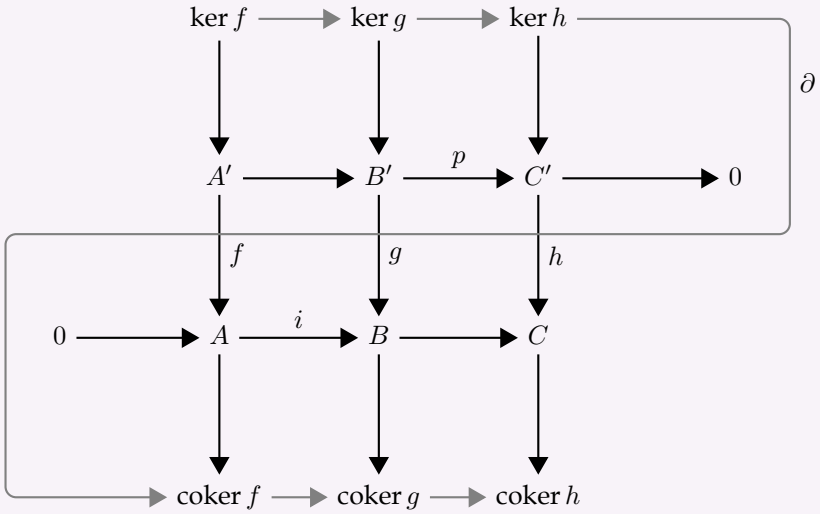
Abstract Algebra

Notes and Exercises



M.m Kay From Chern Class

2023 年 6 月 21 日

前言

这个 Note 是作者在大二学年以朱富海、邓少强老师的抽象代数为主要参考书的学习笔记. 抽象代数 I——邓少强老师，抽象代数 II、Galois 理论——徐彬斌老师.

其中抽象代数 II 和 Galois 理论部分参考了徐彬斌老师的讲义与讲稿，感恩人间天使.

主要参考教材：

1. 抽象代数，邓少强，朱富海；
2. *Abstract Algebra*，Dummit，Foote；
3. 近世代数三百题，冯克勤，章璞.

凯淼淼

2023 年 6 月 21 日

目录

第一章 群论 **1**

1.1 半群与群 . . . 1

1.1.1 Notes . . . 1

1.1.2 Exercises From Z.Fh . . . 3

1.2 子群与陪集 . . . 9

1.2.1 Notes . . . 9

1.2.2 Exercises From Z.Fh . . . 11

1.3 正规子群与商群 . . . 17

1.3.1 Notes . . . 17

1.3.2 Exercises From Z.Fh . . . 18

1.4 群的同态与同构 . . . 21

1.4.1 Notes . . . 21

1.4.2 Exercises From Z.Fh . . . 23

1.5 循环群 . . . 27

1.5.1 Notes . . . 27

1.5.2 Exercises From Z.Fh . . . 27

1.6 对称群与交错群 . . . 30

1.6.1 Notes . . . 30

1.6.2 Exercises From Z.Fh . . . 31

1.6.3 S_n 的自同构群 $\mathrm{Aut}(S_n)$ . . . 33

1.7 群的扩张与 John—Hölder 定理 . . . 35

1.8 可解群和幂零群 . . . 36

1.8.1 Notes . . . 36

1.9 群在集合上的作用 . . . 37

1.9.1 Notes . . . 37

1.9.2 Exercises From Z.Fh . . . 39

1.10 Sylow 定理 . . . 43

1.10.1 Notes . . . 43

1.10.2 Exercises From Z.Fh . . . 48

1.10.3 p-群的性质 . . . 50

1.11 群的直积 . . . 51
1.11.1 群的直积 . . . 51
1.11.2 有限生成的 Abel 群 . . . 53
1.12 群的半直积 . . . 54
1.13 2021 伯苓班抽象代数 I 期中考试 . . . 56
1.14 2022 伯苓班抽象代数 I 期中考试 . . . 59

第二章 环论 61
2.1 环的定义与基本性质 . . . 61
2.1.1 Notes . . . 61
2.1.2 Exercises From Z.Fh . . . 62
2.2 理想与商环 . . . 66
2.2.1 Notes . . . 66
2.2.2 Exercises From Z.Fh . . . 68
2.3 四元数体 . . . 72
2.3.1 Notes . . . 72
2.3.2 Exercises From Z.Fh . . . 72
2.3.3 除环的正规子除环 . . . 73
2.4 环的同态 . . . 75
2.4.1 Notes . . . 75
2.4.2 Exercises From Z.Fh . . . 76
2.4.3 幺环上的中国剩余定理 . . . 80
2.5 整环上的因子分解 . . . 82
2.5.1 Notes . . . 82
2.5.2 Exercises From Z.Fh . . . 85
2.6 素理想与极大理想 . . . 88
2.6.1 Notes . . . 88
2.6.2 Exercises From Z.Fh . . . 91
2.7 主理想整环与欧几里得整环 . . . 93
2.7.1 Notes . . . 93
2.7.2 Exercises From Z.Fh . . . 95
2.7.3 PID 不一定是 ED 的反例 . . . 96
2.7.4 素元、不可约元、素理想、极大理想 . . . 98
2.8 环上的多项式 . . . 100
2.8.1 Notes . . . 100

2.9 整环上的多项式 . . . 105
2.10 2021 伯苓班抽象代数 I 期末考试 . . . 106

第三章 模论 **109**
3.1 模的基本概念 . . . 109
3.1.1 Notes . . . 109
3.1.2 Some Meaningful Exercises . . . 112
3.2 自由模与环上的线性代数 . . . 113
3.2.1 Notes . . . 113
3.2.2 Some Meaningful Exercises . . . 116
3.3 PID 上的有限生成模 . . . 117
3.3.1 Notes . . . 117
3.3.2 Some Meaningful Exercises . . . 121
3.4 模的张量积 . . . 122
3.4.1 Notes . . . 122
3.4.2 Some Meaningful Exercises . . . 122
3.5 正合序列——射影模、内射模与平坦模 . . . 123
3.5.1 Notes . . . 123
3.5.2 Some Meaningful Exercises . . . 123

第四章 域论 **125**
4.1 域的基本概念 . . . 125
4.1.1 Notes . . . 125
4.1.2 Some Meaningful Exercises . . . 127
4.2 代数扩张 . . . 129
4.2.1 Notes . . . 129
4.2.2 Some Meaningful Exercises . . . 132
4.3 分裂域 . . . 134
4.3.1 Notes . . . 134
4.3.2 Some Meaningful Exercises . . . 137
4.4 域的正规扩张与可分扩张 . . . 139
4.4.1 Notes . . . 139
4.4.2 Some Meaningful Exercises . . . 144

第五章 Galois 理论 **147**
5.1 域的代数闭包 . . . 147

5.1.1 Notes . . . 147
5.1.2 Some Meaningful Exercises . . . 147
5.2 Galois 群 . . . 148
5.2.1 Notes . . . 148
5.2.2 Some Meaningful Exercises . . . 153
5.3 Galois 扩张与 Galois 对应 . . . 154
5.3.1 Notes . . . 154
5.3.2 Some Meaningful Exercises . . . 156
5.4 多项式的 Galois 群 . . . 157
5.4.1 Notes . . . 157
5.5 有限域 . . . 158
5.5.1 Notes . . . 158
5.6 本原元 . . . 160
5.6.1 Notes . . . 160
5.7 根式扩张 . . . 161
5.7.1 Notes . . . 161
5.8 可解群与根式可解 . . . 166
5.8.1 Notes . . . 166
5.9 Galois 覆盖 . . . 168

第六章 抽象代数结论拾遗 169
6.1 群论 . . . 169

第七章 高等代数难点回顾 171
7.1 一道选拔考试题的探讨 . . . 171

1 群论

1.1 半群与群

1.1.1 Notes

定义 1.1.1: 半群，幺半群，交换幺半群

若非空集合 S 上定义了一个满足结合律的二元运算 $*$，则称 $\{S,*\}$ 为一个**半群**，若半群 S 中存在一个元素 e，使得对任意 $a\in S$ 有

$$ea=a\quad (或ae=a)$$

则称 e 为 S 的一个**左 (右) 幺元**. 若 e 既是左幺元，又是右幺元，则称 e 为 S 的**幺元**，含幺元的半群称为**幺半群**.

