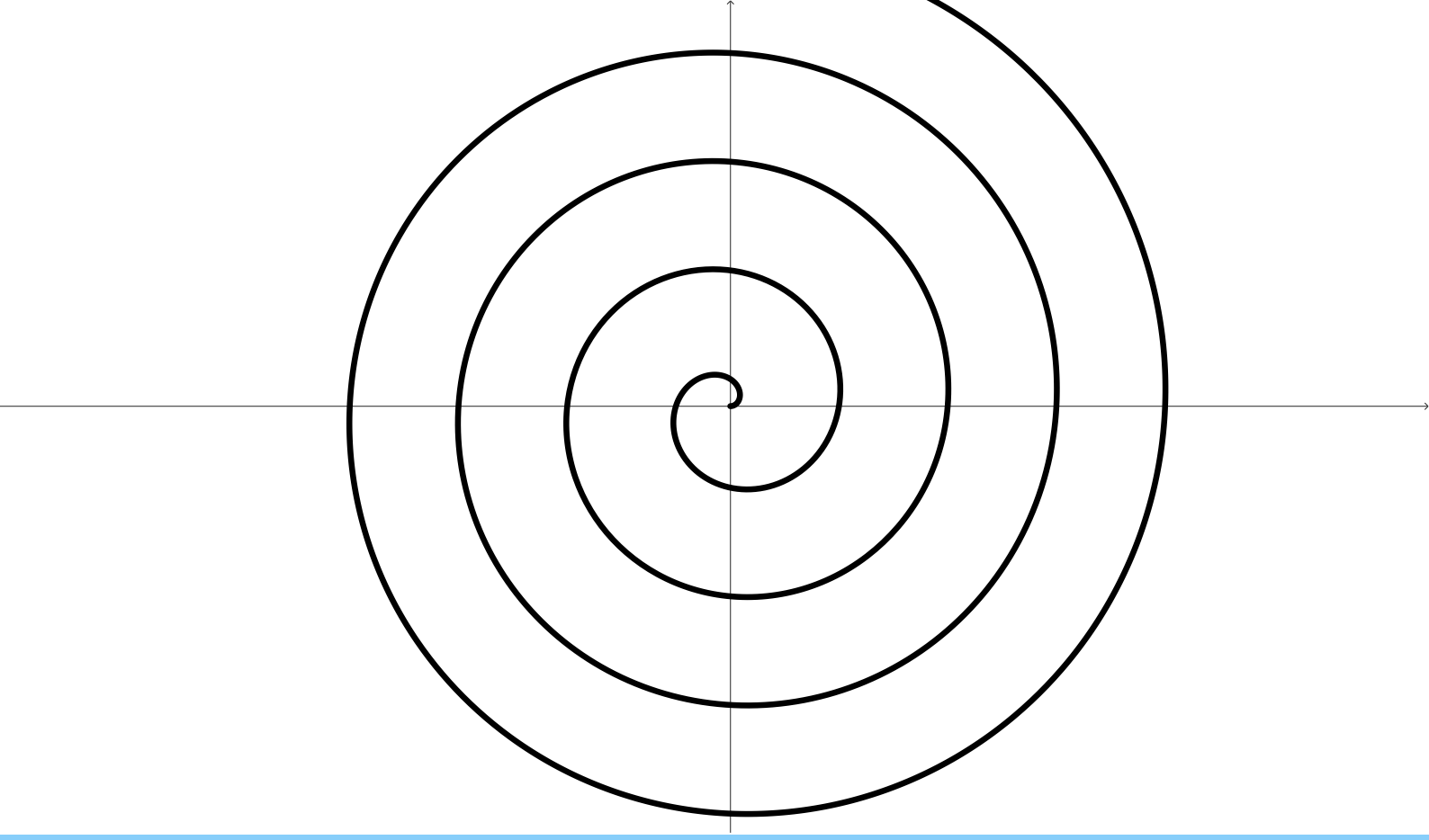

Galois 理论 - 笔记

作者：若水
邮箱：ethanmxzhou@163.com
主页：helloethanzhou.github.io
时间：July 20, 2024

Après cela, il y aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.

