我们能得到的新的可构造数即为这些直线和圆的交点。我们可以建立坐标系，做出 x 轴和 y 轴。假设已经做出了 $\mathbb{Q}$ 扩域 K，设 $K_1 = K \cap \mathbb{R}$，即为已经做出的可构造的实数，那么 $K = \{a + b\sqrt{-1} \mid a, b \in K_1\}$。以 K 中两点出发可做出的直线为

$$ax + by + c = 0, \qquad a, b, c \in K_1.$$

而以 K 中点为圆心，K_1 中数为半径的圆的方程为

$$(x - d)^2 + (y - e)^2 = r^2, \qquad d, e, r \in K_1.$$

而下一个可构造点只能是这些直线和圆的交点，因此只可能有如下三种情况：

1. 直线与直线的交点。此时容易看出交点坐标仍是 K_1 中的元素。

2. 直线和圆的交点。联立方程可得

$$\begin{cases} ax + by + c = 0, \\ (x - d)^2 + (y - e)^2 = r^2. \end{cases}$$

   此时该方程组的解即为可构造数，而通过消元容易看出 x 是一个至多二次的方程的解，故 $[K_1(x) : F_1] \leq 2$，利用直线方程可以知道 $y \in K_1(x)$。因此 $x + y\sqrt{-1} \in K(x)$。

3. 圆和圆的交点。联立方程可得

$$\begin{cases} (x - d_1)^2 + (y - e_1)^2 = r_1^2, \\ (x - d_2)^2 + (y - e_2)^2 = r_2^2. \end{cases}$$

   将两个方程做差可以转化为圆和直线相交的情况。

综上所述，由 K 经过直线和圆的交点得到的新的可构造数在 K 的某个二次扩域中。因此我们有下面的定理。

定理 4.2.1. 复数 a 是可构造的当且仅当存在二次扩张序列

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n,$$

使得 $a \in K_n$，其中 K_{i+1}/K_i 都是二次扩张。特别地，$[\mathbb{Q}(a) : \mathbb{Q}]$ 是 2 的幂次。

注 10. 注意到上述定理的逆命题是不对的，即若 $[\mathbb{Q}(a) : \mathbb{Q}]$ 是 2 的幂次，a 也不一定是可构造的。例如，设 a 是多项式 $x^4 - 4x + 2$ 的一个根，那么 $[\mathbb{Q}(a) : \mathbb{Q}] = 4$，但是 a 是不可构造的。

现在我们可以解决三大尺规作图问题了。

三等分任意角： 给定一个角度 3θ，要做出 θ，即等价于 $\cos\theta$ 是可构造的。利用三倍角公式有

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta,$$

例如我们考虑 $\theta = 20°$，那么 $\cos 3\theta = \frac{1}{2}$。容易看出 $4x^3 - 3x - \frac{1}{2}$ 在 $\mathbb{Q}$ 上是不可约的，因此 $\cos 20°$ 在 $\mathbb{Q}$ 的一个三次扩域中，因此是不可构造的。

倍立方： 这等价于 $\sqrt[3]{2}$ 是可构造的，然而这显然是不对的。

化圆为方： 这等价于 $\sqrt{\pi}$ 是可构造的。但是 Lindemann 证明了 π 是超越数，所以 $\sqrt{\pi}$ 是不可构造的。

上面证明了 $\cos 20°$ 是不可构造的，那么一个很自然的问题便是哪些整数角度是可构造的？首先我们容易看出 $1°$ 和 $2°$ 是不可构造的，否则利用倍角公式容易看出 $\cos 20°$ 是可构造的。另一方面，我们可以证明 $\cos 3°$ 是可构造的，事实上，我们有

$$\cos 3° = \frac{1}{8}(\sqrt{3}+1)\sqrt{5+\sqrt{5}} + \frac{1}{16}(\sqrt{6}-\sqrt{2})(\sqrt{5}-1). \tag{4.1}$$

习题

练习 4.2.1. 证明正五边形可以通过尺规作图作出。

练习 4.2.2. 证明正九边形不可以通过尺规作图作出。

练习 4.2.3. 证明公式 (4.1)。

练习 4.2.4. 证明正十七边形可以通过尺规作图作出。

练习 4.2.5. 折纸的文化起源可以追溯到中国，并与中国造纸术的发展密切相关。东汉时期（公元 *1–2* 世纪），随着蔡伦对造纸术的改进，纸张逐渐走向社会生活，其良好的可塑性很快被运用于礼俗活动与民间技艺之中。此后，随着纸张及相关技艺向外传播，折纸也传入周边地区，并在不同文化语境中演化出各具特色的审美与技术；其中，日本在近代对折纸进行了系统化与艺术化的发展，使其以“*Origami*”之名在当代世界范围内广为人知。下面我们将介绍折纸构造的六个公理。

(O_1) 给定两个不同的点 p_1 和 p_2，存在且仅存在一条经过 p_1 与 p_2 的折痕。

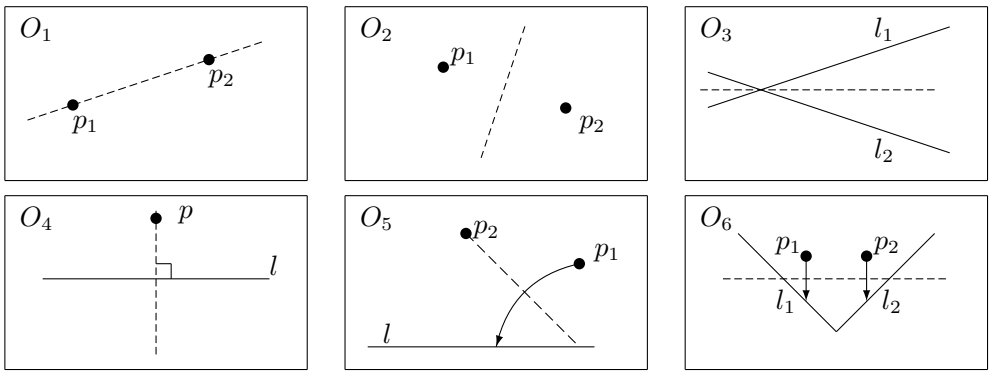
(O_2) 给定两个不同的点 p_1 和 p_2，存在且仅存在一条折痕（垂直平分线），使得折叠后 p_1 与 p_2 重合。

(O_3) 给定两条直线 l_1 和 l_2，存在一条折痕（角平分线），使得折叠后 l_1 与 l_2 重合。

(O_4) 给定一点 p_1 和一条直线 l_1，存在且仅存在一条经过 p_1 且垂直于 l_1 的折痕。

(O_5) 给定两点 p_1, p_2 和一条直线 l_1，存在一条折痕，使得折叠后 p_1 落在 l_1 上，且该折痕经过 p_2。

(O_6) 给定两点 p_1, p_2 以及两条直线 l_1, l_2，存在一条折痕，使得折叠后 p_1 落在 l_1 上，同时 p_2 落在 l_2 上。



定义 *1.* 设初始点集为 $\{0,1\} \subset \mathbb{C}$，并将复平面 $\mathbb{C}$ 视为折纸的欧氏平面。若一个复数 $z \in \mathbb{C}$ 所对应的点能够通过有限次折纸操作得到，即作为一系列折痕的交点出现，其中每一步操作仅允许使用折纸六个公理所规定的基本折叠方式。我们称 z 为折纸可构造的复数。

1. 简述为什么折纸可构造的复数构成一个域。*(*提示：由 O_4 可以构造平行线。*)*

2. 在 O_5 中，把 $p_1 = (1,0)$ 折叠到 $l_1 : y = 1$ 上，得到经过 $p_2 = \left(1, \frac{a+1}{2}\right)$ 的折痕。证明：此折痕的斜率 k 满足二次方程：
$$k^2 = a.$$

3. 在 O_6 中，把 $p_1 = \left(\frac{q}{2}, \frac{p+1}{2}\right)$ 折到直线 $l_1 : x = -\frac{q}{2}$ 上，点 $p_2 = (0,1)$ 折到直线 $l_2 : y = 0$ 上。证明：此折痕的斜率 k 满足三次方程：
$$k^3 + pk + q = 0.$$
据此说明倍立方与三等分角问题均可通过折纸构造实现。

4. 证明：z 是折纸可构造的，当且仅当存在域扩张：
$$L_0 = \mathbb{Q} \subseteq L_1 \subseteq \cdots \subseteq L_n,$$
使得 $z \in L_n$ 且 $[L_j : L_{j-1}] = 2$ 或 3。

5. 证明：正七边形是折纸可构造的。

4.3 分裂域与代数闭域

4.3.1 分裂域

定义 4.3.1. 设 K/F 是一个域扩张，$f(x) \in F[x]$。若 $f(x)$ 在 $K[x]$ 中能分解为一次因式的乘积，并且对 K 的任意真子域 M，$f(x)$ 在 M 上都不能分解为一次因式的乘积，那么我们称 K 是 $f(x)$ 的一个**分裂域**。

例 4.3.2. 1. 设 $F=\mathbb{Q}, f(x)=x^2-2$，那么 $K=\mathbb{Q}(\sqrt{2})$ 是 $f(x)$ 的一个分裂域。但是我们要注意到分裂域并不是唯一的，例如域 $L=\mathbb{Q}[T]/(T^2-2)$ 也是 $f(x)$ 的一个分裂域，因为在 $L[x]$ 中我们有分解式 $f(x)=(x+T)(x-T)$，但是我们有同构 $\mathbb{Q}(\sqrt{2})\simeq\mathbb{Q}[T]/(T^2-2)$。事实上，我们后面将会证明 $f(x)$ 的任意两个分裂域都是同构的。

2. 设 $F=\mathbb{Q}, f(x)=x^3-2$，那么 $K=\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})$ 是 $f(x)$ 的一个分裂域。

我们再讨论一类常见的域。

例 4.3.3. 设 n 是一个正整数，我们讨论多项式 x^n-1 在 $\mathbb{Q}$ 上的分裂域。我们假设该分裂域包含在 $\mathbb{C}$ 中，那么容易看出 $\zeta_n=\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}}$ 是 x^n-1 在 $\mathbb{C}$ 中的一个根，并且其余所有根都是形如 $\zeta_n^k, k=0,1,\ldots,n-1$。因此它的分裂域便是 $\mathbb{Q}(\zeta_n)$。我们称 $\mathbb{Q}(\zeta_n)$ 为 n-次分圆域。但是要计算扩张次数 $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ 并不是一件简单的事，我们先考虑 $n=p$ 为素数的情况，一般的情况将在后面进行讨论。在素数的情况，我们知道 $x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+1)$。设 $g(x)=x^{p-1}+x^{p-2}+\cdots+1$，于是 $g(x+1)=((x+1)^p-1)/x=x^{p-1}+px^{p-2}+\cdots+p$，因此根据 *Eisenstein* 判别法可知 $g(x)$ 是不可约多项式。因此 $g(x)$ 即为 ζ_p 在 $\mathbb{Q}$ 上的极小多项式，故 $[\mathbb{Q}(\zeta_p):\mathbb{Q}]=p-1$。

例 4.3.4. 设 $F=\mathbb{Q}$，$f(x)=x^p-2$，其中 p 是一个素数。那么 $f(x)$ 在 $\mathbb{C}$ 中的所有根是 $\sqrt[p]{2}\zeta_p^k$，$k=0,1,\ldots,p-1$。那么 $\mathbb{Q}(\sqrt[p]{2},\zeta_p)$ 便是 $f(x)$ 的一个分裂域，下面我们计算其扩张次数。根据上面的例子可知 $[\mathbb{Q}(\zeta_p):\mathbb{Q}]=p-1$。另一方面，由于 x^p-2 在 $\mathbb{Q}$ 上不可约，因此 $[\mathbb{Q}(\sqrt[p]{2}):\mathbb{Q}]=p$。而 p 和 $p-1$ 互素，因此根据习题*4.1.10*可知 $[\mathbb{Q}(\sqrt[p]{2},\zeta_p):\mathbb{Q}]=p(p-1)$。

定理 4.3.5. 设 $f(x)$ 是域 F 上的 n 次多项式，那么存在 f 在 F 上的分裂域 K，且 $[K:F]\leq n!$。

证明. 我们对 n 进行归纳，当 $n=1$ 时，结论是平凡的。下面假设 $n>1$，不妨设 $f(x)$ 是不可约的，否则设 $f(x)=f_1(x)f_2(x)$，根据归纳假设知存在 $f_1(x),f_2(x)$ 的分裂域 K_1,K_2 使得 $[K_1:F]\leq(\deg f_1)!, [K_1:F]\leq(\deg f_2)!$，因此根据命题4.1.17可知

$$[K_1K_2:F]\leq(\deg f_1)!\cdot(\deg f_2)!<n!.$$

因此我们下面假设 $f(x)$ 是不可约的，记 $F_1=F[x]/(f(x))$，此时 F_1 是一个域，并且记 x 在 F_1 中的像是 $\bar{x}$，根据定义可知 $\bar{x}$ 是 $f(x)$ 在 F_1 中的一个根，因此不妨设 $f(x)$ 在 F_1 中可分解为 $(x-\bar{x})f_1(x)$。根据归纳假设知存在 $f_1(x)$ 在 F_1 上的分裂域 K 且有 $[K:F_1]\leq(n-1)!$，所以 $[K:F]\leq n!$。根据定义知 $f(x)$ 在 K 中可分解为一次因式的乘积，因此存在 K 的子域 K' 为 $f(x)$ 的分裂域，且 $[K':F]\leq n!$。