命题 1.1.1: 思考题

(1) 存在半群 S，S 中有左幺元，但没有右幺元.

(2) 若一个半群 S 中既有左幺元，又有右幺元，S 是否一定为幺半群?

解 (1) 考虑 $S=\left\{\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\middle|a,b\in\mathbb{R}\right\}$ 关于矩阵乘法构成的半群，则易见其有无穷多左幺元 $\begin{pmatrix}1 & c\\ 0 & 0\end{pmatrix}$，其中 $c\in\mathbb{R}$，而容易验证其没有右幺元.

(2) 设 S 有左幺元 e_1，右幺元 e_2，则有 $e_1=e_1\cdot e_2=e_2$，从而左右幺元均相等，故有唯一元素为左幺元与右幺元，从而为幺半群. ♠

定义 1.1.2: 逆元

设 S 是幺半群，e 是幺元，$a\in S$，若存在 $b\in S$，使得 $ba=e(ab=e)$，则称 b 为 a 的**左逆元 (右逆元)**. 若 $ba=ab=e$，则称 b 为 a 的**逆元**.

命题 1.1.2: 思考题

(1) 存在幺半群 S 及 $a\in S$，a 存在左逆元，但不存在右逆元.

(2) 若幺半群 S 中元素 a 既有左逆元，又有右逆元，则 a 一定是可逆元.

解 (1) 习题 1.1-3.

(2) 设 $ba = ac = e$，则 $b = be = bac = c$，从而 $ba = ab = e$，则 a 可逆. ♠

定义 1.1.3: 群、Abel 群、有限群、无限群

幺半群 G 中的每个元都是可逆元，则 G 为一个**群**，若 G 上的运算还满足交换律，则称 G 为 **Abel 群**. 群 G 中的元素称为 G 的**阶**，记为 $|G|$. 若 $|G| = \infty$，则称 G 为**无限群**，若 $|G| < \infty$，则称 G 为**有限群**.

事实上为了证明一个结构为群，我们并不总需要沿着证封闭性、证结合律 (从而为半群)、找到幺元 (从而为幺半群)、找到每个元素的逆元 (从而为群) 这样一个繁琐的步骤 (虽然对于大部分新奇的结构这样的推理都是必要的)，我们有如下简化的定理来验证：

定理 1.1.1: 半群成为群的一个充要条件

设 G 是一个**半群**，则 G 是一个群当且仅当同时满足以下两个条件

(1)G 中存在左幺元，即存在 $e \in G$，使得任意 $a \in G$，有 $ea = a$；

(2)G 中任意元素都存在左逆元，即对任意 $a \in G$，存在 $b \in G$ 使得 $ba = e$.

证明 必要性是 trivial 的，下证充分性，设 $ba = e = cb$，即考虑 a, b 的左幺元，从而有 $ce = cba = ea = a$，则 $e = bce = ab$，从而 $ab = ba = e$，则有 $ae = ea = a$，从而半群 G 为幺半群，进而又每个元素均为可逆元，从而 G 为群，即证. ♣

Remark. 注意这里的左逆元是“广义的”左逆元，因为左逆元是定义在幺半群上的，但这里 e 仅为左幺元，所以需要特别 care 一下.

命题 1.1.3: 思考题

(1) 若上述定理全部改为右幺元与右逆元，则定理依然成立.

(2) 若改为一左一右，则命题不再成立.

解 (1) 证明完全类似.

(2) 考虑一个二元集合 $\{a, b\}$，定义运算 $a * a = a, a * b = b, b * a = a, b * b = b$，从而存在左幺元 a，b 有右逆元 a，a 有右逆元 a，但显然不存在右幺元，从而不构成群，即为一个反例. ♠

定理 1.1.2: 利用消去律证明半群是群

设 G 是一个半群，则 G 是群当且仅当对任意 $a, b \in G$ 方程 $ax = b$ 及 $yb = a$ 有解.

证明 必要性证明也是 trivial 的，下证充分性，为了证明 G 是群，只需证明存在左幺元，且任意元均存在左逆元.

设 $a \in G$，则存在 e 使得 $ea = a$，从而下希望成立 $eb = b$，而注意到 $ay = b$ 有解，从而 $eb = eay = ay = b$，即证，故存在 e 为左幺元. 从而又 $ba = e$ 恒有解，从而存在左逆元，故由定

理 1.1.1 可知即证. ♣

命题 1.1.4: 上面定理的一个直接应用

有限半群 G 若满足左、右消去律，则 G 是群.

证明 设 $G=\{a_1,\cdots,a_n\}$，从而考虑任一方程 $a_ix=a_j$，考虑左陪集 a_iG，从而由左消去律可知 $a_ix=a_iy$ 则 $x=y$，从而 $a_iG=G$，则存在 x 使得 $a_ix=a_j$，同理 $ya_i=a_j$ 也恒有解，故由定理 1.1.2 即证. ♣

Remark. 注意上述命题对无限半群并不成立，因为很容易举出反例 $\{\mathbb{N}_+,+\}$.

定理 1.1.3: 从幺半群出发生成群

设 S 是幺半群，记 $U(S)$ 为 S 中可逆元的全体，则 $U(S)$ 构成群.

证明 我们仅证明关于运算的封闭性，注意到任意 $a,b\in U(S)$，则 $a^{-1},b^{-1}\in U(S)$，从而 $(ab)(b^{-1}a^{-1})=(b^{-1}a^{-1})=ab=e$，则 $ab\in U(S)$，从而封闭性验证，显然构成群. ♣

Remark. 注意定理的关键在于证明左幺元与左逆元的存在是 trivial 的，但是更关键的是，$U(S)$ 是半群么？封闭性是需要验证的!

1.1.2 Exercises From Z.Fh

1.解 (1) 是二元运算，但 $a-(b-c)\neq(a-b)-c$，从而不满足结合律，不是半群；

(2) 是二元运算，又 $(a*b)*c=(a+b-ab)*c=a+b-ab+c-ac-bc+abc=a*(b*c)$，从而满足结合律，故构成半群，而显然 $a*0=0*a=a$，从而存在幺元 0，故为幺半群，而若考虑 3，则若其有逆元 x 则 $3+x-3x=0$，则 $x\notin\mathbb{Z}$，从而不构成群；

(3) 显然 $2*\dfrac{1}{2}=2\cdot\dfrac{1}{2}=1\notin G$，从而定义的 $*$ 不为二元运算，则后面的自然都不满足；

(4) 熟知本原多项式的乘积仍为本原多项式，从而为二元运算，显然满足结合律，从而构成半群，而又有幺元 1，从而为幺半群，显然不为群 (多项式度易得到矛盾)；

(5) 显然为半群，有幺元 1，从而为幺半群，显然没有逆元，从而不为群；

(6) 是二元运算，且由 $(a*b)*c=(a^b)*c=a^{bc}=a*(b*c)$，从而为半群，而由 $a*1=a$，但 $1*a=1\neq a$，从而不为幺半群. ♠

Remark. 验证二元运算即验证封闭性.

2.证明 注意到幺元为 $\left(1,\dfrac{1}{2}\right)$，且封闭性，结合性与交换性证明是显然的，略去. ♣

3.证明 考虑 $g_k\in M(\mathbb{N})$，且 $g_k(n)=\begin{cases}n-1, & n\geq 1\\ k, & n=0\end{cases}$，从而对任意 $k\in\mathbb{N}$ 有 $g_k\circ f(n)=n$，从而 g_k 为左逆元，故有无穷多左逆元，但是若存在右逆元 h，则可知 $f(h(0))=0$，也即 $h(0)+1=0$，则 $h(0)=-1\notin\mathbb{N}$，矛盾，从而不存在右逆元. ♣

Remark. 这就是课本思考题中的一个例子.

4.证明 设 $\cdot$，$*$ 的幺元分别为 e_1, e_2，从而我们由 $(e_1 * e_2)\cdot(e_2 * e_1) = (e_1 \cdot e_2) * (e_2 \cdot e_1)$，这表明 $e_1 = e_1 \cdot e_1 = e_2 * e_2 = e_2$，从而运算的幺元为同一个，记为 e，从而有 $(a*e)\cdot(e*d) = (a\cdot e)*(e\cdot d)$，即 $a \cdot d = a * d$，从而由 a, d 的任意性可知两种运算为同一个.