— Evariste Galois

目录

第一章 Galois 扩张

1.1 Galois 对应

定义 1.1.1 (域扩张)

对于域 k 与 K，称 K/k 为域扩张，如果存在同态映射 $\varphi: k \to K$。

定义 1.1.2 (中间域)

对于域扩张 $k \subset F \subset K$，称 F 为 K/k 的中间域。

定义 1.1.3 (自同构群)

定义域 K 的自同构群为

$$\mathrm{Aut}(K) = \{\text{同构映射}\varphi: K \to K\}$$

定义 1.1.4 (k-自同构群)

定义域扩张 K/k 的 k-自同构群为

$$\mathrm{Aut}_k(K) = \{\text{同构映射}\varphi: K \to K \mid \varphi(x) = x, \forall x \in k\}$$

证明 我们来证明 $\mathrm{Aut}_k(K)$ 关于映射的复合构成群。

对于封闭性，任取 $\varphi, \psi \in \mathrm{Aut}_k(K)$，由于 $\varphi, \psi: K \to K$ 为同构映射，那么 $\varphi \circ \psi: K \to K$ 为同构映射。由于 $\varphi|_k = \psi|_k = \mathbb{1}_k$，那么 $(\varphi \circ \psi)_k = \mathbb{1}_k$，进而 $\varphi \circ \psi \in \mathrm{Aut}_k(K)$。

对于单位元，显然 $\mathbb{1}_K \in \mathrm{Aut}_k(K)$，且对于任意 $\varphi \in \mathrm{Aut}_k(K)$，成立

$$\varphi \circ \mathbb{1}_K = \mathbb{1}_K \circ \varphi = \varphi$$

因此 $\mathbb{1}_K$ 为 $\mathrm{Aut}_k(K)$ 的单位元。

对于逆元，任取 $\varphi \in \mathrm{Aut}_k(K)$，显然 $\varphi^{-1}: K \to K$ 成立

$$\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \mathbb{1}_K$$

因此 φ^{-1} 为 φ 的逆元。

对于交换律，这对映射的复合显然是成立的。

综上所述，$\mathrm{Aut}_k(K)$ 关于映射的复合构成群。

定义 1.1.5 (不动域)

对于域扩张 K/k，定义子群 $G < \mathrm{Aut}_k(K)$ 的不动域为

$$\mathrm{Inv}_K(G) = \{x \in K \mid \varphi(x) = x, \forall \varphi \in G\}$$

证明 我们来证明 $\mathrm{Inv}_K(G)$ 构成域。

显然 $\mathrm{Aut}_k(K)$ 对加法和乘法封闭，这是因为 $\varphi(x+y) = \varphi(x) + \varphi(y)$ 且 $\varphi(xy) = \varphi(x)\varphi(y)$。

显然 K 的加法单位元 0 和乘法单位元 1 分别为 $\mathrm{Inv}_K(G)$ 的加法单位元和乘法单位元，这是因为 $0, 1 \in k$。

对于任意 $x \in K$，显然 x 在 K 中的加法逆元 $-x$ 和乘法逆元 x^{-1}（此时要求 $x \neq 0$）分别为 x 在 $\mathrm{Inv}_K(G)$ 中的加法逆元和乘法逆元，这是因为对于 $\varphi \in G$，$\varphi(-x) = -x$ 且 $\varphi(x^{-1}) = \varphi(x)^{-1}$。

显然 $\mathrm{Aut}_k(K)$ 对于加法和乘法满足交换律和结合律以及分配律，这是因为 K 对于加法和乘法满足交换律和结合律以及分配律。

综上所述，$\mathrm{Inv}_K(G)$ 构成域。

定义 1.1.6 (Galois 对应)

称域扩张 K/k 的 Galois 对应为

$$\{\text{域扩张}K/k\text{的中间域}\} \longleftrightarrow \{\text{自同构群}\mathrm{Aut}_k(K)\text{的子群}\}$$
$$F \longmapsto \mathrm{Aut}_F(K)$$
$$\mathrm{Inv}_K(G) \longmapsfrom G$$