定理 4.3.6. 多项式 $f(x)\in F[x]$ 在 F 上的分裂域都是同构的。

证明. 事实上，我们可以证明一个更一般地结论：设 $\varphi:F_1\to F_2$ 是一个同构，$f(x)\in F_1[x]$，定义 $\varphi(f)(x)\in F_2[x]$ 为将 φ 作用在 $f(x)$ 的系数上得到的多项式。再设 K_1,K_2 分别为 $f(x),\varphi(f)(x)$ 在 F_1,F_2 上的分裂域，那么 φ 可延拓为同构 $K_1\simeq K_2$。

我们对 $\deg f$ 进行归纳。当 $n=1$ 时，结论显然成立。下面假设结论对 $n-1$ 成立。设 $p(x)$ 为 $f(x)$ 在 $F[x]$ 上的一个不可约因式。α_1,α_2 分别是 $p(x)$ 和 $\varphi(p)(x)$ 在 K_1,K_2 中的根，构造如下同构：

$$\begin{array}{ccc} F_1(\alpha_1) & \longrightarrow & F_2(\alpha_2) \\ \alpha_1 & \longmapsto & \alpha_2 \end{array}$$

于是 $f(x),\varphi(f)(x)$ 在 $F_1(\alpha_1),F_2(\alpha_2)$ 中分别能分解为 $(x-\alpha_1)f_1(x)$ 和 $(x-\alpha_2)f_2(x)$。而 $\deg f_1,\deg f_2\leq n-1$。容易证明 K_1,K_2 均为 $f_1(x),f_2(x)$ 在 F_1,F_2 上的分裂域。根据归纳假设，我们可以得到 $K_1\simeq K_2$。

4.3.2 代数闭包

定义 4.3.7. 设 F 是一个域，若域 $\overline{F}$ 是 F 的代数扩张，并且任何多项式 $f(x) \in F[x]$ 都在 $\overline{F}$ 中是完全分裂的，即在 $\overline{F}$ 中能分解成一次因式的乘积，那么我们称 $\overline{F}$ 是 F 的**代数闭包**。

定义 4.3.8. 若 $K[x]$ 中的任意一个多项式在 K 中均有一个根，那么则称 K 是**代数闭域**.

下面的命题给出了代数闭包和代数闭域两个概念的联系。

命题 4.3.9. *设 $\overline{F}$ 是 F 的代数闭包，那么 $\overline{F}$ 是代数闭域。反之，若 K 是代数闭域，F 是 K 的子域，那么 K 存在一个子域是 F 的代数闭包。*

证明. 设 $f(x) \in \overline{F}[x]$，并且 α 是 $f(x)$ 的一个根，那么 $\overline{F}(\alpha)$ 是 $\overline{F}$ 上的代数扩张，根据定理4.1.14可知 $\overline{F}(\alpha)/F$ 也是代数扩张，因此 α 在 F 上是代数的，故 $\alpha \in \overline{F}$。因此 $\overline{F}$ 是代数闭域。

反之，若 K 是代数闭域，令 $\overline{F} = \{a \in K \mid a \text{ 在 } F \text{ 上是代数的}\}$。那么 $\overline{F}$ 显然是 F 的代数扩张。另一方面，对任意 $f(x) \in F[x]$，由于 K 是代数闭域，因此 $f(x)$ 在 K 中至少有一个根，设为 α，但是 α 在 F 上是代数的，因此 $\alpha \in \overline{F}$，故 $f(x)$ 能在 $\overline{F}$ 中分解是完全分裂的，因此 $\overline{F}$ 是 F 的代数闭包。

注 11. 我们要注意代数闭包和代数闭域是有区别的，因为代数闭域不一定是其子域的代数扩张。例如由代数基本定理我们知道 $\mathbb{C}$ 是代数闭域，但是它不是 $\mathbb{Q}$ 上的代数闭包，因为如前所述，像 π, e 这些数都是超越的。

下面我们证明任意域均有代数闭包，其证明的想法是自然的，我们不断的将 $F[x]$ 中多项式的根加入到 F 的扩域中，因为任何一个多项式的根的个数都是有限的，所以只需要有限次操作即可囊括它的所有根。

定理 4.3.10. *任意域 F 均有代数闭包。*

证明. 对 $F[x]$ 中的每一个非常数的首一多项式 $f(x)$，我们对应一个未定元 x_f，考虑多项式环 $R = F[\cdots x_f \cdots]$，设 I 是 R 中由所有 $f(x_f)$ 生成的理想，其中 f 遍历所有的非常数的首一多项式。我们先证明 I 是非平凡的，否则会存在多项式 $f_1(x_{f_1}), \ldots, f_n(x_{f_n})$ 及元素 $g_1, \ldots, g_n \in R$ 使得

$$g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \cdots + g_n(x_{f_n}) = 1. \tag{4.2}$$

设 K 是多项式 $f_1(x), \ldots, f_n(x)$ 在 F 上的分裂域，并设 $\alpha_i \in K$ 是 $f_1(x)$ 在 K 中的一个根。在式(4.2)中取 $x_{f_i} = \alpha_i$ 可得 $0 = 1$，显然是矛盾的。于是由定理3.3.2可知存在包含 I 的极大理想 $\mathfrak{m}$，并且由命题3.3.3知 $K_1 := R/\mathfrak{m}$ 是域。根据构造可知 $F[x]$ 中的每一个元素 $f(x)$ 在 K_1 中均至少有一个根，即为 x_f 的像，因为 $f(x_f) \in \mathfrak{m}$。我们将上述过程中的 F 用 K_1 代替，可以构造得到一个新的扩域 K_2，并将此过程依次进行下去，我们可以得到一系列域扩张:

$$F \subseteq K_1 \subseteq K_2 \subseteq \ldots.$$

根据构造过程可知每一个 $K_i[x]$ 中的元素均在 K_{i+1} 中有一个根。最后取

$$K = \bigcup_{i \geq 1} K_i.$$

显然 K 是 F 的一个域扩张。设 $h(x) \in K[x]$，那么 $h(x)$ 的系数一定均在某个 K_i 中，即有 $h(x) \in K_i[x]$，故 $h(x)$ 在 K_{i+1} 中至少有一个根，所以 $h(x)$ 在 K 中至少有一个根，因此 K 是代数闭域。最后利用命题4.3.9可以得到 F 的代数闭包。

习题

练习 4.3.1. 求下列多项式在 $\mathbb{Q}$ 上的分裂域：

1. x^4-2；
2. x^4+2
3. x^6-4。

练习 4.3.2. 设 $F\subseteq L\subseteq K$ 是三个域，若 K 是 $f(x)\in F[x]$ 在 F 上的分裂域，证明 K 是 $f(x)$ 在 L 上的分裂域。

练习 4.3.3. 设 K 是 F 上的二次扩域，证明 K 是 F 的分裂域。

练习 4.3.4. 设 K/F 是一个有限域扩张。证明 K 是 F 的一个分裂域当且仅当每一个 $F[x]$ 中的不可约多项式 $f(x)$，若 $f(x)$ 在 K 中有一个根，那么 $f(x)$ 在 K 中完全分裂。

练习 4.3.5. 设 $K_1,K_2\subseteq K$ 是 F 上的两个域扩张。假设它们都是 F 上的分裂域。

1. 证明 K_1K_2 是 F 上的分裂域；
2. 证明 $K_1\cap K_2$ 是 F 上的分裂域。

练习 4.3.6. 设 K 是一个域且特征不等于 3，$P(x)$ 是 K 上的三次多项式，L 是 $P(x)$ 在 K 上的一个分裂域。

1. 证明 $[L:K]\in\{1,2,3,6\}$，并且 $P(x)$ 是不可约的当且仅当 $[L:K]\in\{3,6\}$。
2. 证明存在多项式 $Q(x)=x^3+px+q\in K[x]$ 使得 L 也是 $Q(x)$ 在 K 上的分裂域。
3. 假设 $P(x)$ 不可约的。记 x_1,x_2,x_3 是 $Q(x)$ 在 L 中的三个根，并记 $\delta=(x_1-x_2)(x_2-x_3)(x_3-x_1)$。证明 $\delta^2=-4p^3-27q^2$。我们称 δ^2 为 $Q(x)$ 的**判别式**。
4. 证明 $[L:K]=3$ 当且仅当 $\delta\in K$。
5. 设 $K=\mathbb{R}(T),P(x)=x^3+(T^2-1)x+T^3-1$，计算此时的 $[L:K]$。

4.4 有限域

这一节我们讨论有限域，我们将证明有限域的存在性。我们首先介绍形式导数。

4.4.1 形式导数

设 F 是一个域，$f(x)\in F[x]$ 为一个多项式。设 K 是 $f(x)$ 在 F 上的一个分裂域，于是 $f(x)$ 在 K 上有如下分解

$$f(x)=(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_k)^{n_k},$$

其中 $\alpha_i\in K$，$n_i\geq 1$。若 $n_i>1$，则称 α_i 是**重根**，否则称为**单根**。

定义 4.4.1. 若 F 上的多项式没有重根，则称该多项式是**可分的**，否则称为**不可分的**。设 K/F 是一个域扩张，若 K 中的任意元素均是 F 上某个可分多项式的根，则称 K/F 是**可分的**，否则称为**不可分的**。

例 4.4.2. 考虑域 $F(t)$ 上的多项式 x^2-t，可以验证该多项式是不可约的。记 $\sqrt{t}$ 是某个分裂域中的根。当 F 的特征不等于 2 的时候，那么 $-\sqrt{t}\neq\sqrt{t}$ 是 x^2-t 的另一个根。此时 x^2-t 是可分的，而当 F 的特征等于 2 时，那么

$$(x-\sqrt{t})^2=x^2-2x\sqrt{t}+t=x^2-t.$$

这意味着此时 x^2-t 是不可分的。

我们先回忆一下多项式的一些知识。设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in F[x]$，我们定义 $f(x)$ 的**形式导数**为 $na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1\in F[x]$，并记为 $f'(x)$。该形式导数和微积分中的导数公式是一致的，但是我们这里只是借用了微积分中的公式，其定义是完全代数上的，不能理解为 $F[x]$ 中的多项式求导。可以直接验证该定义同样满足如下公式

$$\begin{aligned}(f(x)+g(x))'&=f'(x)+g'(x)\\(f(x)g(x))'&=f(x)g'(x)+f'(x)g(x).\end{aligned}$$

利用形式导数的概念，我们可以给出多项式有重根的条件，该结果和实数域上多项式的结果是一致的。

命题 4.4.3. α 是多项式 $f(x)$ 的重根当且仅当 α 是 $f'(x)$ 的根。特别地，$f(x)$ 是可分的当且仅当 $f(x)$ 和 $f'(x)$ 的公因式是 1。

证明. 假设 $f(x)=(x-\alpha)g(x)$，于是 $f'(x)=g(x)+(x-\alpha)g'(x)$。因此 α 是 $f'(x)$ 的根当且仅当 α 是 $g(x)$ 的根，由此可得原结论。

例 4.4.4.