设运算为 $*$，又由 $(e*a)*(b*e) = (e*b)*(a*e)$，从而 $a*b = b*a$，故运算满足交换律，又对任意 a, b, c，则 $(a*b)*c = (a*b)*(e*c) = (a*e)*(b*c) = a*(b*c)$，从而满足结合律，综上即证. ♣

5.解 设 $G = \{a, b\}$，则枚举 16 种情况 (不知道有没有聪明点的方法)，可知幺半群有 (以群表的形式展现)，

$$\begin{pmatrix} & a & b \\ a & b & a \\ b & a & b \end{pmatrix}, \begin{pmatrix} & a & b \\ a & a & b \\ b & b & b \end{pmatrix}, \begin{pmatrix} & a & b \\ a & b & a \\ b & a & a \end{pmatrix}.$$

其中第一个亦为群，第二、三个均不为群. ♠

6.证明 设有限半群 $S = \{a_1, \cdots, a_n\}$，设 e_1, e_2 均为左幺元，则 $e_1 a = a = e_2 a$，由右消去律可知 $e_1 = e_2$，从而左幺元唯一. 又对任意 $a_j \in S$，从而考虑 Sa_j，则由右消去律可知 $Sa_j = G$，从而存在 $a_i \in S$ 使得 $a_i a_j = e$，故由左逆元，从而可知 S 为群. ♣

7.解 考虑二元群表 $\begin{pmatrix} & a & b \\ a & a & a \\ b & b & b \end{pmatrix}$，则容易看见这是一个例子. ♠

8.解 考虑自然数上的加法结构 $\{\mathbb{N}, +\}$，即可知是一个例子. ♠

9.证明 易见 $A\Delta B \subseteq A \bigcup B \subseteq X$，从而满足封闭性，不难证明结合律，且考虑 $\varnothing$，则 $A\Delta\varnothing = \varnothing\Delta A = A$，从而 $\varnothing$ 为幺元，且 $A\Delta A = \varnothing$，故 A 自己作为自己的逆元，从而可知 $(P(X), \Delta)$ 构成一个群.

设 $X = \{0, 1\}$，则 $P(X) = \{\varnothing, \{0\}, \{1\}, \{0, 1\}\}$，从而群表为

$$\begin{pmatrix} & \varnothing & \{0\} & \{1\} & \{0,1\} \\ \varnothing & \varnothing & \{0\} & \{1\} & \{0,1\} \\ \{0\} & \{0\} & \varnothing & \{0,1\} & \{1\} \\ \{1\} & \{1\} & \{0,1\} & \varnothing & \{0\} \\ \{0,1\} & \{0,1\} & \{1\} & \{0\} & \varnothing \end{pmatrix}.$$

综上我们完成了题目. ♣

10.证明 设 $w_k = \mathrm{e}^{\frac{2k\pi\sqrt{-1}}{n}}$，从而可知 w_n 为幺元，w_{n-k} 与 w_k 互为逆元，从而构成乘法群. ♣

11.解 (1)、(2)、(3) 显然，下考虑 (4)，注意到 $\mathbb{Z}_p^*$ 关于乘法为群，从而考虑任一元素的逆元，若为幂幺元，则 $x^2 \equiv 1 (\mathrm{mod}\ p)$，从而 $x = \overline{1}$ 或 $\overline{p-1}$，而其余元素均可两两配对互为逆元，从而

我们有

$$(p-1)!\equiv(p-1)\cdot\prod_{a\in\mathbb{Z}_p^*,\ a\neq p-1\text{或}1}\left(a\cdot a^{-1}\right)\equiv -1(\mathrm{mod}\ p).$$

综上即证 (4) 的 Wilson 定理. ♠

12.证明 对模 n 的缩系，由 11 可知其关于乘法构成群，从而考虑 $\langle a\rangle<\mathbb{Z}_n^*$，从而由 Lagrange 定理，有 a 的阶 $d=|\langle a\rangle|\big|\varphi(n)$，从而 $a^d=\overline{1}$，进而 $a^{\varphi(n)}=\overline{1}$，即 $a^{\varphi(n)}\equiv 1(\mathrm{mod}\ n)$，即证 Euler 定理. 从而注意到 $\varphi(p)=p-1$，即证 Fermat 小定理. ♣

13.解 证明是群是 trivial 的，这里仅证明封闭性和逆元，注意到对 $A,B\in\mathrm{SL}(n,\mathbb{Z}_n)$，则有 $\det A\equiv\det B\equiv 1(\mathrm{mod}\ n)$，从而 $\det(AB)=\det A\cdot\det B\equiv 1(\mathrm{mod\ n})$，即证封闭性.

而对于任意 $A=A=\begin{pmatrix}\bar{a} & \bar{b}\\ \bar{c} & \bar{d}\end{pmatrix}$，其逆为 $A=\begin{pmatrix}\bar{d} & -\bar{b}\\ -\bar{c} & \bar{a}\end{pmatrix}$，对于一般的 $m\in\mathbb{N}^*$，我们定义 $\mathrm{SL}(m,\mathbb{Z}_n)=\{A\in M_m(\mathbb{Z}_n)|\det A\equiv 1(\mathrm{mod}\ n)\}$. ♠

14.证明 我们不难注意到以下两个事实

$$aa'=a'(aaa')=(a'aa)a'=a'a,\quad bb'=a'(abb')=(a'ab)b'=a'a,$$

从而我们可知对任意 $a,b\in G$，有 $aa'=a'a=bb'=b'b$，不妨记其为 e，从而可知 e 为半群 G 的幺元，且 a' 为 a 的逆元，从而综上我们可知 G 为群. ♣

15.证明 结合律与封闭性不难验证，我们又注意到有左幺元 $(1,0)$，且任意 $(c,d)\in G$，由 $c\neq 0$ 可知有左逆元 $\left(\frac{1}{c},-\frac{d}{c}\right)$，从而可知 G 为群. ♣

16.解 (1) 对于 $T_{(A,\beta)}$ 有逆映射 $T_{(A^{-1},-A^{-1}\beta)}$，从而不难看见是双射；

(2) 封闭性与结合律不难验证，幺元即 $T_{(\boldsymbol{I}_n,0)}$，且逆元即为 (1) 中结构. ♠

17.证明 例子不妨就考虑所有矩阵 $\mathrm{diag}\{a,0,\cdots,0\}(a\in\mathbb{R}\setminus\{0\})$，不难看到其构成群.

对于这样的群 G，设其幺元为 I_G，从而设其秩为 k，则考虑 $\mathrm{Im}(I_G)$ 的一组基，将其扩充为一组标准正交基，组成方阵 T，从而可知 $T^{-1}I_GT=\begin{pmatrix}E_k & O\\ O & O\end{pmatrix}$，其中 E_k 非奇异，则由任意 $A\in G$，$I_GA=AI_G=A$，则考虑 $\widetilde{A}=T^{-1}AT=\begin{pmatrix}A_1 & A_2\\ A_3 & A_4\end{pmatrix}$，从而有

$$\begin{pmatrix}A_1E_k & O\\ A_3E_k & O\end{pmatrix}=\begin{pmatrix}A_1 & A_2\\ A_3 & A_4\end{pmatrix}\begin{pmatrix}E_k & O\\ O & O\end{pmatrix}=\begin{pmatrix}E_k & O\\ O & O\end{pmatrix}\begin{pmatrix}A_1 & A_2\\ A_3 & A_4\end{pmatrix}=\begin{pmatrix}E_kA_1 & E_kA_2\\ O & O\end{pmatrix},$$

进而可知 $A_2=A_3=A_4=O$，且 $A_1E_k=E_kA_1=A_1$，又 $A\in G$ 有逆元 B，从而 $A_1B_1=B_1A_1=E_k$，则由 E_k 满秩可知 A_1,B_1 均满秩，即可逆，综上即证. ♣

18.证明 (1) 封闭性与结合律显然，幺元即恒等变换 id，而由正交变换为保距变换，进而为双射，从而若 $\sigma\in G_F$，则 σ^{-1} 存在也显然保持 F 不变，从而构成群.

(2) 我们考虑正 n 边形的对称性，其绕中心旋转 $\frac{k\pi}{n}(1\leq k\leq n)$ 仍然于原来重合，另外易见正 n 边形有且仅有 n 条对称轴，从而可知对称群中的变换仅有 $2n$ 种，即阶为 $2n$.