♣

证明 任取 K/k 的中间域 F，对于任意 $\sigma \in \mathrm{Aut}_F(K)$，那么 $\sigma : K \to K$ 为同构映射，且 $\sigma|_F = \mathbb{1}_F$。由于 $k \subset F$，因此 $\sigma|_k = \mathbb{1}_k$，于是 $\sigma \in \mathrm{Aut}_k(K)$，进而 $\mathrm{Aut}_F(K) \subset \mathrm{Aut}_k(K)$。由 k-自同构群的定义1.1.4，$\mathrm{Aut}_F(K)$ 构成群，进而 $\mathrm{Aut}_F(K)$ 为 $\mathrm{Aut}_k(K)$ 的子群。

任取 $\mathrm{Aut}_k(K)$ 的子群 G，由不动域的定义1.1.5，$\mathrm{Aut}_F(K)$ 构成 K 的子域。而由 k-自同构群的定义1.1.4，$k \subset \mathrm{Aut}_F(K)$，进而 $\mathrm{Aut}_F(K)$ 构成 K/k 的中间域。

定义 1.1.7 (Galois 群)

定义域扩张 K/k 关于中间域 F 的 Galois 群为

$$\mathrm{Gal}(K/F) = \mathrm{Aut}_F(K)$$

♣

注 为了方便，对于域扩张 K/k 的 Galois 对应，引入记号

$$\mathscr{F} = \{\text{域扩张}K/k\text{的中间域}\},\quad \mathscr{G} = \{\text{自同构群}\mathrm{Aut}_k(K)\text{的子群}\},\quad \mathrm{Gal}(F) = \mathrm{Gal}(K/F),\quad \mathrm{Inv}(G) = \mathrm{Inv}_K(G)$$

引理 1.1.8

对于域扩张 K/k，Galois 对应 $\mathrm{Gal} : \mathscr{F} \to \mathscr{G}$ 与 $\mathrm{Inv} : \mathscr{G} \to \mathscr{F}$ 为反序映射，换言之——

1. 对于 $F_1, F_2 \in \mathscr{F}$，如果 $F_1 \subset F_2$，那么 $\mathrm{Gal}(F_1) \supset \mathrm{Gal}(F_2)$。
2. 对于 $G_1, G_2 \in \mathscr{G}$，如果 $G_1 \subset G_2$，那么 $\mathrm{Inv}(G_1) \supset \mathrm{Inv}(G_2)$。

♡

证明 对于 1，任取 $F_1, F_2 \in \mathscr{F}$，使其成立 $F_1 \subset F_2$。任取 $\varphi \in \mathrm{Gal}(F_2)$，那么 $\varphi : K \to K$ 为同构映射，且 $\varphi|_{F_2} = \mathbb{1}_{F_2}$，因此 $\varphi|_{F_1} = \mathbb{1}_{F_1}$，进而 $\varphi \in \mathrm{Gal}(F_1)$。由 φ 的任意性，$\mathrm{Gal}(F_1) \supset \mathrm{Gal}(F_2)$。

对于 2，任取 $G_1, G_2 \in \mathscr{G}$，使其成立 $G_1 \subset G_2$。任取 $x \in \mathrm{Inv}(G_2)$，那么对于任意 $\varphi \in G_2$，成立 $\varphi(x) = x$，因此对于任意 $\varphi \in G_1$，成立 $\varphi(x) = x$，进而 $x \in \mathrm{Inv}(G_1)$。由 x 的任意性，$\mathrm{Inv}(G_1) \supset \mathrm{Inv}(G_2)$。

引理 1.1.9

对于域扩张 K/k 的 Galois 对应 $\mathrm{Gal} : \mathscr{F} \to \mathscr{G}$ 与 $\mathrm{Inv} : \mathscr{G} \to \mathscr{F}$，如果 $F \in \mathscr{F}$ 且 $G \in \mathscr{G}$，那么

$$F \subset \mathrm{Inv}(\mathrm{Gal}(F)),\qquad G \subset \mathrm{Gal}(\mathrm{Inv}(G))$$

♡

证明 对于左式，由于

$$\begin{aligned} x \in F &\Longrightarrow (x \in K)\text{且}(\forall\text{同构映射}\varphi : K \to K \quad (\varphi|_F = \mathbb{1}_F \Longrightarrow \varphi(x) = x)) \\ &\Longleftrightarrow (x \in K)\text{且}(\forall \varphi \in \mathrm{Gal}(F), \varphi(x) = x) \\ &\Longleftrightarrow x \in \mathrm{Inv}(\mathrm{Gal}(F)) \end{aligned}$$