1. 考虑有限域 $\mathbb{F}_p$ 上的多项式 $x^{p^n}-x$，它的形式导数为 $p^nx^{p^n-1}-1=-1$。因此它的形式导数没有根，故 $x^{p^n}-x$ 的任意一个根都是单根。

2. 考虑有限域 $\mathbb{F}_p$ 上的多项式 x^n-1，它的形式导数为 nx^{n-1}。当 p 整除 n 时，该形式导数是零多项式，故 x^n-1 的任意一个根都是重根，反之，若 p 不整除 n，则该形式导数的根只有 0（$n-1$ 重）。但显然 0 不是 x^n-1 的根，因此 x^n-1 的所有根均为单根。

4.4.2 有限域的存在性

命题 4.4.5. 设 F 是一个有限域，那么它的特征一定是素数，并且 F 的元素个数一个是素数的幂。同时 F 中任意元素 α 均满足 $a^{|F|}-a=0$。

证明. 根据命题4.1.2可知域 F 的特征为 0 或者是一个素数。若 F 的特征是 0，那么 $0,1,2,\ldots,n,\ldots$ 是互不相同的，这与 F 元素个数有限矛盾，假设 F 的特征是 p，那么 F 可视作 $\mathbb{F}_p$ 上的线性空间，设维数是 n，那么 $|F|=p^n$。由于 $\mathbb{F}^*$ 是 p^n-1 阶的交换群，因此根据推论2.3.12可知对任意 $a\in F$ 使得 $a^{p^n-1}=1$。

上述结论表明有限域的阶只能是素数的幂，那么一个自然的问题是任意素数的幂阶的有限域是否一定存在。下面的定理便回答了这一问题。

引理 4.4.6. 设 F 是一个特征为 p 的域，那么对任意 $a,b\in F$，我们有

$$(a+b)^p=a^p+b^p.$$

证明. 根据二项式展开有

$$(a+b)^p=a^p+\binom{1}{p}a^{p-1}b+\binom{2}{p}a^{p-2}b^2+\cdots+b^p.$$

当 $1\le k\le p-1$ 时，我们有 $\binom{k}{p}=\frac{p!}{k!(k-p)!}$，其分子是 p 的倍数，而分母和 p 互素，因此 $\binom{k}{p}$ 是 p 的倍数，由于 F 是特征 p 的，因此 $\binom{k}{p}=0$。故有 $(a+b)^p=a^p+b^p$。

定理 4.4.7. 设 p 是一个素数，n 是一个正整数，那么存在阶为 p^n 的有限域，并且在同构的意义下，它是唯一的。我们将阶为 $q=p^n$ 的有限域记为 $\mathbb{F}_q$。

证明. 根据定理4.3.5, 设 K 是多项式 $x^{p^n}-x$ 在 $\mathbb{F}_p$ 上的一个分裂域。根据命题4.4.3可知 $x^{p^n}-x$ 没有重根，因此它恰有 p^n 个根，记 $\mathbb{F}_{p^n}$ 为其所有根的集合。对任意 $a,b\in\mathbb{F}_{p^n}$，我们有 $(ab)^{p^n}=a^{p^n}b^{p^n}$，$(a^{-1})^{p^n}=(a^{p^n})^{-1}=a^{-1}$，以及

$$(a+b)^{p^n}=a^{p^n}+b^{p^n}=a+b.$$

这表明 $\mathbb{F}_{p^n}$ 构成一个域。

最后我们证明唯一性。设 F 是任意 p^n 元有限域，由于 F^* 构成一个 p^n-1 阶乘法群，根据推论2.3.12知 F 中的元素均是多项式 $x^{p^n}-x$ 的根。而多项式 $x^{p^n}-x$ 没有重根，因此 F 中的元素恰好构成 $x^{p^n}-x$ 的所有根，这表明 F 是 $x^{p^n}-x$ 在 $\mathbb{F}_p$ 上的分裂域。由定理4.3.6可知 F 在同构意义下是唯一的。

推论 4.4.8. 设 F 是有限域 $\mathbb{F}_{p^n}$ 的子域，那么 F 是 p^m 阶域，且 $m\mid n$。反之，对任意 $m\mid n$，$\mathbb{F}_{p^n}$ 存在唯一的子域 F 使得 $|F|=p^m$。

证明. 若 F 是 $\mathbb{F}_{p^n}$ 的子域，那么 $\mathbb{F}_{p^n}$ 可视为 F 上的线性空间，设其维数为 k 于是有 $p^n=(p^m)^k$，即有 $m\mid n$。反之，考虑 $\mathbb{F}_{p^n}$ 中所有满足 $x^{p^m}-x$ 的元素组成的集合，根据定理4.4.7可知其构成唯一的 p^m 元有限域。

例 4.4.9. 由于 $\mathbb{F}_{p^n}$ 在同构意义下是唯一的，因此任取一个 $\mathbb{F}_p$ 上的 n 次不可约多项式 $f(x)$，那么我们有 $\mathbb{F}_{p^n}\simeq\mathbb{F}_p[x]/(f(x))$。例如 $f(x)=x^2+x-1$ 是 $\mathbb{F}_2$ 上的不可约多项式，设 α 是 $f(x)$ 的一个根，那么 $\mathbb{F}_4=\mathbb{F}_2[\alpha]$，更具体一点，我们可以将 $\mathbb{F}_4$ 显式写出来

$$\mathbb{F}_4=\{0,1,\alpha,1+\alpha\}.$$

而这些元素之间的运算也是直接的，只需注意到 $\alpha^2=1-\alpha$ 即可。例如 $(1+\alpha)^2=1+2\alpha+\alpha^2=\alpha$。下图显示了 $\mathbb{F}_4$ 中任意两个元素的乘法：

	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$1+\alpha$	1
$\alpha+1$	0	$\alpha+1$	1	α

最后我们讨论一下有限域上的多项式。

定理 4.4.10. 设 p 是一个素数，n 是一个正整数，那么我们有

$$x^{p^n}-x=\prod_{\deg f\mid n} f(x), \tag{4.3}$$

其中上述乘积遍历所有的 $\mathbb{F}_p[x]$ 上满足 $\deg f \mid n$ 的首一不可约多项式。

证明. 设 $f(x)$ 是 $\mathbb{F}_p$ 上的 m 次首一不可约多项式，其中 $m \mid n$。于是 $K=\mathbb{F}_p[x]/(f(x))$ 是 $\mathbb{F}_p$ 上的 m 次扩张，由推论4.4.8可知我们有嵌入 $K \to \mathbb{F}_{p^n}$。因此 $\mathbb{F}_{p^n}$ 中包含 $f(x)$ 的根，由 $f(x)$ 不可约可得 $f(x) \mid x^{p^n}-x$。因此(4.3)式的右边整除左边。另一方面，设 $f(x)$ 是 $x^{p^n}-x$ 的一个 m 次首一不可约因式，设 $\alpha \in \mathbb{F}_{p^n}$ 为 $f(x)$ 的一个根，于是 $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ 是 m 次扩张。由推论4.4.8可知 $m \mid n$。因此(4.3)式成立。

例 4.4.11. $\mathbb{F}_2[x]$ 上有一个二次不可约多项式：x^2+x+1，有三个四次不可约多项式：$x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1$。因此我们有

$$x^{16}-x=x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

注 12. 更一般地，我们可以计算出 $\mathbb{F}_p$ 上的 n 次首一不可约多项式的个数。设 $\mathbb{F}_p$ 上的 n 次首一不可约多项式的个数为 $a(n)$，根据(4.3)式可得

$$p^n=\sum_{d\mid n} d a(d).$$

利用 Möbius 反演公式可得

$$a(n)=\frac{1}{n}\sum_{d\mid n} p^d \mu(n/d),$$

其中 μ 是 Möbius 函数：若 n 含有平方因子，则 $\mu(n)=0$，若 n 无平方因子，设 $n=p_1\cdots p_r$，则 $\mu(n)=(-1)^r$；

习题

练习 4.4.1. 将 x^8-x 在 $\mathbb{F}_2[x]$ 中分解为不可约多项式的乘积。

练习 4.4.2. 求多项式 x^2+x+1 在 $\mathbb{F}_2$ 上的分裂域。

练习 4.4.3. 求多项式 x^3+2x+1 在 $\mathbb{F}_3$ 上的分裂域。

练习 4.4.4. 证明 $\mathbb{F}_3[x]/(x^2+x+2)$ 和 $\mathbb{F}_3[x]/(x^2+2x+2)$ 是同构，并将该同构显式的写出来。

练习 4.4.5. 设 F 是特征为 p 的有限域，证明 F 中任意元素在 F 中均可开 p 次方。

练习 4.4.6. 设 $f(x)$ 是 $\mathbb{F}_q$ 上的 n 次不可约多项式，证明 $f(x)$ 整除 $x^{q^n-1}-1$。

练习 4.4.7. 设 F 是一个有限域，证明对任意 $a \in F$ 存在 $b,c \in F$ 使得 $a=b^2+c^2$。

练习 4.4.8. 设 $p \geq 5$ 是一个素数，考虑多项式 $f(x)=x^2+x+1 \in \mathbb{F}_p[x]$。

1. 证明 $f(x)$ 在 $\mathbb{F}_p$ 中有一个根当且仅当 $p \equiv 1 \pmod 3$。

2. 设 L 是 $f(x)$ 在 $\mathbb{F}_p$ 上的分裂域，设 α 是 $f(x)$ 在 L 中的一个根，并记 $\beta = 2\alpha + 1$。证明 $\beta^2 = -3$。

3. 证明 -3 在 $\mathbb{F}_p$ 中是平方数当且仅当 $p \equiv 1 \pmod 3$。

练习 4.4.9. 设 $p \neq 5$ 是一个素数，记 L 为多项式 $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_p[x]$ 在 $\mathbb{F}_p$ 上的分裂域。

1. 令 $\alpha \in L$ 为 $f(x)$ 的一个根，证明 $L = \mathbb{F}_p[\alpha]$。

2. 证明

$$[L : \mathbb{F}_p] = \begin{cases} 1 & \text{如果 } p \equiv 1 \pmod 5 \\ 2 & \text{如果 } p \equiv -1 \pmod 5 \\ 4 & \text{如果 } p \equiv \pm 2 \pmod 5 \end{cases}$$

3. 令 $\beta = \alpha + \alpha^{-1}$。证明 $(2\beta + 1)^2 = 5$。

4. 证明 5 在 $\mathbb{F}_p$ 中是平方数当且仅当 $p \equiv \pm 1 \pmod 5$。

练习 4.4.10 (Chevalley-Warning 定理)**.** 设 $P \in \mathbb{F}_q[x_1, \ldots, x_n]$ 是 d 次齐次多项式，$0 < d < n$。设 $V = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid P(x_1, \ldots, x_n) = 0\}$。

1. 设 $Q = 1 - P^{q-1}, S = \sum_{x \in \mathbb{F}_q^n} Q(x)$。证明 $S = |V|$；

2. 证明 $S = 0$，由此证明 P 有一个非平凡的零点；

3. 证明存在 n 次齐次多项式 P 使得 P 只有平凡零点。

练习 4.4.11. 证明 $\bigcup_{n=0}^{\infty} \mathbb{F}_{p^{n!}}$ 是 $\mathbb{F}_p$ 的一个代数闭包。

练习 4.4.12. 设 K 是一个域，若 K 的任意有限扩张都是可分的，我们则称 K 是**完美域**。

1. 证明任意特征 0 的域都是完美域。

2. 证明有限域都是完美域。

3. 设 F 是特征 p 的域，证明 F 是完美域当且仅当 $F^p = F$，即对任意 $x \in F$ 均存在 $y \in F$ 使得 $x = y^p$。

4. 请构造一个包含无限个元素的完美域。

5. 请构造一个包含无限个元素但不是代数闭域的完美域。

练习 4.4.13. 设 L/K 是代数扩张，假设 $K[x]$ 中任意一个多项式在 L 中都有一个根，本题的目标是证明 L 是 K 的一个代数闭包。

1. 若 K 是完美域，证明 L 是 K 的一个代数闭包。

2. 下面假设 K 的特征为 $p > 0$。证明 $M = \{x \in L \mid \text{存在} n \in \mathbb{N} \text{使得} x^{p^n} \in K\}$ 是完美域。

3. 证明 $M[x]$ 中任意一个多项式在 L 中都有一个根，并证明 L 是 K 的一个代数闭包。

4.5 分圆域

这一节我们将考虑分圆域 $\mathbb{Q}(\zeta_n)$。记 μ_n 为所有 n 次单位根的集合。易知 μ_n 由 ζ_n 生成，且 $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$。若 $\zeta \in \mu_n$ 的阶为 n，则称之为 n-次本原单位根。根据命题2.2.11可知 $\zeta = \zeta_n^k$ 是 n-次本原单位根的充要条件是 $(k,n)=1$，因此 n-次本原单位根的个数是 $\varphi(n)$。

定义 4.5.1. 我们定义 n-次分圆多项式为以所有 n-次本原单位根作为根的多项式，即：

$$\Phi_n(x) = \prod_{\substack{1\le k<n,\\ (k,n)=1}} (x-\zeta_n^k).$$

由于 $\mu_d \subset \mu_n$ 当且仅当 $d \mid n$，并且对任意 $\zeta \in \mu_n$，一定存在 $d \mid n$ 使得 ζ 是 d-次本原单位根。于是我们有

$$x^n - 1 = \prod_{k=1}^{n}(x-\zeta_n^k) = \prod_{d\mid n} \prod_{\substack{\zeta\in\mu_d\\ \zeta \text{ 是 } d\text{-次本原}}} (x-\zeta) = \prod_{d\mid n}\Phi_d(x). \tag{4.4}$$