(3) 正多面体对称群的阶为面数乘以每个面的顶点数，又正多面体仅有 5 种，从而**不难**知道(当然很难)，正四面体对称群的阶为 12，正六面体对称群的阶为 24，正八面体对称群的阶为 24，正十二面体对称群的阶为 60，正二十面体对称群的阶为 60. ♣

Remark. 证明材料可见知乎回答，用到了轨道的知识，当然 zfh 的本意肯定是让咱们单纯的读者慢慢数对称轴对吧 (X)

19.解 表述的令人迷惑....，没太理解，解释可看知乎，大概是群表示论的内容? ♠

20.证明 (1) 交换性是显然的，我们先证明结合律，对任意数论函数 f,g,h，从而对任意 $n\in\mathbb{N}^*$，

$$(f*g)*h(n)=\sum_{d|n}h(d)(f*g)\left(\frac{n}{d}\right)=\sum_{d|n}h(d)\sum_{e|\frac{n}{d}}f(e)g\left(\frac{n}{ed}\right)=\sum_{abc=n}f(a)g(b)h(c),$$

则不难得到 $f*(g*h)(n)=\sum\limits_{abc=n}f(a)g(b)h(c)=(f*g)*h(n)$，可知结合律成立.

而考虑幺元 $e(n)=\begin{cases}1, & n=1\\ 0 & n\geq 2\end{cases}$，从而可知 $(S,*)$ 为交换幺半群.

(2) 若 f 可逆，从而存在 $g\in S$，使得 $f*g=e$，从而 $f(1)g(1)=e(1)=1$，则 $f(1)\neq 0$；若 $f(1)\neq 0$，下面归纳构造 g 使得其为 f 的逆，注意到 $f(1)g(1)=1$，从而取 $g(1)=\dfrac{1}{f(1)}$，则由 $f(1)g(2)+f(2)g(1)=0$，从而 $g(2)=-\dfrac{f(2)g(1)}{f(1)}$，假设 $k\leq n$ 均定义 $g(k)$，则由

$$g(n+1)f(1)+\sum_{d|n+1,d>1}g\left(\frac{n+1}{d}\right)f(d)=0,$$

从而由 $\dfrac{n+1}{d}\leq n$，从而有归纳假设可知为确定值，从而 $g(n+1)$ 可被确定，故归纳可构造出 g 使得为 f 的逆.

(3) 交换性显然，又注意到 $f(1)=f^2(1)$，且若 $f(1)=0$，则由 f 积性，则 $f(m)\equiv 0$，从而可知 $f(1)=1\neq 0$，则积性函数 f 均可逆，因此下只需证明封闭性.

对任意 $m,n\in\mathbb{N}^*$，设 $m=p_1^{a_1}\cdots p_t^{a_t}$，$n=q_1^{b_1}\cdots q_s^{b_s}$，其中 p_i,q_j 互不相等，从而有

$$\begin{aligned}
f*g(mn)&=\sum_{x_1=0}^{a_1}\cdots\sum_{x_t=0}^{a_t}\sum_{y_1=0}^{b_1}\cdots\sum_{y_s=0}^{b_t}f\left(\prod_{i=1}^{t}p_i^{x_i}\cdot\prod_{j=1}^{s}q_j^{y_j}\right)g\left(\prod_{i=1}^{t}p_i^{a_i-x_i}\cdot\prod_{j=1}^{s}q_j^{b_j-y_j}\right)\\
&=\sum_{x_1=0}^{a_1}\cdots\sum_{x_t=0}^{a_t}\sum_{y_1=0}^{b_1}\cdots\sum_{y_s=0}^{b_t}f\left(\prod_{i=1}^{t}p_i^{x_i}\right)\cdot f\left(\prod_{j=1}^{s}q_j^{y_j}\right)g\left(\prod_{i=1}^{t}p_i^{a_i-x_i}\right)\cdot g\left(\prod_{j=1}^{s}q_j^{b_j-y_j}\right)\\
&=\left[\sum_{x_1=0}^{a_1}\cdots\sum_{x_t=0}^{a_t}f\left(\prod_{i=1}^{t}p_i^{x_i}\right)g\left(\prod_{i=1}^{t}p_i^{a_i-x_i}\right)\right]\cdot\left[\sum_{y_1=0}^{b_1}\cdots\sum_{y_s=0}^{b_t}f\left(\prod_{j=1}^{s}q_j^{y_j}\right)g\left(\prod_{j=1}^{s}q_j^{b_j-y_j}\right)\right]\\
&=f*g(m)\cdot f*g(n)
\end{aligned}$$

故可知 $f*g$ 也为积性函数，综上可知 $(S,*)$ 构成 Abel 群.

(4) 注意到对素数 p，$f*g(p^3)=ax^3+bx^2+b^2x+b^3y$，其中 $a=f(1),b=f(p),x=g(p),y=g(1)$，而 $f*g(p)=ax+by$，则 $(ax+by)^3\neq ax^3+bx^2+b^2x+b^3y$，从而可知 $f*g$ 不为完全积性函数，从而不满足封闭性，故不为 Abel 群. ♣

21.证明 (1) 注意到对 $(m,n)=1$，若 m,n 中有一个平方因子，则 $\mu(mn)=0=\mu(m)\mu(n)$，若 $m=p_1\cdots p_t$，$n=q_1\cdots q_s$，从而 $\mu(mn)=(-1)^{s+t}=\mu(m)\mu(n)$，从而 $\mu(n)$ 为积性函数.

设 $\psi(n)=\sum\limits_{m\leq n,(m,n)=1} w_n^m$，其中 w_n 为 n 次单位根，我们往证 $\psi(n)=\mu(n)$，分三步证明：

Step 1. 证明 $\psi(1)=1,\psi(p)=-1$，其中 p 为素数.

其中 $\psi(1)=1$ 是显然的，而又有 $\psi(p)=\sum\limits_{m\leq p,(m,p)=1} w_p^m=\sum\limits_{m=1}^{p-1} w_p^m=-1$，成立.

Step 2. 证明 $\psi(p^t)=0$，对任意 $t\geq 2$.

我们注意到

$$\psi(p^t)=\sum_{m=1}^{p^t} w_{p^t}^m-\sum_{m\leq p^t,(m,p^t)>1} w_{p^t}^m=-\sum_{m\leq p^t,(m,p^t)>1} w_{p^t}^m=-\sum_{m=1}^{p^{t-1}} w_{p^{t-1}}^m=0.$$

Step 3. 证明 $\psi(n)$ 是积性函数.

对任意 $(m,n)=1$，我们有

$$\psi(m)\psi(n)=\left(\sum_{t\leq m,(t,m)=1} w_m^t\right)\left(\sum_{s\leq n,(t,n)=1} w_n^s\right)=\sum_{\substack{t\leq m,(t,m)=1\\ s\leq n,(t,n)=1}} w_m^t w_n^s,$$

而 $w_m^t w_n^s=\exp\left(\dfrac{2(ms+nt)\pi\sqrt{-1}}{mn}\right)$，又注意到任意 $(s_1,t_1)\neq(s_2,t_2)$，则若 $ms_1+nt_1\equiv ms_2+nt_2(\mathrm{mod}\ n)$，则有 $m|n(t_1-t_2)$，而 $(m,n)=1$，从而 $m|t_1-t_2$，而 $|t_1-t_2|<m$，从而 $t_1=t_2$，同理 $m_1=m_2$，矛盾！从而组合 $ms+nt$ 互不模 mn 同余，又由 Euler 函数积性，从而 $\varphi(mn)=\varphi(m)\varphi(n)$，从而 $ms+nt$ 构成模 mn 的缩系，也即

$$\psi(m)\psi(n)=\sum_{\substack{t\leq m,(t,m)=1\\ s\leq n,(t,n)=1}} w_m^t w_n^s=\sum_{l\leq mn,(l,mn)=1} w_{mn}^l=\psi(mn).$$

综上，我们进一步不难得到 $\psi(n)$ 的取值与 $\mu(n)$ 完全一致，从而可知 $\psi(n)=\mu(n)$，即证.