那么 $F \subset \mathrm{Inv}(\mathrm{Gal}(F))$。

对于右式，由于

$$\begin{aligned} \varphi \in G &\Longrightarrow (\varphi : K \to K\text{为同构映射})\text{且}(\forall x \in K \quad ((\forall \psi \in G, \psi(x) = x) \Longrightarrow \varphi(x) = x)) \\ &\Longleftrightarrow (\varphi : K \to K\text{为同构映射})\text{且}(\forall x \in \mathrm{Inv}(G), \varphi(x) = x) \\ &\Longleftrightarrow \varphi \in \mathrm{Gal}(\mathrm{Inv}(G)) \end{aligned}$$

那么 $G \subset \mathrm{Gal}(\mathrm{Inv}(G))$。

引理 1.1.10

对于域扩张 K/k 的 Galois 对应 $\mathrm{Gal}:\mathscr{F}\to\mathscr{G}$ 与 $\mathrm{Inv}:\mathscr{G}\to\mathscr{F}$，成立

$$\mathrm{Gal}\circ\mathrm{Inv}\circ\mathrm{Gal}=\mathrm{Gal},\qquad \mathrm{Inv}\circ\mathrm{Gal}\circ\mathrm{Inv}=\mathrm{Inv}$$

♡

证明 对于左式，任取 $F\in\mathscr{F}$，则 $\mathrm{Gal}(F)\in\mathscr{G}$。一方面，由引理1.1.9，$\mathrm{Gal}(F)\subset\mathrm{Gal}(\mathrm{Inv}(\mathrm{Gal}(F)))$，即 $\mathrm{Gal}(F)\subset(\mathrm{Gal}\circ\mathrm{Inv}\circ\mathrm{Gal})(F)$。另一方面，由引理1.1.9，$F\subset\mathrm{Inv}(\mathrm{Gal}(F))$。又由引理1.1.8，$\mathrm{Gal}F\supset\mathrm{Gal}(\mathrm{Inv}(\mathrm{Gal}(F)))$，即 $\mathrm{Gal}F\supset(\mathrm{Gal}\circ\mathrm{Inv}\circ\mathrm{Gal})(F)$。综合两方面，$\mathrm{Gal}F=(\mathrm{Gal}\circ\mathrm{Inv}\circ\mathrm{Gal})(F)$。由 F 的任意性，$\mathrm{Gal}\circ\mathrm{Inv}\circ\mathrm{Gal}=\mathrm{Gal}$。

对于右式，任取 $G\in\mathscr{G}$，则 $\mathrm{Inv}(G)\in\mathscr{F}$。一方面，由引理1.1.9，$\mathrm{Inv}(G)\subset\mathrm{Inv}(\mathrm{Gal}(\mathrm{Inv}(G)))$，即 $\mathrm{Inv}(G)\subset(\mathrm{Inv}\circ\mathrm{Gal}\circ\mathrm{Inv})(G)$。另一方面，由引理1.1.9，$G\subset\mathrm{Gal}(\mathrm{Inv}(F))$。又由引理1.1.8，$\mathrm{Inv}G\supset\mathrm{Inv}(\mathrm{Gal}(\mathrm{Inv}(F)))$，即 $\mathrm{Inv}(G)\supset(\mathrm{Inv}\circ\mathrm{Gal}\circ\mathrm{Inv})(G)$。综合两方面，$\mathrm{Inv}(G)=(\mathrm{Inv}\circ\mathrm{Gal}\circ\mathrm{Inv})(G)$。由 G 的任意性，$\mathrm{Inv}\circ\mathrm{Gal}\circ\mathrm{Inv}=\mathrm{Inv}$。

1.2 Artin 引理

引理 1.2.1 (Artin 引理)