例 4.5.2. 我们可以显式的写出前面若干个分圆多项式。

$$\Phi_1(x) = x-1, \quad \Phi_2(x) = x+1, \quad \Phi_3(x) = x^2+x+1, \quad \Phi_4(x) = x^2+1,$$

$$\Phi_6(x) = x^2-x+1, \quad \Phi_8(x) = x^4+1, \quad \Phi_9(x) = x^6+x^3+1.$$

若 p 是素数，那么所有大于 0 小于 p 的整数都和 p 互素，因此 $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1}+\cdots+x+1$。我们注意到这些 $\Phi_n(x)$ 的系数均是 0 或 ± 1，一个有趣的问题便是是否所有的 $\Phi_n(x)$ 均有这个性质，然而很遗憾的是这是不对的，第一个反例是 $\Phi_{105}(x)$：

$$\Phi_{105}(x) = x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-2x^{41}+\cdots-2x^7-x^6-x^5+x^2+x+1.$$

另一个相对弱一些的观察是这些多项式都是整系数多项式，而这个观察则是正确的。

引理 4.5.3. $\Phi_n(x)$ 均是整系数的首一多项式，次数为 $\varphi(n)$。

证明. 如前所述，$\deg \Phi_n(x) = \varphi(n)$。下面我们通过对 n 进行归纳来证明 $\Phi_n(x)$ 是首一整系数多项式。当 $n=1,2$ 时，根据上面的计算可知结论成立，假设对任意 $k<n$，均有 $\Phi_k(x)$ 是首一整系数多项式。下面考虑 n 的情况。根据式4.4可知 $x^n-1 = f(x)\Phi_n(x)$，其中 $f(x) = \prod_{d\mid n, d<n}\Phi_d(x)$。由归纳假设知 $f(x)$ 是首一整系数多项式。于是利用欧几里得算法可知 $f(x)$ 在 $\mathbb{Q}[x]$ 中也整除 x^n-1，因此 $\Phi_n(x) \in \mathbb{Q}[x]$。最后利用 Gauss 引理3.7.2可知 $f(x)$ 在 $\mathbb{Z}[x]$ 中整除 x^n-1，因此 $\Phi_n(x)$ 也是整系数的，其首项系数显然等于 1。

更进一步，我们有如下结论：

定理 4.5.4. $\Phi_n(x)$ 在 $\mathbb{Z}[x]$ 中都是不可约的。

证明. 若存在首一整系数多项式 $f(x), g(x)$ 使得 $\Phi_n(x) = f(x)g(x)$，不妨设 $f(x)$ 是不可约的。设 ζ 是 $f(x)$ 的一个根，那么 $f(x)$ 即为 ζ 的极小多项式。对任意和 n 互素的素数 p，ζ^p 仍是一个 n-次本原单位根。因此它是 $f(x)$ 或者 $g(x)$ 的根。

若 $g(\zeta^p) = 0$。那么 ζ 是 $g(x^p)$ 的根，因此 $f(x)$ 整除 $g(x^p)$。设 $h(x) \in \mathbb{Z}[x]$ 使得 $g(x^p) = f(x)h(x)$。对该式两边取模 p 有 $\overline{g}(x^p) = \overline{f}(x)\overline{h}(x)$。利用引理4.4.6类似的方法可以证明 $\overline{g}(x^p) = (\overline{g}(x))^p$。因此我们

有 $(\overline{g}(x))^p = \overline{f}(x)\overline{h}(x)$。根据推论3.6.6知 $\mathbb{F}_p[x]$ 是 UFD，故 $\overline{f}(x)$ 和 $\overline{g}(x)$ 在 $\mathbb{F}_p[x]$ 中有公因式。另一方面，我们对 $\Phi_n(x) = f(x)g(x)$ 两边取模 p 得 $\overline{\Phi}_n(x) = \overline{f}(x)\overline{g}(x)$，故 $\overline{\Phi}_n(x)$ 在 $\mathbb{F}_p[x]$ 中有重因式。然而由于 p 不整除 n，故 $x^n - 1$ 在 $\mathbb{F}_p$ 上不可能有重根，而 $\overline{\Phi}_n(x)$ 是 $x^n - 1$ 的因式，由此得到矛盾。

这意味着对任意 $f(x)$ 的根 ζ 及和 n 互素的素数 p 均有 ζ^p 是 $f(x)$ 的根。于是对任意和 n 互素的整数 m，将 m 写成素数乘积的形式 $m = p_1p_2\cdots p_r$，我们可以得到 ζ^{p_1} 是 $f(x)$ 的根，$(\zeta^{p_1})^{p_2}$ 也是 $f(x)$ 的根，依次进行下去可以得到 ζ^m 是 $f(x)$ 的根，故所有的 n-次本原单位根都是 $f(x)$ 的根，所以必有 $f(x) = \Phi_n(x)$。

作为推论，我们可以计算 $\mathbb{Q}(\zeta_n)$ 在 $\mathbb{Q}$ 上的扩张次数。

推论 4.5.5. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$。

证明. 根据定理4.5.4可知 $\Phi_n(x)$ 是 ζ_n 的极小多项式，因此扩张次数即为 $\Phi_n(x)$ 的次数。

最后我们再给出分圆域的一些基本性质。

引理 4.5.6. *若 m, n 是互素的两个正整数，那么我们有 $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$ 以及 $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$。*

证明. 根据定义显然有 $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$。由于 m, n 互素，故存在整数 a, b 使得 $am + bn = 1$，因此 $\zeta_{mn} = \zeta_n^a\zeta_m^b \in \mathbb{Q}(\zeta_m, \zeta_n)$。由此可得 $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$。另一方面，根据命题4.1.17及推论4.5.5可知

$$\varphi(mn) = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_m)][\mathbb{Q}(\zeta_m) : \mathbb{Q}] \leq \varphi(m)\varphi(n) = \varphi(mn). \tag{4.5}$$

由此可得不等式4.5必须严格取等号，因此有 $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_m)] = \varphi(n)$。故由命题4.1.17可得 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)] \geq \varphi(n)$。由此可知必有 $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$。

更一般地，我们有如下结论。

命题 4.5.7. *对任意正整数 m, n 我们有 $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{[m,n]})$ 及 $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(m,n)})$。这里 $[m, n], (m, n)$ 分别表示 m, n 的最小公倍数和最大公约数。*

证明. 记 $m = p_1^{k_1}\cdots p_s^{k_s}, n = p_1^{\ell_1}\cdots p_s^{\ell_s}$，其中 p_i 是互不相同的素数，这里我们允许某些 k_i, ℓ_i 为 0。于是根据引理4.5.6可得

$$\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{p_1^{k_1}})\cdots\mathbb{Q}(\zeta_{p_s^{k_s}}), \quad \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{k_1}})\cdots\mathbb{Q}(\zeta_{p_s^{k_s}}).$$

因此我们有

$$\begin{aligned}
\mathbb{Q}(\zeta_m, \zeta_n) =& \mathbb{Q}(\zeta_{p_1^{k_1}})\cdots\mathbb{Q}(\zeta_{p_s^{k_s}})\mathbb{Q}(\zeta_{p_1^{k_1}})\cdots\mathbb{Q}(\zeta_{p_s^{k_s}}) \\
=& \mathbb{Q}(\zeta_{p_1^{k_1}})\mathbb{Q}(\zeta_{p_1^{k_1}})\cdots\mathbb{Q}(\zeta_{p_s^{k_s}})\mathbb{Q}(\zeta_{p_s^{k_s}}) \\
=& \mathbb{Q}(\zeta_{p_1^{\max(k_1,\ell_1)}})\cdots\mathbb{Q}(\zeta_{p_s^{\max(k_s,\ell_s)}}) \\
=& \mathbb{Q}(\zeta_{p_1^{\max(k_1,\ell_1)}p_s^{\max(k_s,\ell_s)}}) = \mathbb{Q}(\zeta_{[m,n]}).
\end{aligned}$$

同样的计算可以证明 $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(m,n)})$。

习题

练习 4.5.1. 设 m,n 是互素的正整数，ζ_m,ζ_n 分别为 m,n 次本原单位根，证明 $\zeta_m\zeta_n$ 是 mn 次本原单位根。

练习 4.5.2. 设 $K/\mathbb{Q}$ 是一个有限扩张，证明 K 中至多只有有限个单位根。

练习 4.5.3. 设 p 是素数，证明如下等式：

1. 当 $n\geq 2$ 时有 $\Phi_n(x)=x^{\varphi(n)}\Phi_n(1/x)$；
2. $\Phi_{p^r}(x)=\Phi_p(x^{p^{r-1}})$；
3. 当 $n>1$ 是奇数时有，$\Phi_{2n}(x)=\Phi_n(-x)$；
4. 设 $m\mid n$，那么有 $\Phi_{mn}(x)=\Phi_n(x^m)$；
5. 当 $(p,m)=1$ 时有 $\Phi_{p^rm}(x)=\Phi_m(x^{p^r})\Phi_m(x^{p^{r-1}})$。

练习 4.5.4. 求最小的正整数 n 使得存在 $n\times n$ 阶整数矩阵 A 满足 $A^{2025}=I$，且对于所有小于 2025 的正整数 m 均有 $A^m\neq I$。

练习 4.5.5. 给定正整数 r，求最小的正整数 n 使得存在 $n\times n$ 阶整数矩阵 A 满足 $A^r=I$，且对于所有小于 r 的正整数 m 均有 $A^m\neq I$。

练习 4.5.6. 设自然数 n 至多有两个奇素因子，则分圆多项式 $\Phi_n(x)$ 的系数只能是 $0,\pm1$。

注 13. 上述命题的逆命题是不成立的，$\Phi_{255255}(x)$ 的系数均为 $0,\pm1$，但 $255255=3\times5\times7\times11\times13\times17$。

练习 4.5.7. 任何整数都可做分圆多项式的系数。

练习 4.5.8. 设 ℓ,p 是两个素数，设 ζ 是一个 ℓ 次本原单位根。本题的目标是研究 $\Phi_\ell(x)$ 在模 p 下的分解。

1. 若 $p=\ell$，那么 $\Phi_\ell(x)=(x-1)^{\ell-1}\in\mathbb{F}_\ell[x]$。
2. 假设 $p\neq\ell$，设 m 是 p 在模 ℓ 下的阶。证明 ζ 在 $\mathbb{F}_p$ 中的极小多项式的次数是 m。
3. 证明对任意不被 ℓ 整除的整数 a 均有 $\mathbb{F}_p(\zeta)=\mathbb{F}_p(\zeta^a)$。由此证明在 $\mathbb{F}_p[x]$ 中，$\Phi_\ell(x)$ 可以分解为 $\frac{\ell-1}{m}$ 个次数为 m 的不可约多项式的乘积。

练习 4.5.9. 设 n 是一个正整数，本题的目标是证明存在无穷多个素数 p 使得 $p\equiv1\pmod n$。

1. 取一个整系数的非常数多项式 $f(x)$，证明集合 $\{d\in\mathbb{N}\mid$ 存在 k 使得 d 是 $f(k)$ 的因子$\}$ 是无限集。
2. 取 $f(x)=\frac{x^n-1}{\Phi_n}\in\mathbb{Z}[x]$，证明存在素数 p 及整数 k 使得 p 整除 $\Phi_n(k)$ 但 p 不整除 $f(k)$。
3. 计算 k 在 $(\mathbb{Z}/p\mathbb{Z})^*$ 中的阶，并由此证明 $p\equiv1\pmod n$。
4. 证明存在无穷多个素数 p 使得 $p\equiv1\pmod n$。

注 14. 本题是著名的 Dirichlet 定理的特例：对任意互素的正整数 n,m，存在无穷多个素数使得 $p\equiv m\pmod n$。

4.6 Galois 理论

4.6.1 Galois 扩张

定义 4.6.1. 设 K/F 是一个域扩张，K 到自身的同构被称为**自同构**，所有的自同构组成的集合记为 $\mathrm{Aut}(K)$。设 $\sigma \in \mathrm{Aut}(K)$，若对任意 $a \in F$ 均有 $\sigma(a) = a$，那么我们称 σ **固定** F，并记所有固定 F 的自同构组成的集合为 $\mathrm{Aut}(K/F)$。

例 4.6.2. 容易验证 $\mathrm{Aut}(\mathbb{Q})$ 和 $\mathrm{Aut}(\mathbb{F}_p)$ 都是平凡的，而 $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$ 则不是平凡的。事实上，$\mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$ 有两个元素，一个是恒等映射，另一个是 $a + b\sqrt{2} \mapsto a - b\sqrt{2}$。

和群的自同构群类似，域的自同构群在映射的复合运算下也构成一个群。

命题 4.6.3. 设 K/F 是一个域扩张，那么 $\mathrm{Aut}(K)$ 构成一个群，并且 $\mathrm{Aut}(K/F)$ 是其一个子群。

命题 4.6.4. 设 K/F 是一个域扩张，$a \in K$ 在 F 上是代数的。那么对任意 $\sigma \in \mathrm{Aut}(K/F)$，$\sigma(a)$ 是 a 在 F 上的极小多项式的根。