(2) 我们考虑 $\lambda(n)=1(n\in\mathbb{N}^*)$，从而对任意 $m=p_1^{a_1}\cdots p_t^{a_t}$，则对 $n\geq 2$，

$$\mu*\lambda(n)=\sum_{d|n}\mu(d)\lambda\left(\frac{n}{d}\right)=\sum_{d|n}\mu(d)=\sum_{k=0}^{t}(-1)^k\binom{n}{k}=(1-1)^t=0=e(n)$$

又显然 $\mu*\lambda(1)=1=e(1)$，从而 $\mu*\lambda=e$，即 λ 为 μ 的逆元.

(3) 注意到 $f*\lambda(n)=\sum\limits_{d|n} f(d)$，从而可知 $f*\lambda=g$，则由 $\lambda^{-1}=\mu$，从而 $f=g*\mu$，即证任意 $n\in\mathbb{N}^*$，有

$$f(n)=g*\mu(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d).$$

即 Mobius 反演公式. ♣

Remark. 如果不用群论也可以这么去证这个经典结论：注意到

$$\sum_{d|n}\mu(d)g\left(\frac{n}{d}\right)=\sum_{d|n}\mu(d)\left(\sum_{q|\frac{n}{d}}f(q)\right)=\sum_{d|n}\sum_{q|\frac{n}{d}}\mu(d)f(q)=\sum_{q|n}\left(\sum_{d|\frac{n}{q}}\mu(d)\right)f(q)=f(n),$$

其中用到了 $\sum_{d|n}\mu(d)=e(n)$，仅在 $n=1$ 处非 0.

1.2 子群与陪集

1.2.1 Notes

定义 1.2.1: 子群

设 H 是群 G 的一个非空子集. 如果 H 对 G 的运算也构成群，则称 H 为 G 的**子群**，记作 $H < G$. 若 $H \neq G$，则称其为**真子群**.

一般为了判别一个非空子集是否为子群，通常用下面这个定理：

定理 1.2.1: 子群的判别定理

设 H 为群 G 的非空子集，则 $H < G$ 的充要条件为任意 $a, b \in H$，有 $ab^{-1} \in H$.

证明 若 $H < G$，则显然有任意 $a, b \in H$，有 $ab^{-1} \in H$.

而反过来，由 H 非空，从而存在 $a \in H$，则有 $e = aa^{-1} \in H$，则有 $a^{-1} = ea^{-1} \in H$，从而这验证了 H 有幺元和逆元，又注意到对 $a, b \in H$，有 $b^{-1} \in H$，从而 $ab = a(b^{-1})^{-1} \in H$，从而满足封闭性，综上可知 $H < G$. ♣

命题 1.2.1: 思考题

证明：$\mathbb{Z}$ 的任何子群都形如 $m\mathbb{Z}$，$m \in \mathbb{N}$.

证明 设 $H < \mathbb{Z}$，从而有 $m \in H \subseteq \mathbb{Z}$ 且 $m \neq 0$，则不妨设 $m > 0$(否则用 $-m$ 代替). 且不妨设 m 为 H 中绝对值最小的数，从而由归纳法不难证明 $mn \in H$ 对任意 $n \in \mathbb{Z}$，从而 $m\mathbb{Z} \subseteq H$，又若存在 $n \in H$ 且 $m \nmid n$，则考虑 $d = \gcd(m, n)$，则由 Bezout 定理，存在 $a, b \in \mathbb{Z}$，使得 $d = am + bn \in H$，而 $0 < d < m$，这与 m 的最小性矛盾！从而 $H = m\mathbb{Z}$，即证. ♣

定义 1.2.2: 元素的阶

设群 G 以及 $a \in G$，考虑子群 $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$，则考虑该子群的阶，并称其为 a 的**阶**.

下面是一个习题课上关于阶的分解思考题：

命题 1.2.2: 习题课思考题

设群 G 中元素 a 的阶为 mn，且 $(m, n) = 1$，证明：存在唯一的 m 阶元 b 与 n 阶元 c 使得有分解 $a = bc = cb$.

Remark. 只需考虑选取 b, c 为 a^k 即可，核心的论证需要 Bezout 定理.

定义 1.2.3: 生成子群、有限生成群

设 S 是群 G 中的一个非空子集，令 $S^{-1}=\{a^{-1}|a\in S\}$，记

$$\langle S\rangle=\{x_1\cdots x_m|m\in\mathbb{N},x_1,\cdots,x_m\in S\cup S^{-1}\},$$

不难看到 $\langle S\rangle$ 为子群，称为 S **生成的子群**. 若存在 S 使得 $\langle S\rangle=G$，则称 S 为 G 的一个**生成组**，如果 G 有一个生成组，则称 G 为**有限生成群**.

命题 1.2.3: 生成子群的等价刻画

证明群 G 中非空子集 S 生成的子群 $\langle S\rangle$ 是 G 中所有包含 S 的子群的交，也是 G 中包含 S 的最小子群.

证明 注意到若 $S\subseteq H<G$, 则 $S\cup S^{-1}\subseteq H$, 从而由封闭性可知 $\langle S\rangle\subseteq H$, 即有 $\langle S\rangle\subseteq\bigcap\limits_{S\subseteq H<G}H$, 而另一方面，显然 $\langle S\rangle<G$，从而 $\bigcap\limits_{S\subseteq H<G}H\subseteq\langle S\rangle$，从而两者相等，即证. ♣

定义 1.2.4: 陪集

设 $H<G$，对 $a\in G$，则

$$aH=\{ah|h\in H\},\quad Ha=\{ha|h\in H\}$$

分别称为以 a 为**代表元**的**左陪集**和**右陪集**，统称为**陪集**.

引理 1.2.1 (陪集间的关系)**.** *设 $H<G$，$a,b\in G$，则 $aH\cap bH=\varnothing$ 或 $aH=bH$，且 $aH=bH$ 当且仅当 $a^{-1}b\in H$.*

证明 若 $b\in aH$，则存在 $h\in H$ 使得 $b=ah$，则有 $a=bh^{-1}\in bH$，从而 $aH=bH$，即证. ♣

定理 1.2.2: 陪集确定的等价关系

设 $H<G$，则由

$$a\mathrm{R}b\Longleftrightarrow a^{-1}b\in H$$

所确定的 G 中的关系 R 为等价关系，且 a 所在的等价类 $\bar{a}$ 恰为以 a 为代表元的 H 的左陪集 aH.

利用这个等价关系得到的商集合称为 G 对 H 的**左陪集空间**，记为 G/H，$|G/H|$ 称为 H 在 G 中的指数，也记为 $[G:H]$.

对于有限群，我们不难发现等价关系对 G 进行了一个划分，从而我们可以立刻得到 Lagrange 定理：若 $H<G$，则有 H 的阶为 G 的阶的因子，即 $|G|=[G:H]\cdot|H|$.

命题 1.2.4: 思考题

对群的阶的任何因子 m，是否都存在子群使得其阶恰为 m?

证明 考虑正六边形的二面体群 D_{12}，可知其元素阶为 2 或 6，从而不难证明其无 4 阶子群. ♣

1.2.2 Exercises From Z.Fh

1.证明 直接挨个验证？我想找一个大群包含 K_4，从而证明是子群，但并没找到. ♣

2.证明 设 $H_\lambda < G(\lambda \in \Lambda)$, 其中 Λ 为指标集, 则易见对 $a, b \in \bigcap\limits_{\lambda\in\Lambda}$, 有 $ab^{-1} \in H_\lambda$, 从而 $ab^{-1} \in \bigcap\limits_{\lambda\in\Lambda}$, 即证为子群. ♣

3.证明 设 $H_1 < G$，$H_2 < G$，且 $H_1 \neq G$，$H_2 \neq G$，反证法若 $H_1 \cup H_2 = G$，则显然 H_1 与 H_2 之间无包含关系，从而存在 $a \in H_1 \setminus H_2$，$b \in H_2 \setminus H_1$，从而若 $ab \in H_1$，则 $b \in H_1$，矛盾！同理 $ab \in H_2$ 矛盾，故 $ab \in G$，但 $ab \notin H_1 \cup H_2$，这即表明 $H_1 \cup H_2 \neq G$，即证. ♣

4.证明 若 H 为有限集合，从而考虑任意 $a, b \in G$，则由消去律与封闭性可知 $aH = H$，故存在 $x \in H$ 使得 $ax = b$，同理存在 $y \in H$ 使得 $ya = b$，从而可知 H 为群，即 $H < G$，另一方面的证明是 trivial 的.

