推论 2 阶为素数的群是循环群。

定理 17.27 群 G 上的共轭关系是 G 上的等价关系.

定理 17.28 G 是群,C 是 G 的中心,则 $\forall a \in G$ 有

$$a \in C \Leftrightarrow \bar{a} = \{a\}.$$

定理 17.29 G 是群,则 $\forall a \in G$, N(a) 是 G 的子群.

定理 17.30 G 是有限群,则 $\forall a \in G$ 有

$$|\bar{a}| = [G:N(a)].$$

定理 17.31 (群的分类方程) G 是有限群, C 是 G 的中心, 设 G 中至少含有两个元素的共轭类有 k个,且 a_1,a_2,\cdots,a_k 分别为这k个共轭类的代表元素,则

$$|G| = |C| + [G:N(a_1)] + [G:N(a_2)] + \dots + [G:N(a_k)].$$

定理 17.32 N 是群 G 的子群,则下列条件互相等价.

- (1) $N \leqslant G$;
- (2) $\forall q \in G \ f \ qNq^{-1} = N;$
- (3) $\forall g \in G$, $\forall n \in N fgng^{-1} \in N$.

定理 17.33 设 φ 是群 G_1 到 G_2 的同态,则 φ 为单同态当且仅当

$$\ker \varphi = \{e_1\}.$$

定理 17.34 $G_1=\langle a\rangle$ 是循环群, φ 是 G_1 到 G_2 的满同态,则 G_2 也是循环群.

定理 17.35 设 φ 是群 G_1 到 G_2 的同态.

- (1) 若 $H \neq G_1$ 的子群,则 $\varphi(H) \neq G_2$ 的子群.
- (2) 若 $H \neq G_1$ 的正规子群,且 φ 是满同态,则 $\varphi(H)$ 是 G_2 的正规子群.

定理 17.36 设 φ 是群 G_1 到 G_2 的同态,则

(1) $\ker \varphi \not\in G_1$ 的正规子群; (2) $\forall a, b \in G_1, \varphi(a) = \varphi(b) \Leftrightarrow a \ker \varphi = b \ker \varphi.$

定理 17.37 (群同态基本定理) 设 G 是群, H 是 G 的正规子群, 则 G 的商群 G/H 是 G 的同态像. 若 G' 是 G 的同态像, $G \stackrel{\circ}{\sim} G'$, 则

$$G/\ker\varphi\cong G'$$
.

定理 17.38 G 是群,则 $\operatorname{End} G$ 关于映射的合成运算构成一个独异点, $\operatorname{Aut} G$ 关于映身的合成运 算构成一个群.

定理 17.39 G 是群,则 $\operatorname{Inn} G \triangleleft \operatorname{Aut} G$.

定理 17.40 设 G 是群, K 和 L 是 G 的子群, 则 $G = K \times L$ 当且仅当下面的条件成立:

- (1) $K \triangleleft G, L \triangleleft G$; (2) $K \cap L = \{e\}$; (3) G = KL.

定理 17.41 设 G 是群, G_1,G_2,\cdots,G_n 是 G 的子群,则 $G=G_1\times G_2\times\cdots\times G_n$ 当且仅当以下 条件成立:

- (1) $G_i \leq G, i = 1, 2, \dots, n;$
- (2) $G_i \cap G_1 G_2 \cdots G_{i-1} G_{i+1} \cdots G_n = \{e\}, i = 1, 2, \cdots, n;$
- (3) $G = G_1 G_2 \cdots G_n$.

定理 17.42 用 r-电路计算一个 m 元函数至少需要 $\lceil \log_m m \rceil$ 个时间单位.

定理 17.43 设 $\langle \mathbb{Z}_n, \otimes \rangle$ 是群, 若存在 $a \in \mathbb{Z}_n$, $a \neq 0$, 且 a 属于 \mathbb{Z}_n 的每一个非平凡的子群,则对 于任意的模n 加法器T, 总存在着某个输入, 使得T 至少依赖于输入的 $2[\log_2 n]$ 位.