对于域 K，如果 $G<\mathrm{Aut}(K)$ 且 $|G|<\infty$，那么

$$[K:\mathrm{Inv}(G)]\le|G|$$

♡

证明 设 $|G|=n$，若要证明 $[K:\mathrm{Inv}_(G)]\le n$，只需证明 K 中任意 $n+1$ 个元素 $u_1,\cdots,u_{n+1}$ 必然 $\mathrm{Inv}(G)$-线性相关。记 $G=\{\varphi_1,\cdots,\varphi_n\}$，其中 $\varphi_1=\mathbb{1}_K$。考虑 K 上的齐次线性方程

$$\begin{pmatrix}\varphi_1(u_1)&\cdots&\varphi_1(u_{n+1})\\ \vdots&\ddots&\vdots\\ \varphi_n(u_1)&\cdots&\varphi_n(u_{n+1})\end{pmatrix}\begin{pmatrix}x_1\\ \vdots\\ x_{n+1}\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$$

由齐次线性方程解的判定，该齐次线性方程存在非零解，取其中非零分量数最少的非零解为 $(a_1,\cdots,a_{n+1})$。必要时调换诸 u_k 与 x_k 的下标，使得 $a_1\neq0$；进而，不妨 $a_1=1$。

断言：诸 $a_k\in\mathrm{Inv}(G)$。从而由线性方程的第一行

$$a_1u_1+\cdots a_{n+1}u_{n+1}=0$$

可知 $u_1,\cdots,u_{n+1}$ 为 $\mathrm{Inv}(G)$-线性相关的。

如果此断言不成立，不妨 $a_2\notin\mathrm{Inv}(G)$，则存在 $\varphi_t\in G$，使得成立 $\varphi_t(a_2)\neq a_2$。将 φ_t 作用于线性方程，可得

$$\begin{pmatrix}(\varphi_t\circ\varphi_1)(u_1)&\cdots&(\varphi_t\circ\varphi_1)(u_{n+1})\\ \vdots&\ddots&\vdots\\ (\varphi_t\circ\varphi_n)(u_1)&\cdots&(\varphi_t\circ\varphi_n)(u_{n+1})\end{pmatrix}\begin{pmatrix}\varphi_t(x_1)\\ \vdots\\ \varphi_t(x_{n+1})\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$$

由于 G 为群且诸 $\varphi_k:K\to K$ 为同构映射，因此 $\varphi_t\circ\varphi_1,\cdots,\varphi_t\circ\varphi_n$ 为 $\varphi_1,\cdots,\varphi_n$ 的置换，从而 $(\varphi_t(a_1)=1,\varphi_t(a_2),\cdots,\varphi_t(a_{n+1}))$ 亦为齐次线性方程的解。而 $(1,\cdots,a_{n+1})$ 为齐次线性方程的解，因此

$$(0,a_2-\varphi_t(a_2),\cdots,a_{n+1}-\varphi_t(a_{n+1}))$$

亦为齐次线性方程的解。由 $\varphi_t(a_2)\neq a_2$，此为非零解，且其非零分量数比 $(1,\cdots,a_{n+1})$ 的非零分量数要少，这与 $(1,\cdots,a_{n+1})$ 的取法矛盾！

1.3 Dedekind 无关性引理

定义 1.3.1 (K-线性特征标)

对于群 G 与域 K，称群同态映射 $\chi : G \to K^\times$ 为 G 的 K-线性特征标。

♣

引理 1.3.2 (Dedekind 无关性引理)

如果 $\chi_1, \cdots, \chi_n$ 为群 G 的互异 K-线性特征标，那么 $\chi_1, \cdots, \chi_n$ 在域 K 上线性无关；换言之，若存在 $c_1, \cdots, c_n \in K$，使得成立 $\sum_{i=1}^{n} c)i\chi_i = 0$，那么 $c_1 = \cdots = c_n = 0$。

♡

证明

命题 1.3.3

如果 K/k 为有限扩张，那么 $|\mathrm{Gal}(K/k)| \le [K : k]$。

♠

证明

1.4 有限 Galois 扩张

定义 1.4.1 (Galois 扩张)

称域扩张 K/k 为 Galois 扩张，如果 K/k 为可分且正规的域扩张。

♣

定理 1.4.2 (有限 Galois 扩张)