若 H 是由 G 中有限阶元组成的集合，如考虑 $G = \mathrm{GL}(2, \mathbb{R})$，$H = \left\{ \begin{pmatrix} 1 & 0 \\ a & -1 \end{pmatrix} \middle| a \in \mathbb{R} \right\}$，易见每个元素均为二阶元，但不满足封闭性，因为 $\begin{pmatrix} 1 & 0 \\ a & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a-b & 1 \end{pmatrix}$，从而不构成子群. ♣

5.证明 注意到 $a, b \in G$，由 $a^2 = b^2 = e$，从而 $a^{-1} = a, b^{-1} = b$，则 $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$，从而为 Abel 群. ♣

7.证明 a 与 a^{-1} 同阶显然，$a^n = e \Leftrightarrow \left(bab^{-1}\right)^n = ba^nb^{-1} = e$，从而两者同阶，设 ab 的阶为 n，即 $e = (ab)^n = a(ba)^{n-1}b$，则 $(ba)^{n-1} = a^{-1}b^{-1}$，从而 $(ba)^n = (ba)(ba)^{n-1} = baa^{-1}b^{-1} = e$，也即 $(ab)^n = e \Leftrightarrow (ba)^n = e$，这即表明两者同阶. ♣

8.证明 (1) 一方面 $(ab)^{mn} = a^{mn}b^{mn} = e$，从而 ab 的阶 $d | mn$，又由 $(ab)^m = b^m$，且 $(m, n) = 1$，则可知 b^m 的阶为 n，从而故 $(ab)^m = b^m$ 阶为 n，从而有 $n = \dfrac{d}{(d, m)}$，从而 $n | d$，同理 $m | d$，则由 $(m, n) = 1$ 可知 $mn | d$，进而 $d = mn$.

(2) 显然有 ab 的阶 $d | [m, n]$，而 $a^db^d = (ab)^d = e$，从而 $a^d = b^{n-d}$，则 $a^d = b^{n-d} = e$，则 $m | d$，同理 $n | d$，从而 $[m, n] | d$，即证 $d = [m, n]$.

(3) 设 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$，$n = p_1^{\beta_1} \cdots p_k^{\beta_k}$，从而考虑 $m_1 = \prod\limits_{\alpha_i \geq \beta_i} p_i^{\alpha_i} \mid m$，$n_1 = \prod\limits_{\alpha_i < \beta_i} p_i^{\beta_i} \mid n$，从而存在 m_1, n_1 阶元，则由 $(m_1, n_1) = 1$ 且 $m_1 n_1 = [m, n]$，从而存在 $[m, n]$ 阶元，即证. ♣

9.证明 设 a^k 的阶为 l，则一方面 $d | kl$，从而 $\dfrac{d}{(d, k)} \Big| kl$，也即 $\dfrac{d}{(d, k)} \Big| l$，又不难证明 $(a^k)^{\frac{d}{(d,k)}} = e$，

从而可知阶为 $\dfrac{d}{(d,k)}$. ♣

10.证明 若存在 $b\in G$ 且其阶为 $l<n$，且 $l\nmid n$，则设 $d=(n,l)$，则 $c=b^d$ 阶为 $\dfrac{l}{d}$，又设 $a^n=e$ 即其阶为 n，则有 ab 的阶为 $[l,n]>n$，这与最大阶矛盾! ♣

11.证明 显然若 $a^n=e,b^n=e$，则 $(b^{-1})^n=e$，从而 $(ab^{-1})^n=a^n(b^{-1})^n=e$，即证. ♣

12.证明 由阶为 k 的元有 $a^k=e$，且 $(a^{-1})^k=e$，且 $a\neq a^{-1}$，否则 $a^2=e$，矛盾，故可知阶为 k 的元可以与其逆配对，从而个数一定是偶数，即证. ♣

13.证明 (1) 显然 $A\in \mathrm{SL}(n,\mathbb{Z})$，则 $A^{-1}=A^*$，即每个元素均为整数，进而 $AB^{-1}\in \mathrm{SL}(n,\mathbb{Z})$，从而为子群;

(2) 我们只需证明 $\mathrm{SL}(2,\mathbb{Z})=\langle T,U\rangle$(另外两个可以由 T,U 生成，反过来也可以生成 T,U)，而对任意 $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in \mathrm{SL}(2,\mathbb{Z})$，由 $ad-bc=1$，从而 $(a,c)=1$，故对 a,c 作辗转相除法，从而对其左乘若干 T,U,T^{-1},U^{-1}，则可以使得变为 $\begin{pmatrix}1&b'\\c'&d'\end{pmatrix}$ 或 $\begin{pmatrix}a'&b'\\1&d'\end{pmatrix}$，进一步可化为 $\begin{pmatrix}1&b''\\0&1\end{pmatrix}$ 或 $\begin{pmatrix}0&-1'\\1&d''\end{pmatrix}$，其中利用行列式为 1 确定了另外一个元素，从而进一步可初等行变换为 $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ 或 $\begin{pmatrix}0&-1\\1&0\end{pmatrix}=S$，又不难发现 $TST=U$，从而 S 也可以被生成，综上任一 $\mathrm{SL}(2,\mathbb{Z})$ 均可由 T,U 生成，进而可被任意两个生成. ♣

Remark. 这是 2011 Yau Contest Algebra and Number Theory 题目.

14.解 (1) 由 $3\mathrm{R}0$，$0\mathrm{R}-3$，但 $3\not R-3$，不满足传递性，不为等价关系;

(2) 容易看见这为等价关系;

(3) 不满足反身性 $x-x=0$ 不为偶数，从而不为等价关系;

(4) 注意到 $O=OI_nO$，从而 $O\mathrm{R}I_n$，但显然 $I_n\not RO$，否则 $I_n=POQ=O$，从而不满足对称性，故不为等价关系. ♠

15.解 (1) 仅不满足反身性的例子：对 $\mathbb{R}$ 上的元素，定义 $a\mathrm{R}b\Leftrightarrow ab>0$，则易见 $0\not R0$;

(2) 仅不满足传递性的例子：14.(1)； (3) 仅不满足对称性的例子：14.(4). ♠

16.证明 (1) 我们注意到对任意 $hk=h_1k_1$，从而 $h^{-1}h_1=kk_1^{-1}$，从而有 $h^{-1}h_1=kk_1^{-1}=q\in H\cap K$，从而 $h_1=hq$，$k_1=q^{-1}k$，从而对 $|H||K|$ 中的所有元素中，可根据是否相等划为若干等价类，且每个等价类中均有 $|H\cap K|$ 个元素，即有 $|HK|=|H||K|/|H\cap K|$.

(2) 若 $HK<G$，则任意 $hk\in HK$，有 $k^{-1}h^{-1}=h_1k_1\in HK$，从而 $hk=k_1^{-1}h_1^{-1}\in KH$，从而 $HK=KH$.

若 $HK=KH$，则任意 $h_1,h_2\in H$，$k_1,k_2\in K$，从而 $(h_1k_1)(k_2^{-1}h_2^{-1})=h_1h_3k_3\in HK$，其中 $k_1k_2^{-1}h_2^{-1}=h_3k_3$，从而 $HK<G$. ♣

17.证明 由 $H_1 \subseteq H_2$，则易有 $H_1 < H_2 < G$，从而由 Lagrange 定理

$$[G:H_2][H_2:H_1] = \frac{|G|}{|H_2|} \cdot \frac{|H_2|}{|H_1|} = \frac{|G|}{|H_1|} = [G:H_1],$$

综上即证 $[G:H_2][H_2:H_1] = [G:H_1]$. ♣

18.证明 设 $G = \{a_1, \cdots, a_{2n+1}\}$，从而考虑 $a_1^2, \cdots, a_{2n+1}^2$，若有两者相等，不妨设为 $a_1^2 = a_2^2$，又设 a_1, a_2 的阶为 d, l，则 $d|2n+1, l|2n+1$，从而 d, l 为奇数，则由 $a_1^d = e = a_2^l$，则 $a_1^{dl} = e = a_2^{dl}$，从而考虑 $q = (d_1 d_2 - 1)/2$，则 $a_1 = a_1^{dl}(a_1^{-2})^q = a_2^{dl}(a_2^{-2})^q = a_2$，矛盾，从而可知 G 中任何元均为唯一确定元的平方. ♣