上述性质表明 $\mathrm{Aut}(K/F)$ 可视作不可约多项式的根之间的一个置换。这便是 Galois 理论中的核心思想。但是我们要注意到 a 的共轭根不一定能从 $\sigma(a)$ 得到，因为一般情况下 K 不一定包含 a 的所有共轭根。

例 4.6.5. 设 $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$，容易看出 σ 完全由其在 $\sqrt[3]{2}$ 上的作用决定。而 $\sqrt[3]{2}$ 的极小多项式为 $x^3 - 2$，因此 $\sigma(\sqrt[3]{2})$ 也只能是 $x^3 - 2$ 的根，但是容易看出 $x^3 - 2$ 的另外两个根并不在 $\mathbb{Q}(\sqrt[3]{2})$ 中，因此我们必有 $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$，即有 σ 是恒等映射，所以 $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$。

命题 4.6.6. 设 $H \leq \mathrm{Aut}(K)$ 是 K 的自同构群的一个子群，那么 $\{a \in K \mid \sigma(a) = a, \forall \sigma \in H\}$ 是 K 的一个子域，该子域被称为 H 的**固定域**。

命题 4.6.7. 设 $F_1 \subseteq F_2 \subseteq K$ 是 K 的两个子域，那么我们有 $\mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$；反之，若 $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ 是 $\mathrm{Aut}(K)$ 的两个子群，F_1, F_2 分别为 H_1, H_2 对应的固定域，那么我们有 $F_2 \subseteq F_1$。

到目前为止我们得到了域 K 的子域和 $\mathrm{Aut}(K)$ 的子群之间的一个对应，为了更进一步研究这个对应关系，我们需要尽可能的多从 $\mathrm{Aut}(K)$ 中得到更多的信息，然而从前面的例子中我们发现 $\mathrm{Aut}(K)$ 有可能是平凡群，此时我们无法从 $\mathrm{Aut}(K)$ 中得到任何有意义的信息。究其原因，我们发现这是因为 K 没有包含 $x^3 - 2$ 的其余根，这便引导我们考虑那些包含了足够多的自同构的域，即 K 应该为某个多项式的分裂域。

定义 4.6.8. 设 K/F 是一个有限扩张，若 $|\mathrm{Aut}(K/F)| = [K : F]$，我们称 K 在 F 上是 **Galois 的**，或者 K/F 是一个 **Galois 扩张**，并称 $\mathrm{Aut}(K/F)$ 为 K/F 的 **Galois 群**，记作 $\mathrm{Gal}(K/F)$。

在给出 Galois 扩张更多性质之前，我们先计算几个例子。

例 4.6.9. 根据例4.6.2可知 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是 *Galois* 扩张，其 *Galois* 群同构于 $\mathbb{Z}/2\mathbb{Z}$。类似地，设 D 是任意非完全平方数，那么 $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ 都是 *Galois* 扩张，并且 *Galois* 群都同构于 $\mathbb{Z}/2\mathbb{Z}$。而例4.6.5表明 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是 *Galois* 扩张。

例 4.6.10. 下面我们考虑域扩张 $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$。容易看出 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 上的自同构完全由 $\sqrt{2},\sqrt{3}$ 的像决定。而 $\sqrt{2},\sqrt{3}$ 的像只能为它们的共轭根，即为 $\pm\sqrt{2},\pm\sqrt{3}$。因此总共有如下四种情况。

$$\sigma_1:\begin{cases}\sqrt{2}&\mapsto\sqrt{2}\\ \sqrt{3}&\mapsto\sqrt{3}\end{cases},\quad \sigma_2:\begin{cases}\sqrt{2}&\mapsto-\sqrt{2}\\ \sqrt{3}&\mapsto\sqrt{3}\end{cases},\quad \sigma_3:\begin{cases}\sqrt{2}&\mapsto\sqrt{2}\\ \sqrt{3}&\mapsto-\sqrt{3}\end{cases},\quad \sigma_4:\begin{cases}\sqrt{2}&\mapsto-\sqrt{2}\\ \sqrt{3}&\mapsto-\sqrt{3}.\end{cases}$$

以上四个映射均可延拓为 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 上的自同构。因此 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ 是 4 阶群。另一方面，容易验证 σ_1 是单位元，而 $\sigma_2,\sigma_3,\sigma_4$ 的阶均为 2，因此 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$。

例 4.6.11. 另一个不平凡的例子是 $\mathbb{Q}(\sqrt[3]{2},\rho)/\mathbb{Q}$。它是多项式 x^3-2 的分裂域。容易看出来 $\mathbb{Q}(\sqrt[3]{2},\rho)$ 的自同构完全由 $\sqrt[3]{2}$ 和 ρ 的像决定。而 $\sqrt[3]{2}$ 的共轭根为 $\sqrt[3]{2},\rho\sqrt[3]{2},\rho^2\sqrt[3]{2}$，$\rho$ 的共轭根为 ρ,ρ^2。因此共有如下六种可能：

$$\sigma_1:\begin{cases}\sqrt[3]{2}&\mapsto\sqrt[3]{2}\\ \rho&\mapsto\rho\end{cases},\quad \sigma_2:\begin{cases}\sqrt[3]{2}&\mapsto\sqrt[3]{2}\\ \rho&\mapsto\rho^2\end{cases},\quad \sigma_3:\begin{cases}\sqrt[3]{2}&\mapsto\rho\sqrt[3]{2}\\ \rho&\mapsto\rho\end{cases},$$

$$\sigma_4:\begin{cases}\sqrt[3]{2}&\mapsto\rho^2\sqrt[3]{2}\\ \rho&\mapsto\rho\end{cases},\quad \sigma_5:\begin{cases}\sqrt[3]{2}&\mapsto\rho\sqrt[3]{2}\\ \rho&\mapsto\rho^2\end{cases},\quad \sigma_6:\begin{cases}\sqrt[3]{2}&\mapsto\rho^2\sqrt[3]{2}\\ \rho&\mapsto\rho^2.\end{cases}$$

可以验证这六个映射均可延拓为 $\mathbb{Q}(\sqrt[3]{2},\rho)$ 的自同构，事实上，它们的像可以显式的写出来。例如，由于 $\{1,\sqrt[3]{2},\sqrt[3]{4},\rho,\rho\sqrt[3]{2},\rho\sqrt[3]{4}\}$ 构成 $\mathbb{Q}(\sqrt[3]{2},\rho)$ 在 $\mathbb{Q}$ 上的一组基，那么 σ_2 即可延拓为

$$\sigma_2: a+b\sqrt[3]{2}+c\sqrt[3]{4}+d\rho+e\rho\sqrt[3]{2}+f\rho\sqrt[3]{4}=a-e\sqrt[3]{2}+(f-c)\sqrt[3]{4}+d\rho+(b-e)\rho\sqrt[3]{2}-c\rho\sqrt[3]{4}.$$

因此 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\rho)/\mathbb{Q})$ 是一个 6 阶群，显然 σ_1 是单位元。而 σ_2,σ_3 的阶分别为 $2,3$。根据定义可知

$$\sigma_3\sigma_2(\sqrt[3]{2})=\sigma_3(\sqrt[3]{2})=\rho\sqrt[3]{2},\quad \sigma_3\sigma_2(\rho)=\sigma_3(\rho^2)=\rho^2,$$

而

$$\sigma_2\sigma_3^2(\sqrt[3]{2})=\sigma_2\sigma_3(\rho\sqrt[3]{2})=\sigma_2(\rho^2\sqrt[3]{2})=\rho\sqrt[3]{2},\quad \sigma_2\sigma_3^2(\rho)=\sigma_2(\rho)=\rho^2.$$

由此可知 $\sigma_3\sigma_2=\sigma_2\sigma_3^2$。因此我们有

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\rho)/\mathbb{Q})=\langle\sigma_2,\sigma_3\rangle\simeq S_3.$$

下面我们探讨一下什么样的扩张会是 Galois 扩张。

定理 4.6.12. 设 K/F 是一个有限域扩张，那么我们有 $|\mathrm{Aut}(K/F)|\le[K:F]$。

证明. 我们对 $[K_1:F_1]$ 进行归纳。当 $[K_1:F_1]=1$ 时，我们有 $K_1=F_1,K_2=F_2$。此时延拓只有 φ 自己。下面假设 $[K_1:F_1]>1$。设 $p(x)$ 是 $f(x)$ 的一个不可约因式，那么 $\varphi(p)(x)$ 是 $\varphi(f)(x)$ 的不可约因式。设 $\alpha\in K_1$ 是 $p(x)$ 的一个根。设 $\sigma:K_1\to K_2$ 是 φ 的一个延拓，$\tau=\sigma|_{F_1(\alpha)}$。那么 $\tau:F_1(\alpha)\to F_2(\tau(\alpha))$ 是一个同构，并且该同构完全由 $\tau(\alpha)$ 决定。另一方面，我们知道 $\tau(\alpha)$ 一定是 $\varphi(p)(x)$ 的一个根。由此我们可以得到如下图表：

$$\begin{array}{lccc}\sigma: & K_1 & \xrightarrow{\sim} & K_2\\ & \big| & & \big|\\ \sigma: & F_1(\alpha) & \xrightarrow{\sim} & F_2(\tau(\alpha))\\ & \big| & & \big|\\ \sigma: & F_1 & \xrightarrow{\sim} & F_2\end{array}$$

反之，根据定理4.3.6可知对任意 $\varphi(p)(x)$ 的任意一个根 β，我们均可以构造满足上面图表的同构 $\tau: F_1(\alpha) \to F_2(\beta)$ 及 $\sigma: K_1 \to K_2$ 使得 $\tau(\alpha) = \beta$。由此可知我们只需计算上面图表的个数，便可得知延拓的个数。而由上面的讨论知将 φ 延拓为 $\tau:$ 的个数等于 $\varphi(p)(x)$ 的不同根的个数，至多等于 $[F_1(\alpha): F_1]$，并且取等号的充要条件是 $\varphi(p)(x)$ 在 K_2 中有 $\deg p$ 个互不相同的根。而对于每一个同构 $\tau: F_1(\alpha) \to F_2(\beta)$，根据归纳假设知它至多可以延拓为 $[K_1: F_1(\alpha)]$ 个同构 $\sigma: K_1 \to K_2$，并且等号成立的充要条件是 K_1 是 $F_1(\alpha)$ 的分裂域。

上述定理告诉我们 $\mathrm{Aut}(K/F)$ 的阶会被 $[K: F]$ 控制住，因此要考虑 K/F 何时是 Galois 扩张，只需考虑等号何时成立即可。作为推论我们可以给出 Galois 扩张的一个判定条件。

推论 4.6.13. *设 K 是 F 上某个可分多项式 $f(x)$ 的分裂域，那么 K/F 是 Galois 的。*

一个自然的问题是什么样的域上的多项式一定是可分的? 根据多项式的理论我们知道多项式是否有重根和其导函数相关，因此利用形式导数的概念，我们可以给出如下两个结论。

命题 4.6.14. *若 F 的特征是 0，那么 F 上的任意不可约多项式都是可分的。*

证明. 设 $f(x) \in F[x]$ 是一个不可约多项式，由于 F 的特征是 0，因此 $\deg f' = n - 1$。若 $f(x)$ 有重根，那么 $f(x)$ 和 $f'(x)$ 有公因式，这与 $f(x)$ 不可约矛盾。故 $f(x)$ 是可分的。

例4.4.2告诉我们上述结论对特征 p 的域不成立，但是该结论对有限域仍然成立。

命题 4.6.15. *设 $\mathbb{F}_q$ 是一个有限域，那么 $\mathbb{F}_q$ 上的任意不可约多项式均是可分的。*

证明. 设 $f(x) \in \mathbb{F}_q[x]$ 是不可约的，若 $f'(x)$ 是非零多项式，那么和前面的证明类似，我们可以得到 $f(x)$ 是可分的。因此我们假设 $f'(x)$ 是零多项式。根据形式导数的定义可知当 $p \nmid n$ 时，$f(x)$ 中 x^n 前的系数必为 0，于是我们不妨设

$$f(x) = a_m x^{mp} + a_{m-1} x^{(m-1)p} + \cdots + a_1 x^p + a_0.$$

由于映射 $\mathbb{F}_p \to \mathbb{F}_p$，$x \mapsto x^p$ 是单射，故它必是双射。因此存在 $b_i \in \mathbb{F}_q$ 使得 $b_i^p = a_i$。因此我们有

$$\begin{aligned} f(x) &= (b_m x^m)^p + (b_{m-1} x^{m-1})^p + \cdots + (b_1 x)^p + b_0^p \\ &= (b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0)^p. \end{aligned}$$

然而这与 $f(x)$ 不可约矛盾。

命题4.6.14和4.6.15表明若 F 是特征 0 或有限域，那么它的有限扩张一定是可分扩张。本文将主要讨论可分扩张，不对不可分扩张做过多的探讨。另一方面，推论4.6.13的逆命题也是成立的，下面我们将证明它的逆命题。