如下命题等价。

1. K/k 为有限、可分、正规的域扩张。
2. 存在 k 上的可分多项式 $f(x)$，使得 K 为 $f(x)$ 在 k 上的分裂域。
3. K/k 为有限扩张，且 $|\mathrm{Gal}(K/k)| = [K : k]$。
4. $\mathrm{Gal}(K/k)$ 为有限群，且 $\mathrm{Inv}_K(\mathrm{Gal}(K/k)) = k$。

♡

第二章 Galois 理论基本定理

定义 2.0.1 (共轭子群)

称群 G 的子群 H 与 H' 互为共轭子群，如果存在 $g \in G$，使得成立 $H' = gHg^{-1}$。

定义 2.0.2 (共轭中间域)

称域扩张 K/k 的中间域 F 与 F' 互为共轭中间域，如果存在 $\varphi \in \mathrm{Gal}(K/k)$，使得成立 $F' = \varphi(F)$。

定理 2.0.3 (Galois 理论基本定理)

如果域扩张 K/k 为有限 Galois 扩张，那么成立如下命题。

1. Galois 对应 $\mathrm{Gal} : \mathscr{F} \to \mathscr{G}$ 与 $\mathrm{Inv} : \mathscr{G} \to \mathscr{F}$ 为互逆且反序的映射，换言之——
$$\mathrm{Inv} \circ \mathrm{Gal} = \mathbb{1}_{\mathscr{F}}, \qquad \mathrm{Gal} \circ \mathrm{Inv} = \mathbb{1}_{\mathscr{G}}$$
2. $\mathrm{Gal}(K/k)$ 的子群 G 与 G' 互为共轭子群 $\iff$ K/k 的中间域 $\mathrm{Inv}_K(G)$ 与 $\mathrm{Inv}_K(G')$ 互为共轭中间域
3. K/k 的中间域 F 与 F' 互为共轭中间域 $\iff$ $\mathrm{Gal}(K/k)$ 的子群 $\mathrm{Gal}(K/F)$ 与 $\mathrm{Gal}(K/F')$ 互为共轭子群
4. $\mathrm{Gal}(K/k)$ 的子群 G 为正规子群 $\iff$ $\mathrm{Inv}_K(G)/k$ 为正规扩张，此时 $\mathrm{Gal}(\mathrm{Inv}_K(G)/k) \cong \mathrm{Gal}(K/k)/G$
5. 对于域扩张 K/k 的中间域 F，K/F 为正规扩张 $\iff$ $\mathrm{Gal}(K/F)$ 为 $\mathrm{Gal}(K/k)$ 的正规子群。

附录 A 群论

附录 B 环论

附录 C 域论

C.1 基本概念

定义 C.1.1 (域)

称代数系统 $(F,+,\cdot)$ 为域，如果加法运算 $+:F\times F\to F$ 和乘法运算 $\cdot:F\times F\to F$ 成立如下命题。

1. 加法单位元：

$$\exists 0\in F,\forall x\in F,\quad 0+x=x+0=x$$

2. 乘法单位元：

$$\exists 1\in F\backslash\{0\},\forall x\in F,\quad 1x=x1=x$$

3. 加法逆元：

$$\forall x\in F,\exists -x\in F,\quad x+(-x)=(-x)+x=0$$

4. 乘法逆元：

$$\forall x\in F\backslash\{0\},\exists x^{-1}\in F,\quad xx^{-1}=x^{-1}x=1$$

5. 加法交换律：

$$\forall x,y\in F,\quad x+y=y+x$$

6. 乘法交换律：

$$\forall x,y\in F,\quad xy=yx$$

7. 加法结合律：

$$\forall x,y,z\in F,\quad (x+y)+z=x+(y+z)$$

8. 乘法结合律：

$$\forall x,y,z\in F,\quad (xy)z=x(yz)$$

9. 分配律：

$$\forall x,y,z\in F,\quad (x+y)z=xz+yz$$
$$\forall x,y,z\in F,\quad x(y+z)=xy+xz$$

♣

定义 C.1.2 (同态映射)

对于域 F 与 K，称映射 $\varphi:F\to K$ 为同态映射，如果对于任意 $x,y\in F$，成立

$$\varphi(x+y)=\varphi(x)+\varphi(y),\qquad \varphi(xy)=\varphi(x)\varphi(y)$$

♣

这是 GitHub 测试。