19.证明 若 R 是群 G 对子群 A 的右陪集代表元系，则由 $Ar_1 = Ar_2$，则有 $r_2 r_1^{-1} \in A$，从而 $r_1 r_2^{-1} \in A$，也即 $(r_1^{-1})^{-1}(r_2^{-1}) \in A$，从而 $r_1^{-1}A = r_2^{-1}A$，从而可知 R^{-1} 是群 G 对子群 A 的左陪集代表元系. ♣

20.证明 由 16 题可知 $|H_1H_2| = |H_1||H_2|/|H_1 \cap H_2|$，从而由 $H_1H_2 \subseteq G$，故有 $|H_1||H_2| \leq |G||H_1 \cap H_2|$，由此即有

$$[G:H_1][G:H_2] = \frac{|G|}{|H_1|} \cdot \frac{|G|}{|H_2|} \geq \frac{|G|}{|H_1 \cap H_2|} = [G:H_1 \cap H_2].$$

又由 17 可知，$[G:H_1 \cap H_2] = [G:H_1][G:H_1 \cap H_2]$，从而 $[G:H_1]|[G:H_1 \cap H_2]$，同理 $[G:H_2]|[G:H_1 \cap H_2]$，又有两者互素从而 $[G:H_1][G:H_2]|[G:H_1 \cap H_2]$，进而由 $[G:H_1 \cap H_2] \leq [G:H_1][G:H_2]$ 可知 $G:H_1][G:H_2] = [G:H_1 \cap H_2]$，从而由取等可知 $G = H_1H_2$. ♣

21.证明 若 G 为偶数阶群为 $\{e, a_1, \cdots, a_{2n-1}\}$，则若 G 中无二阶元，则 $a_1, \cdots, a_{2n-1}$ 的阶均为大于 2 的正整数，从而由题目 12 可知，每个阶为 $k > 2$ 的元的个数为偶数，从而非幺元一共有偶数个，不为 $2n-1$，矛盾！从而 G 中一定有 2 阶元.

考虑正三角形的二面体群 $D_6 = \{\mathrm{id}, \tau, \tau^2, \sigma, \sigma\tau, \sigma\tau^2\}$，其中 τ 为顺时针旋转 $120°$，σ 为翻折，从而可知 D_6 中元的阶为 2 或 3，不存在 6 阶元，即为一个反例. ♣

22.证明 由 $G \subseteq \mathrm{GL}(n, \mathbb{R})$，从而由第 4 题可知满足封闭性，故构成群，即 $G < \mathrm{GL}(n, \mathbb{R})$.

若 $\sum_{i=1}^{m} \mathrm{tr}A_i = 0$，也即 $\mathrm{tr}\left(\sum_{i=1}^{m} A_i\right) = 0$，下面归纳证明对任意 $k \in \mathbb{N}^*$，有 $\mathrm{tr}\left(\sum_{i=1}^{m} A_i\right)^k = 0$，更进一步，我们将归纳证明对 $(A_1 + \cdots + A_m)^k$ 可分为 n^{k-1} 组，且每一组均为对 G 全体求和.

假设命题对 k 成立，则对 $(A_1+\cdots+A_m)^{k+1} = A_1(A_1+\cdots+A_m)^k+\cdots+A_m(A_1+\cdots+A_m)^k$，设 $(A_1 + \cdots + A_m)^k$ 可划分为 n^{k-1} 组，对其中任一组，有 $A_1G = A_2G = \cdots = A_mG = G$(这是由群的消去律保证)，从而可知 $(A_1 + \cdots + A_m)^{k+1}$ 是对 $n \cdot n^{k-1} = n^k$ 组 G 进行求和，从而由可知命题成立，设 $A = \sum_{i=1}^{m} A_i$，则有

$$\mathrm{tr}A^k = 0, \quad \forall k \in \mathbb{N}^*.$$

从而设 A 不同的非零特征值为 $\lambda_1,\cdots,\lambda_t$(若存在的话)，其重数分别为 $d_1,\cdots,d_t$，则我们结合 $\mathrm{tr}A^k=m_1\lambda_1^k+\cdots+m_t\lambda_t^k=0$，从而写成线性方程组即

$$\begin{pmatrix}1&1&\cdots&1\\ \lambda_1&\lambda_2&\cdots&\lambda_t\\ \vdots&\vdots&\cdots&\vdots\\ \lambda_1^{t-1}&\lambda_2^{t-1}&\cdots&\lambda_t^{t-1}\end{pmatrix}\begin{pmatrix}d_1\lambda_1\\ d_2\lambda_2\\ \vdots\\ d_t\lambda_t\end{pmatrix}=0,$$

则由左侧为 Vandermonde 矩阵可逆，故有 $\lambda_1=\cdots=\lambda_t=0$，矛盾！从而 A 的特征值均为 0，从而 A 为幂零矩阵，设 $A^l=O$，则有 $(A_1+\cdots+A_m)^l=O$，而由上述论证我们不难得到 $(A_1+\cdots+A_m)^l=n^{l-1}(A_1+\cdots+A_m)=O$，即 $A=O$，从而可知 $\sum\limits_{i=1}^{m}A_i=O$，即证. ♣

Remark. 本题是第九届 CMC 初赛第三题.

23.证明 (1) 显然任意 $x\in A\cap B$，则 $gx\in gA,gx\in gB$ 从而 $g(A\cap B)\subseteq gA\cap gB$，另一方面 $ga=gb\in gA\cap B$，则 $a=b\in A\cap B$，即证.

(2) 设 $[G:A]=m<\infty,[G:B]=n<\infty$，我们先证明 $[A:A\cap B]\le[G:B]=n$. 注意到若 $a_1(A\cap B)\neq a_2(A\cap B)$，从而 $a_1^{-1}a_2\notin A\cap B$，也即 $a_1^{-1}a_2\notin B$，即 $a_1B\neq a_2B$，这意味着 $A/A\cap B$ 中的不同左陪集蕴含着 G/B 中对应的代表元左陪集不同，意味着后者陪集代表元系更多，从而即证 $l=[A:A\cap B]\le[G:B]=n$.

我们下面证明 $[G:A\cap B]=[G:A][A:A\cap B]$，由右侧乘积均为有限数，从而考虑 G 对 A 的左陪集分解 $G=\bigcup\limits_{i=1}^{m}g_iA$ 与 A 对 $A\cap B$ 的左陪集分解 $A=\bigcup\limits_{i=1}^{l}a_i(A\cap B)$，则我们有

$$G=\bigcup_{i=1}^{m}\bigcup_{j=1}^{l}g_ia_j(A\cap B),\quad(*).$$

又注意到若 $g_ia_j(A\cap B)=g_{i'}a_{j'}(A\cap B)$，则 $(g_{i'}a_{j'})^{-1}g_ia_j\in A\cap B$，即 $g_{i'}^{-1}g_i\in A$，从而 $g_{i'}A=g_iA$，即 $i'=i$，又由 $a_{i'}^{-1}g_{i'}^{-1}g_ia_i\in B$，又由 $g_{i'}=g_i$，从而 $a_{i'}^{-1}a_i\in B$，从而 $a_{i'}B=a_iB$，即 $i=i'$，综上有 $(*)$ 为 G 对 $A\cap B$ 的左陪集分解，从而 $[G:A\cap B]=ml\le mn=[G:A][G:B]$.

(3) **扩展结论**：$[G:A\cap B]\ge\mathrm{lcm}([G:A],[G:B])$.

由上述证明我们不难得到 $[G:A\cap B]=[G:A][A:A\cap B]=[G:B][B:A\cap B]$，从而有 $m|[G:A\cap B]$ 和 $m|[G:A\cap B]$，这即表明 $\mathrm{lcm}(m,n)|[G:A\cap B]$，即证.