命题 4.6.16. *设 $G \subseteq \mathrm{Aut}(G)$ 是一个有限群，并设 F 是 G 的固定域。那么我们有 $|G| = [K: F]$ 且 $G = \mathrm{Gal}(K/F)$。*

证明. 由于 $G \subseteq \mathrm{Aut}(K/F)$，根据定理4.6.12知 $|G| \leq [K:F]$。若 $|G| < [K:F]$，记 $n = |G|$，并设 $G = \{\tau_1, \tau_2, \ldots, \tau_n\}$。再取 $\alpha_1, \alpha_2, \ldots, \alpha_{n+1} \in K$ 使得它们在 F 上是线性无关的。考虑如下矩阵

$$A = \begin{pmatrix} \tau_1(\alpha_1) & \tau_1(\alpha_2) & \cdots & \tau_1(\alpha_{n+1}) \\ \tau_2(\alpha_1) & \tau_2(\alpha_2) & \cdots & \tau_2(\alpha_{n+1}) \\ \vdots & \vdots & & \vdots \\ \tau_n(\alpha_1) & \tau_n(\alpha_2) & \cdots & \tau_n(\alpha_{n+1}) \end{pmatrix}.$$

由于 $\mathrm{rank}(A) \leq n$，故 A 的列向量是线性相关的，不妨设 k 是使得某些列向量线性相关的最少向量个数，并不妨假设 A 的前 k 列线性相关。因此存在 $c_i \in K$ 使得

$$c_1\tau_i(\alpha_1) + c_2\tau_i(\alpha_2) + \cdots + c_k\tau_i(\alpha_k) = 0, \qquad i = 1, 2, \ldots, n. \tag{4.6}$$

由 k 的最小性可知所有的 c_i 均不等于 0，故不妨设 $c_1 = 1$。任取 $\sigma \in G$，由于 $\sigma G = G$，故将 σ 作用在(4.6)中的 n 个等式可得

$$\sigma(c_1)\tau_i(\alpha_1) + \sigma(c_2)\tau_i(\alpha_2) + \cdots + \sigma(c_k)\tau_i(\alpha_k) = 0, \qquad i = 1, 2, \ldots, n.$$

联合等式(4.6)可得

$$(c_2 - \sigma(c_2))\tau_i(\alpha_2) + \cdots + (c_k - \sigma(c_k))\tau_i(\alpha_k) = 0, \qquad i = 1, 2, \ldots, n.$$

由 k 的最小性可知 $c_2 - \sigma(c_2) = \cdots = c_k - \sigma(c_k) = 0$。由于该式对任意 $\sigma \in G$ 均成立，因此有 $c_2, \ldots, c_k \in F$。然而此时再由等式(4.6)可得

$$\tau_i(c_1\alpha_1 + c_2\alpha_2 + \ldots c_k\alpha) = 0.$$

这表明 $c_1\alpha_1 + c_2\alpha_2 + \ldots c_k\alpha = 0$，但是这与 $\alpha_1, \alpha_2, \ldots, \alpha_k$ 线性无关矛盾。因此我们有 $|G| = [K:F]$。由于 $G \subseteq \mathrm{Aut}(K/F)$ 且 $|\mathrm{Aut}(K/F)| \leq [K:F]$，因此我们有 K/F 是 Galois 扩张，且 $G = \mathrm{Gal}(K/F)$。

引理 4.6.17. *设 K/F 是有限 Galois 扩张，设 $f(x) \in F[x]$ 是 F 上的不可约多项式，若 $f(x)$ 在 K 中有一个根，那么 $f(x)$ 在 K 中是完全分裂的。*

证明. 设 α 是 $f(x)$ 在 K 中的一个根，记 $G = \mathrm{Gal}(K/F) = \{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n\}$。考虑元素

$$\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha), \tag{4.7}$$

不妨设 $\alpha, \alpha_2, \ldots, \alpha_r$ 是其中互不相同的元素，并设 $g(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_r)$。对任意 $\tau \in G$，τ 可视作(4.7)的一个置换，因此也是 $\alpha, \alpha_2, \ldots, \alpha_r$ 的一个置换，故 τ 也固定 $g(x)$ 的所有系数，由 τ 的任意性知 $g(x) \in F[x]$。由于 $f(x)$ 是不可约的，并且 $f(x)$ 和 $g(x)$ 有公共根，因此必有 $f(x) \mid g(x)$。另一方面，将 $f(x), g(x)$ 视作 $K[x]$ 中的多项式，则显然有 $g(x) \mid f(x)$。因此有 $f(x) = g(x)$。特别地，$f(x)$ 是可分多项式并且所有根都在 K 中。

最后我们证明推论4.6.13的逆命题也成立。

定理 4.6.18. *设 K/F 有限扩张，则 K/F 是 Galois 的当且仅当 K 是 F 上某个可分多项式的分裂域。*

证明. 设 $\alpha_1, \alpha_2, \ldots, \alpha_n$ 是 K/F 上的一组基。于是由引理4.6.17它们的极小多项式 $m_{\alpha_i,F}(x)$ 是可分的，且根均在 K 中，于是将它们中重复的去掉以后相乘得到的多项式记为 $f(x)$。显然 $f(x)$ 的根均在 K 中，另一方面，由于 α_i 均是 $f(x)$ 的根，因此 $f(x)$ 的分裂域包含 K。故 K 是 $f(x)$ 在 F 上的分裂域。

4.6.2 Galois 对应

最后我们给出 Galois 理论的基本定理。

定理 4.6.19. 设 K/F 是一个 *Galois* 扩张，$G = \mathrm{Gal}(K/F)$ 为其 *Galois* 群。那么我们有如下一一对应关系：

$$\left\{\begin{array}{ll} & K \\ K \text{ 中包含} & | \\ F \text{ 的子域 } E & E \\ & | \\ & F \end{array}\right\} \longleftrightarrow \left\{\begin{array}{ll} & 1 \\ & | \\ G \text{ 的子群 } H & H \\ & | \\ & G \end{array}\right\}$$

$$\begin{array}{ccc} E & \longrightarrow & \{G \text{ 中固定 } E \text{ 的自同构}\} \\ \{H \text{ 的固定域}\} & \longleftarrow & H \end{array}$$

该对应关系满足如下性质：

1. 假设 E_1, E_2 对应的是 H_1, H_2，那么 $E_1 \subseteq E_2$ 当且仅当 $H_2 \leq H_1$；
2. $[K : E] = |H|$ 且 $[E : F] = |G : H|$；
3. K/E 一定是 *Galois* 的，其 *Galois* 群为 $\mathrm{Gal}(K/E) = H$；
4. E/F 是 *Galois* 的当且仅当 H 是 G 的正规子群。在这种情况下，我们有 $\mathrm{Gal}(E/F) \simeq G/H$；

证明. 给定 G 的两个子群 $H_2 \leq H_1$，它们的固定域分别为 E_1, E_2。那么对任意 $x \in E_1$，及任意 $\sigma \in H_1$ 均有 $\sigma(x) = x$。特别地，对任意 $\sigma \in H_2$ 均有 $\sigma(x) = x$，这表明 $x \in E_2$，因此 $E_1 \subseteq E_2$。反之，给定 K 中包含 F 的两个子域 $E_1 \subseteq E_2$，其对应的自同构群为 H_1, H_2，那么对任意 $\sigma \in H_2$，σ 均固定 E_2 中的元素，因此也固定 E_1 中的元素，于是 $\sigma \in H_1$，即有 $H_2 \leq H_1$。这便证明了 (1)，由此立即得到上述 Galois 对应是一一对应关系。

若 E 是子群 H 的固定域，根据命题4.6.16可知 $|H| = [K : E]$ 及 $|G| = [K : F]$。由此可得 $|G : H| = |G|/|H| = [E : F]$。这便证明了 (2)。

由 $[K : E] = |H|$ 可立刻得到 (3)。

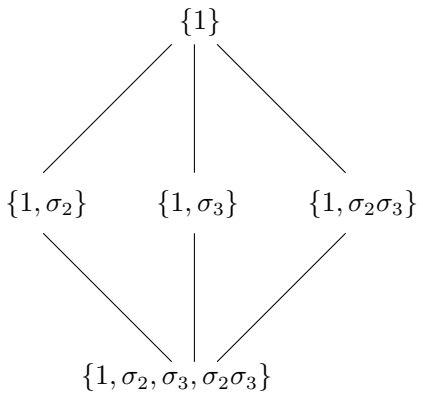
假设 H 是 G 的正规子群，E 是其固定域。任取 $x \in E$，并设 x' 是 x 在 K 中的任意一个共轭根。由于 K/F 是 Galois 的，因此存在 $\sigma \in G$ 使得 $\sigma(x) = x'$。对任意 $\tau \in H$ 有 $\tau(x') = \sigma(\sigma^{-1}\tau\sigma(x))$。由于 H 是正规子群且 H 固定 E 中所有元素，因此有 $\sigma^{-1}\tau\sigma(x) = x$。于是 $\tau(x') = \sigma(x) = x'$，由 τ 的任意性可知 $x' \in E$。因此 x 的所有共轭根都在 E 中。最后取 E/F 的一组基 $\alpha_1, \ldots, \alpha_r$，于是在去掉它们的极小多项式 $m_{\alpha_1,F}(x), \ldots, m_{\alpha_r,F}(x)$ 中重复的后，将其相乘得到 $f(x)$，由于 K/F 是可分的，于是 $f(x)$ 是可分的，而 E 是 $f(x)$ 的分裂域，因此由定理4.6.18可知 E/F 是 Galois 的。

反之，假设 E/F 是 Galois 的，考虑映射 $\varphi : G \to \mathrm{Gal}(E/F)$，$\varphi(\sigma) = \sigma|_E$。容易验证 φ 是定义良好的且是一个群同态。而 φ 的核为

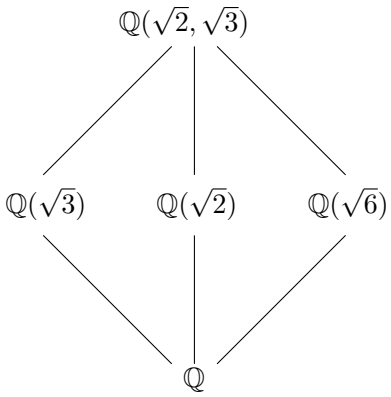
$$\ker\varphi = \{\sigma \in G \mid \sigma|_E = \mathrm{id}\} = \mathrm{Gal}(K/E) = H.$$

因此 H 是 G 的正规子群。最后由 (2) 知 $|G/H| = [E : F] = |\mathrm{Gal}(E/F)|$。因此我们由同构基本定理有 $\mathrm{Gal}(E/F) \simeq G/H$。

例 4.6.20. 最后我们考虑例4.6.10和例4.6.11中的 *Galois* 对应。根据例4.6.10,我们知道 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$。因此它共有 1 个 1 阶子群，3 个 2 阶子群，以及 1 个四阶子群，具体展示如下图

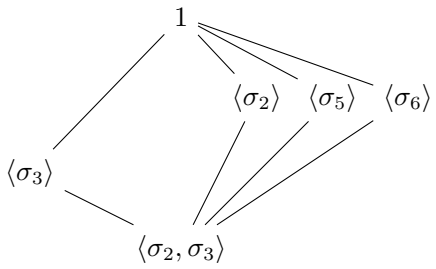


而它们对应的固定域则如下图所展示的：

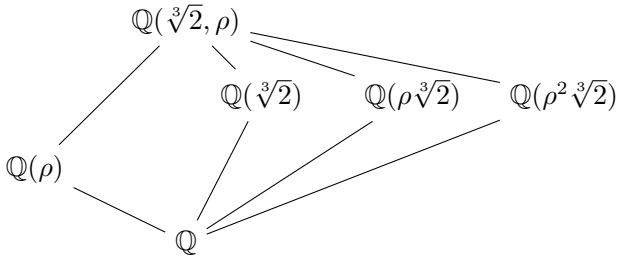


在这种情况下，$\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ 的 *Galois* 群是交换群，因此它的所有子群均为正规子群，所以它的中间域都是 $\mathbb{Q}$ 上的 *Galois* 扩张。

例4.6.11中的情况则会复杂一些。我们知道 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\rho)/\mathbb{Q})$ 同构于 S_3，因此它有 1 个 1 阶子群，3 个 2 阶子群，1 个 3 阶子群以及 1 个 6 阶子群，具体展示如下图：



而它们对应的固定域则如下图所展示：



在这种情况下，$\mathbb{Q}(\sqrt[3]{2},\rho)/\mathbb{Q}$ 的 *Galois* 群不是交换群，而它的二阶子群都不是正规子群，所以对应的三个三次扩域 $\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q}(\rho\sqrt[3]{2}),\mathbb{Q}(\rho^2\sqrt[3]{2})$ 都不是 $\mathbb{Q}$ 上的 *Galois* 扩张。而唯一的一个三阶子群是正规子群，所以其对应的二次扩域 $\mathbb{Q}(\rho)$ 是 $\mathbb{Q}$ 上的 *Galois* 扩张。

4.6.3 有限域的 Galois 群

这一节我们讨论有限域的 Galois 群。在有限域 $\mathbb{F}_{p^n}$ 中有一个非常重要的同构，被称之为 **Frobenius 自同构**，它是将 x 映为 x^p。一般来说这样的映射既不会是同态，也不会是满射，因为域中的元素一般不能开 p-次方。但是在有限域这个特殊的情况下，它会是一个同构。

定理 4.6.21. 有限域 $\mathbb{F}_{p^n}/\mathbb{F}_p$ 的 *Galois* 群同构于 $\mathbb{Z}/n\mathbb{Z}$，*Frobenius* 自同构 $\sigma_p : x \mapsto x^p$ 是其一个生成元。并且 $\mathbb{F}_{p^n}$ 的子域为 $\mathbb{F}_{p^d}$，其中 d 为 n 的因子，其为 σ_p^d 的固定域。

证明. 根据定理4.4.7可知 $\mathbb{F}_{p^n}$ 是可分多项式 $x^{p^n}-x$ 的分裂域，因此由定理4.6.18可知 $\mathbb{F}_{p^n}/\mathbb{F}_p$ 是 Galois 扩张。

根据引理4.4.6可知 σ_p 是域同态。由于 $x^p=0$ 只有一个 p-重根 $x=0$，故 σ_p 是单射，从而 σ_p 是双射。这表明 σ_p 是一个自同构，从而对任意 $0\le k\le n-1$，σ_p^k 都是 $\mathbb{F}_{p^n}$ 上的自同构，并且它们互不相同。否则会存在小于 n 的正整数 m 使得 σ_p^m 是恒等映射，即对任意 $x\in\mathbb{F}_{p^n}$ 均有 $x^{p^m}=x$，但是这个方程至多只有 p^m 个解，由此得到矛盾。另一方面，我们知道 $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|=[\mathbb{F}_{p^n}:\mathbb{F}_p]=n$。故 $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)=\{\sigma_p^k \mid 0\le k\le n-1\}\simeq\mathbb{Z}/n\mathbb{Z}$。

最后，由于 $\mathbb{Z}/n\mathbb{Z}$ 的子群均形如 $d\mathbb{Z}/n\mathbb{Z}$，其中 d 是 n 的因子，因此最后一个结论由 Galois 基本定理4.6.19即可得到。

4.6.4 分圆域的 Galois 群

下面我们讨论分圆域的 Galois 群。设 ζ_n 是一个 n-次本原单位根，那么根据定理4.5.4可知它的极小多项式即为 $\Phi_n(x)$，因此它的共轭根均形如 ζ_n^k，并且 $\mathbb{Q}(\zeta_n)$ 即为 $\Phi_n(x)$ 的分裂域。所以 $\mathbb{Q}(\zeta_n)$ 的自同构均由 ζ_n 的像完全决定。另一方面，设正整数 $1\le a<n$ 且与 n 互素，记 σ_a 为由 $\sigma_a(\zeta_n)=\zeta_n^a$ 所延拓得到的自同构。容易看出 σ_a 仅依赖于 a 模 n 的剩余类。因此我们有如下定理。

定理 4.6.22. $\mathbb{Q}(\zeta_n)$ 的 *Galois* 群同构于 $(\mathbb{Z}/n\mathbb{Z})^*$，并且该同构由如下映射给出

$$\begin{array}{ccc}(\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ a \pmod n & \longmapsto & \sigma_a.\end{array}$$

证明. 该定理的证明是直接的。对任意 $a,b\in(\mathbb{Z}/n\mathbb{Z})^*$，我们有

$$(\sigma_a\sigma_b)(\zeta_n)=\sigma_b(\zeta_n^b)=\zeta_n^{ab}=\sigma_{ab}(\zeta_n),$$

即有 $\sigma_a\sigma_b=\sigma_{ab}$。因此上述映射是同态。而 σ_a 是恒等映射当且仅当 $\sigma_a(\zeta)=\zeta$，即有 $a\equiv 1\pmod n$。故该映射是单射。而 $(\mathbb{Z}/n\mathbb{Z})^*$ 和 $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ 的阶均为 $\varphi(n)$。故该映射是同构。

例 4.6.23. 设 K 是 $\mathbb{Q}$ 上包含 n-次单位根的域，下面我们计算多项式 x^n-a 在 K 上的 *Galois* 群，其中 a 是一个有理数。事实上，由于 K 包含 n-次单位根，因此 x^n-a 在 K 上的分裂域即为 $K(\sqrt[n]{a})$ 并且 $\sqrt[n]{a}$ 的共轭跟都形如 $\sqrt[n]{a}\zeta_n$。设 $\sigma\in\mathrm{Gal}(K(\sqrt[n]{a})/K)$，那么 σ 完全由它在 $\sqrt[n]{a}$ 上的作用决定。因此存在唯一的 k_σ 使得 $\sigma(\sqrt[n]{a})=\sqrt[n]{a}\zeta_n^{k_\sigma}$。由此我们可以得到同态

$$\begin{array}{ccc}\mathrm{Gal}(K(\sqrt[n]{a})/K) & \longrightarrow & \mu_n\\ \sigma & \longmapsto & \zeta_n^{k_\sigma}.\end{array}$$

于是 $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ 同构于 μ_n 的一个子群，而 μ_n 是 n-阶循环群，它的所有子群恰好为 μ_m，其中 $m\mid n$。由此我们得到同构：$\mathrm{Gal}(K(\sqrt[n]{a})/K)\simeq\mu_m$，其中 $m=[K(\sqrt[n]{a}):K]$。

例 4.6.24. 根据上述定理我们知道

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{17})/\mathbb{Q})\simeq(\mathbb{Z}/17\mathbb{Z})^*.$$

容易知道 $(\mathbb{Z}/17\mathbb{Z})^*$ 是 16 阶循环群，其一个生成元是 $\overline{3}$。另一方面我们知道 16 阶循环群恰好有一个阶分别为 $1,2,4,8,16$ 的子群，下面具体展示了这五个子群：

$$H_1=\{\overline{1}\},\quad H_2=\{\overline{1},\overline{16}\},\quad H_4=\{\overline{1},\overline{4},\overline{13},\overline{16}\},\quad H_8=\{\overline{1},\overline{2},\overline{4},\overline{8},\overline{9},\overline{13},\overline{15},\overline{16}\},\quad H_{16}=(\mathbb{Z}/17\mathbb{Z})^*.$$

如果我们记

$$a_1=\zeta_{17}+\zeta_{17}^2+\zeta_{17}^4+\zeta_{17}^8+\zeta_{17}^9+\zeta_{17}^{13}+\zeta_{17}^{15}+\zeta_{17}^{16},\quad b_1=\zeta_{17}+\zeta_{17}^4+\zeta_{17}^{13}+\zeta_{17}^{16},\quad c_1=\zeta_{17}+\zeta_{17}^{16},$$

那么 H_1,H_2,H_4,H_8,H_{16} 的固定域分别为

$$K_1=\mathbb{Q}(\zeta_{17}),\quad K_2=\mathbb{Q}(c_1),\quad K_4=\mathbb{Q}(b_1),\quad K_8=\mathbb{Q}(a_1),\quad \mathbb{Q}.$$

这五个域在 $\mathbb{Q}$ 上的扩张次数分别为 $16,8,4,2,1$，并且有 $\mathbb{Q}\subseteq K_8\subseteq K_4\subseteq K_3\subseteq K_2\subseteq K_1$。因此由定理 4.2.1 可知 ζ_{17} 是可构造的，即正 17 边形是可通过尺规作图得到的。该结论最早由 *Gauss* 证明的。更进一步，我们记

$$a_2=\zeta_{17}^3+\zeta_{17}^5+\zeta_{17}^6+\zeta_{17}^7+\zeta_{17}^{10}+\zeta_{17}^{11}+\zeta_{17}^{12}+\zeta_{17}^{14},\quad b_2=\zeta_{17}^2+\zeta_{17}^8+\zeta_{17}^9+\zeta_{17}^{15},$$

$$b_3=\zeta_{17}^6+\zeta_{17}^7+\zeta_{17}^{10}+\zeta_{17}^{11},\quad b_4=\zeta_{17}^3+\zeta_{17}^5+\zeta_{17}^{12}+\zeta_{17}^{14},\quad c_2=\zeta_{17}^4+\zeta_{17}^{13}.$$

那么我们可以证明 a_1,a_2 是方程 $x^2+x-4=0$ 的两个根，b_1,b_2 是方程 $x^2-a_1x-1=0$ 的两个根，b_3,b_4 是方程 $x^2-a_2x-1=0$ 的两个根，c_1,c_2 是方程 $x^2-b_1x+b_4=0$ 的两个根。由此可以给出 $c_1=2\cos\frac{2\pi}{17}$ 的具体表达式为：

$$\frac{1}{8}\left(-1+\sqrt{17}+\sqrt{2(17-\sqrt{17})}+2\sqrt{17+3\sqrt{17}-\sqrt{2(17-\sqrt{17})}-2\sqrt{2(17+\sqrt{17})}}\right).$$

更一般地，利用和上述例子相同的方法我们可以得到正 n-边形可通过尺规作图得到的充要条件。

定理 4.6.25. *正 n-边形可通过尺规作图得到当且仅当 $n=2^k p_1\cdots p_s$，其中 p_i 是互不相同的素数，并且均形如 $2^{2^\ell}+1$。*

前几个形如 $2^{2^\ell}+1$ 的素数分别为 $2^1+1=3, 2^2+1=5, 2^4+1=17, 2^8+1=257, 2^{16}+1=65537$。这类素数被称为 **Fermat 素数**，当时 Fermat 猜测所有形如 $2^{2^\ell}+1$ 的数都是素数，然而 Euler 证明了 $2^{32}+1=641\times 6700417$ 不是素数。到目前为止，已知的Fermat 素数[1]也仅有前面所列出来的 5 个，因此大家猜测是否只有有限个 Fermat 素数。

由上述定理我们可以看出分圆域的 Galois 群均为 Abel 群，这种 Galois 群是 Abel 群的扩张我们称之为 **Abel 扩张**。Galois 理论中一个重要的问题就是什么样的群可以成为 $\mathbb{Q}$ 上某个 Galois 扩张的 Galois 群。对于 Abel 群的情况，我们可以给出完整的回答。

定理 4.6.26. *设 G 是一个有限 Abel 群，那么存在一个包含 $\mathbb{Q}$ 的域 K 使得 $\mathrm{Gal}(K/\mathbb{Q})\simeq G$。*

证明. 设 G 的阶为 n，由有限 Abel 群的结构定理2.6.11可知存在正整数 $n_1, n_2, \ldots, n_s$ 使得

$$G\simeq \mathbb{Z}^r\times \mathbb{Z}/n_1\mathbb{Z}\times \mathbb{Z}/n_2\mathbb{Z}\times\cdots\times \mathbb{Z}/n_s\mathbb{Z},$$

根据 Dirichlet 定理（见习题4.5.9）我们知道对任意正整数 m 均存在无穷个素数 p 使得 $p\equiv 1 \pmod m$。因此我们取不同的素数 $p_1, p_2, \ldots, p_s$ 使得 $p_i\equiv 1 \pmod{n_i}$。于是 $\mathbb{Z}/n_i\mathbb{Z}$ 同构于 $\mathbb{Z}/(p_i-1)\mathbb{Z}\simeq(\mathbb{Z}/p_i\mathbb{Z})^*$ 的子群。令 $n=p_1p_2\ldots p_s$，由中国剩余定理3.2.17我们有

$$(\mathbb{Z}/n\mathbb{Z})^*\simeq(\mathbb{Z}/p_1\mathbb{Z})^*\times(\mathbb{Z}/p_2\mathbb{Z})^*\times\cdots\times(\mathbb{Z}/p_s\mathbb{Z})^*.$$

因此 G 同构于 $(\mathbb{Z}/n\mathbb{Z})^*$ 的一个子群。由定理4.6.22有 $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})\simeq(\mathbb{Z}/n\mathbb{Z})^*$。因此由 Galois 对应定理4.6.19知存在 $\mathbb{Q}(\zeta_n)$ 的子域 K 使得 $\mathrm{Gal}(K/\mathbb{Q})\simeq G$。

反过来，任意一个 $\mathbb{Q}$ 上的 Abel 扩张均可均可嵌入到某个分圆域中。

定理 4.6.27 (Kronecker-Weber)**.** *设 K 是 $\mathbb{Q}$ 上的有限 Abel 扩张，那么存在 m 使得 $K\subseteq\mathbb{Q}(\zeta_m)$。*

4.6.5 低次多项式的 Galois 群

这一节我们主要讨论多项式的 Galois 群。设 $f(x)$ 是 $\mathbb{Q}$ 上的多项式，那么它的 Galois 群即为它的分裂域在 $\mathbb{Q}$ 上的 Galois 群。设 $f(x)$ 的一个分裂域为 K，$\alpha_1, \ldots, \alpha_n$ 是 $f(x)$ 的 n 个根。对任意 $\sigma\in\mathrm{Gal}(K/F)$，它一定将 α_i 映射到某个 α_j（j 可能和 i 相等），并且不同的根的像不同。这意味着我们可以将 σ 视为 $\{1,2,\ldots,n\}$ 的一个置换。由此我们可以将 $\mathrm{Gal}(K/F)$ 视为 S_n 的一个子群。在计算多项式的 Galois 群时，下面定义的判别式是一个重要的概念：

$$D=\prod_{i<j}(\alpha_i-\alpha_j)^2.$$

命题 4.6.28. *$f(x)$ 的 Galois 群是 A_n 的子群当且仅当判别式 $D\in\mathbb{Q}^2$。*

[1] https://oeis.org/A000215.

计算 $\mathbb{Q}$ 上的二次、三次及四次多项式的 Galois 群。通过简单的变量替换，我们可以只需要讨论首一整系数的多项式即可。

设 $f(x)=x^2+ax+b\in\mathbb{Z}[x]$ 是二次不可约多项式，记 $D=a^2-4b$。于是 D 不是完全平方数，并且 $f(x)$ 的分裂域即为 $\mathbb{Q}(\sqrt{D})$。根据例4.6.9可知其 Galois 群同构于 $\mathbb{Z}/2\mathbb{Z}$。

下面考虑三次多项式的情况，设 $f(x)=x^3+ax^2+bx+c\in\mathbb{Z}[x]$ 是三次不可约多项式，通过变量替换 $x=y-a/3$，我们可以得到 $g(y)=y^3+py+q$，其中 $p=b-a^2/3, q=(2a^3-9ab+27c)/27$。容易看出 $f(x)$ 和 $g(y)$ 的分裂域和判别式都是相同的。设 $\alpha_1,\alpha_2,\alpha_3$ 是 $g(y)$ 的三个解，直接计算可以得到判别式为

$$D=(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^3=-4p^3-27q^2.$$

代入 $p=b-a^2/3, q=(2a^3-9ab+27c)/27$ 可以得到 $f(x)$ 的判别式为

$$D=a^2b^2-4b^3-4a^3c-27c^2+18abc.$$

习题

练习 4.6.1. 设 $\sigma:\mathbb{C}\to\mathbb{C}$ 定义为 $\sigma(z)=\overline{z}$，证明 $\sigma\in\mathrm{Aut}(\mathbb{C})$，并求 σ 的固定域。

练习 4.6.2. 求 $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2}))$。

练习 4.6.3. 本题的目标是计算 $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$。

1. 设 $\sigma\in\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$，证明对任意 $a>0$ 有 $\sigma(a)>0$。
2. 证明若 $-\frac{1}{m}<a-b<\frac{1}{m}$，则有 $-\frac{1}{m}-\sigma(a)-\sigma(b)<\frac{1}{m}$。由此证明 σ 是 $\mathbb{R}$ 上的连续函数。
3. 证明 σ 是恒等映射。

练习 4.6.4. 设 K 是一个域，证明 $\mathrm{Aut}(K(t)/K)\simeq\mathrm{GL}_2(K)/\{\pm I_2\}$，其同构由如下对应给出

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\longleftrightarrow\left(f(t)\mapsto f\left(\frac{at+b}{ct+d}\right)\right).$$

计算自同构 $f(t)\mapsto f(t+1)$ 的固定域。(提示：利用练习4.1.19)

练习 4.6.5. 设 L/K 是一个域扩张，且 $K\subsetneq L\subseteq K(x)$。

1. 证明 x 在 L 上是代数的。
2. 假设 $P(T)=T^n+F_{n-1}T^{n-1}+\cdots+F_0\in L[T]$ 是 x 在 L 上的极小多项式。证明存在 i 使得 $F_i\notin K$。
3. 证明 $L=K(F_i)$。
4. 是否存在有理函数 $F(x)\in K(x)$ 使得 $F\circ F\circ\cdots\circ F=x$？

练习 4.6.6. 求下列多项式在 $\mathbb{Q}$ 上的 *Galois* 群

(1). x^3-5, (2). x^4-2

练习 4.6.7. 设 $K=\mathbb{Q}(\sqrt[8]{2},\mathrm{i}), F_1=\mathbb{Q}(\mathrm{i}), F_2=\mathbb{Q}(\sqrt{2}), F_3=\mathbb{Q}(\sqrt{-2})$。证明

$$\mathrm{Gal}(K/F_1)\simeq\mathbb{Z}/8\mathbb{Z},\quad \mathrm{Gal}(K/F_2)\simeq D_8,\quad \mathrm{Gal}(K/F_3)\simeq Q_8$$

练习 4.6.8. 设 $a=\sqrt{5+\sqrt{21}}$, $K=\mathbb{Q}(a)$。

1. 证明 $K/\mathbb{Q}$ 是 *Galois* 扩张；
2. 求 $\mathrm{Gal}(K/\mathbb{Q})$；
3. 求 K 的所有子域；
4. $\mathbb{Q}(\sqrt{5+\sqrt{37}})/\mathbb{Q}$ 是否是 *Galois* 的？
5. $\mathbb{Q}(\sqrt{5+\sqrt{15}})/\mathbb{Q}$ 是否是 *Galois* 的？

练习 4.6.9. 写出 $\mathbb{Q}(\zeta_{12})$ 的所有子域。

练习 4.6.10. 设 $d\in\mathbb{N},\zeta=\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}}$。设 A 为 $d-1$ 阶的方阵，其 (i,j) 位置元素为 $a_{ij}=\zeta^{ij}-\zeta^{(i-1)j}$。证明 $\det(A^2)\in\mathbb{Z}$。当 $d\equiv 0,3\pmod 4$ 时，证明 $\det(A)\notin\mathbb{Z}$。

练习 4.6.11. 设 $P(x)=x^4+ax^2+b$ 是 $\mathbb{Q}$ 上的不可约多项式，K 是 $P(x)$ 在 $\mathbb{Q}$ 上的一个分裂域。记 $\pm\alpha,\pm\beta$ 是 $P(x)$ 在 K 中的根。

1. 证明 $\mathrm{Gal}(K/\mathbb{Q})$ 同构于 D_8 的一个子群。
2. 证明 $\mathrm{Gal}(K/\mathbb{Q})$ 只能同构于如下三个群之一

$$\mathbb{Z}/4\mathbb{Z},\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},D_8.$$

3. 证明 $\alpha^2-\beta^2\notin\mathbb{Q}$。
4. 证明 $\mathrm{Gal}(K/\mathbb{Q})\simeq\mathbb{Z}/4\mathbb{Z}$ 当且仅当 $\frac{\alpha}{\beta}-\frac{\beta}{\alpha}\in\mathbb{Q}$；$\mathrm{Gal}(K/\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ 当且仅当 $\alpha\beta\in\mathbb{Q}$
5. 计算下列多项式的 *Galois* 群，并计算其分裂域的所有子域。

$$(i)\ x^4-4x^2-1,\qquad (ii)\ x^4-6x^2+4,\qquad (iii)\ x^4+5x^2+5.$$

练习 4.6.12. 设 K/F 是一个有限扩张，

1. 若 $\sigma_1,\dots,\sigma_n\in\mathrm{Aut}(K/F)$ 两两不同，那么 $\sigma_1,\dots,\sigma_n$ 在 K 上线性无关，即若 $x_1,\dots,x_n\in K$ 满足 $x_1\sigma_1+\cdots+x_n\sigma_n=0$，那么必有 $x_1=\cdots=x_n=0$。
2. 证明 $|\mathrm{Aut}(K/F)|\le[K:F]$。

练习 4.6.13. 设 $p_1,p_2,\dots,p_n$ 是 n 个两两不同的素数。

1. 证明扩张 $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})/\mathbb{Q})$ 是 *Galois* 扩张，记 G 为其 *Galois* 群；
2. 证明 G 中任意非单位元素的阶都是 2，由此证明存在整数 r 使得 $G\simeq(\mathbb{Z}/2\mathbb{Z})^r$；
3. 通过计算 $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ 的二次子域的个数证明 $G\simeq(\mathbb{Z}/2\mathbb{Z})^n$。

练习 4.6.14 (Hilbert 90 定理)**.** 设 L/K 是一个有限 *Galois* 扩张，$G=\mathrm{Gal}(L/K)$。

1. 假设 $\mathrm{Gal}(L/K)$ 是 n 次循环群，σ 为一个生成元，$x\in L$。证明 $\prod_{\tau\in\mathrm{Gal}(L/K)}\tau(x)=1$ 当且仅当存在 $y\in L^*$ 使得 $x=\sigma(y)/y$；
2. 若不假设 $\mathrm{Gal}(L/K)$ 是循环的。设函数 $f:\mathrm{Gal}(L/K)\to L^*$ 满足对任意 $\tau_1,\tau_2\in\mathrm{Gal}(L/K)$ 有 $f(\tau_1\tau_2)=\tau_1(f(\tau_2))f(\tau_1)$。证明存在 $x\in L^*$ 使得对任意 $\tau\in\mathrm{Gal}(L/K)$ 均有 $f(\tau)=\tau(x)x^{-1}$。

练习 4.6.15 (Artin-Schreier 扩张)**.** 设 K 是特征 $p>0$ 的域，L/K 是 p 次 *Galois* 扩张。设 σ 是 $\mathrm{Gal}(L/K)$ 的一个生成元。

1. 证明存在 $x\in L$ 使得 $\sigma(x)-x=1$；
2. 证明存在 $a\in K^*$ 使得 L 是 X^p-X-a 的分裂域。

练习 4.6.16. 设 p 是一个素数，$a\in\mathbb{F}_p$，设 $f(x)=x^p-x-a\in\mathbb{F}_p[x]$。

1. 若 $a=0$，将 $f(x)$ 分解为不可约多项式的乘积。

   下面假设 $a\neq 0$。
2. 证明 $f(x+1)=f(x)$。
3. 设 $g(x)$ 是 $f(x)$ 的一个不可约因式，证明 $g(x+1)$ 也是 $f(x)$ 的不可约因式。
4. 证明 $g(x+1)=g(x)$。
5. 证明若多项式 $h(x)\in\mathbb{F}_p[x]$ 的次数小于 p 且 $h(x+1)=h(x)$，那么 $h(x)$ 是常数多项式，由此证明 $f(x)$ 是不可约的。
6. 设 $b\in\mathbb{Z}$ 和 p 互素，证明 x^p-x-b 在 $\mathbb{Q}[x]$ 中不可约。

练习 4.6.17. 设 Ω 是一个特征 0 的代数闭域。设 K 是 Ω 的一个子域且 Ω/K 是有限扩张。下面我们将证明 $\Omega=K(\sqrt{-1})$。设 i 是 x^2+1 在 Ω 中的一个根，记 $G=\mathrm{Gal}(\Omega/K(i))$。

1. 证明 Ω/K 是 *Galois* 扩张；
2. 若 G 是非平凡的，设 p 是 $|G|$ 的一个素因子。证明存在 Ω 的子域 L 使得 Ω/L 是 p 次 *Galois* 扩张且 L 包含 $K(i)$；
3. 证明存在 $a\in L$ 使得 $P(x)=x^p-a$ 在 L 上是不可约的且 Ω 是 $P(x)$ 的分裂域；
4. 设 $\alpha\in\Omega$ 是 $P(x)$ 的一个根，计算 $N_{\Omega/L}(\alpha)$；
5. 证明 $\Omega=K(i)$；
6. 证明 $\mathrm{Aut}(\bar{\mathbb{Q}}/\mathbb{Q})$ 中的有限阶非平凡元素一定是二阶的。

练习 4.6.18. 设 p 是一个素数，$K=\mathbb{F}_p(T)$。考虑多项式 $f(x)=x^p-Tx-T, g(x)=x^{p-1}-T$。

1. 证明 f,g 在 K 上是不可约且可分的；
2. 令 M 为 g 在 K 上的分裂域。证明 $\mathrm{Gal}(M/K)$ 同构于 $\mathbb{F}_p^*$；
3. 令 L 为 f 在 K 上的分裂域。证明 g 在 L 中分裂，且 $\mathrm{Gal}(L/K)\simeq\mathbb{F}_p\rtimes\mathbb{F}_p^*$，其中 $\mathbb{F}^*$ 在 $\mathbb{F}_p$ 上的作用为乘法。