综上我们可得到如下结论 ♣

命题 1.2.5: 有限指数子群交的指数估计

设 G 为群 (不一定有限)，$A,B<G$ 且 $[G:A]<\infty,[G:B]<\infty$，则我们成立

$$\mathrm{lcm}([G:A],[G:B])\le[G:A\cap B]\le[G:A][G:B].$$

24.证明 (1) 若 $h_1gk_1 = h_2gk_2$，等价于 $k_1k_2^{-1} = g^{-1}h_1^{-1}h_2g$，从而 $k_1k_2^{-1} \in g^{-1}Hg \cap K := M$，则对任意 $h, k \in H, K$，我们考虑 $\{(i,j)|h_igk_j = hgk\}$，则可知 $Mk_j = Mk$，即存在 $m \in M$，$k_j = mk$，则 $h_i = hgm^{-1}g$ 也被唯一确定，从而可知 $\{(i,j)|h_igk_j = hgk\} \Leftrightarrow Mk$，从而元素个数为 $|M|$，故可知对所有 hgk，相等的汇聚一类，每一类均有 $|M|$ 个，从而我们有

$$|HgK| = \frac{|H||K|}{|M|} = \frac{|H||K|}{|K|/[K : g^{-1}Hg \cap K]} = |H|[K : g^{-1}Hg \cap K],$$

同理我们可证另一方面，综上我们完成了证明.

(2) 我们证明 $Hg_1K \bigcap Hg_2K \neq \varnothing$ 蕴含着 $Hg_1K = Hg_2K$，注意到由交非空，从而存在 $h_1g_1k_1 = h_2g_2k_2$，即有 $g_2 = h_2^{-1}h_1g_1k_1k_2^{-1}$，从而任意 $hg_2k = h_3g_1k_3 \in Hg_1K$，从而同理可得另一方面进而两个双陪集相等，从而 G 可分解为不相交的双陪集的并，即证. ♣

Remark. 根据代数三百题，本题或许遗漏了“G 为有限群”这一重要条件.

25.证明 由 $H < G$, 从而由题 24 可知, 存在 G 的双陪集分解, 使得 $G = \bigcup AgA$, 而事实上我们进一步可以将每个 AgA 看作若干不交陪集的并, 即存在 $a_i, b_i \in A$ 使得 $AgA = \bigcup Aga_i = \bigcup b_igA$, 进而由 24(2) 可得到划分的陪集均有 $[A : A \cap gAg^{-1}]$ 个，从而我们可以考虑

$$AgA = \bigcup Ab_iga_i = \bigcup b_iga_iA,$$

其中利用了 $Ab_i = a_iA = A$，从而我们对双陪集分解中的每个 g，都可以选取出与 g 有关的 b_i, a_i 使得

$$G = \bigcup AgA = \bigcup\bigcup Ab_iga_i = \bigcup\bigcup b_iga_iA,$$

则考虑 $g_1, \cdots, g_n$ 选取为所有 b_iga_i 即可. ♣

Remark. 这个解答 copy 自代数三百题 P52，确实很有难度。。。

证明(另外一个证明) 任取 $S = \{g_1, \cdots, g_n\}$ 为一组左陪集代表元系，即有 $G = \bigcup_{i=1}^{n} g_iH$，从而易见 $G = \bigcup_{i=1}^{n}(g_iH)^{-1} = \bigcup_{i=1}^{n} Hg_i^{-1}$ 为右陪集的并，即 $T = \{g_1^{-1}, \cdots, g_n^{-1}\}$ 为一组右代表元系，我们希望成立 $g_iH = Hg_i^{-1}$，但明显这并不总成立:

Case I. 若 $g_iH = Hg_i^{-1}$, 从而可知 $g_i \in Hg_i^{-1}$, 也即 $g_i^2 \in H$, 从而有 $g_i^2H = H$, 进而 $g_iH = g_i^{-1}H$, 从而同时取逆，即有 $Hg_i = (g_i^{-1}H)^{-1} = Hg_i^{-1}$，因此在这种情况下，我们惊喜的发现即有 $gH_i = Hg_i$，这部分满足了我们的预期，这部分元素组成的集合记为 S_1.

Case 2. 若 $g_iH \neq Hg_i^{-1}$，即存在 $g \in g_iH$ 但 $g \notin Hg_i^{-1}$，从而一方面 $gH = g_iH$，$Hg^{-1} = Hg_i^{-1}$，从而 $g^2 \notin H$，否则 $g \in Hg^{-1} = Hg_i^{-1}$，矛盾! 从而我们有 $g^{-1}H \neq gH$，$Hg^{-1} \neq Hg$，假设 $g^{-1}H = g_jH$，从而我们用 g, g^{-1} 代替 S 中的 g_i, g_j，对应的 T 中 g_i^{-1}, g_j^{-1} 换为 g^{-1}, g.

综上对每个 $g_i \in S \setminus S_1$，我们能找到一个 g_j 使得可以整体替换为为 g, g^{-1}，因此不断替换下去，即可得到 $S' = S_1 \cup \{g, g^{-1}, \cdots\} = T'$，这既是符合要求的一组代表元系，既为左陪集代表元系，也为右陪集代表元系.(这蕴含着 $S \setminus S_1$ 元素个数为偶数一神奇现象) ♣

Remark. 这个证明也算自然，为了凑出右陪集，自然会考虑去对左陪集同时取逆，那么就会想怎么把逆变得和原来一样，就会发现如果 $gH = Hg^{-1}$，就会有 $g^2 \in H$ 这样的好事，如果对其他的则可以巧妙配对.

1.3 正规子群与商群

1.3.1 Notes

定义 1.3.1: 正规子群、单群

设 $h < G$，如果对任意 $g \in G$，$h \in H$，成立

$$ghg^{-1} \in H,$$

则称 H 为 G 的一个**正规子群**，记为 $H \lhd G$.

易见一个非平凡群 G 至少有两个正规子群 G 和 $\{e\}$，称为**平凡正规子群**，如果一个非平凡群只有平凡的正规子群仅有平凡正规子群，则称其为**单群**.

定义正规子群的本质目的来源于在左陪集上定义运算的渴望，如果我们希望成立 $aH \cdot bH = abH$，那么这蕴含着 $bH = Hb$，对任意 $b \in G$，这即正规子群的定义来源.

命题 1.3.1: 思考题

构造 G 与非空子集 S 使得满足条件

$$gsg^{-1} \in G, \quad \forall g \in G, s \in S,$$

但 S 不为 G 的正规子群.

解 考虑 $G = \mathrm{GL}(n, \mathbb{R})$，从而考虑 $S = \{M \in G | \det M = 2\} \subseteq G$，从而易见任意 $J \in G$，有 $\det(JMJ^{-1}) = 2$，从而仍在子集 S 中，但显然 S 无法构成群，更无法成为正规子群. ♠

定义 1.3.2: 共轭、共轭类

如果对 $a, b \in G$，存在 $g \in G$ 使得 $b = gag^{-1}$，则称 a 和 b 是**共轭**的，进一步，与 a 共轭的全体记为 $C_a = \{gag^{-1} | g \in G\}$，称为 a 的**共轭类**.

利用正规子群，我们便不难实现最初的动机：

定义 1.3.3: 商群

设 $H \lhd G$，则 G/H 可以定义二元运算构成群，称为 G 对 H 的**商群**.

命题 1.3.2: 思考题

设 $H < G$，若能在左陪集空间 G/H 上定义群结构，是否一定有 H 为 G 的正规子群?

解 答案是否定的，因为由 Zorn 引理，任何一个集合上都可以定义群结构，因此如果仅仅只是存在群结构，那 H 与 G 并没有任何直接联系. 但是另一方面，若群结构里自然定义了运算为

$aH * bH = abH$，那一定是正规子群. ♠

Remark. 这部分内容来自知乎回答.

定理 1.3.1: 正规子群的亚“传递”性

若 $H < G$，$N \lhd G$，则 $H \cap N \lhd H$.

证明 显然 $H \cap N < H$，且任意 $n \in H \cap N$，$h \in H$，则有 $hnh^{-1} \in N$(由 N 的正规性)，又 $n \in H$，从而 $nhn^{-1} \in H$，则 $nHn^{-1} \in H \cap N$，从而可知 $H \cap N \lhd H$，即证. ♣

Remark. 这里笔者起名叫亚传递性，为什么捏，因为一般的传递性 $H \lhd G$，$K \lhd H$ 并不能保证 $K \lhd G$，反例可见习题 8.

定义 1.3.4: 子群上的半直积与内直积

设 $N \lhd G$，且存在 $H < G$ 使得 $H \cap N = \{e\}$ 且 $HN = G$，则称 G 为 H 与 N 的**半直积**，记为 $G = H \ltimes N$，特别地，若 H 也为正规子群，则称 G 为 H 与 N 的**内直积**，记为 $G = H \times N$.

1.3.2 Exercises From Z.Fh

1.证明 一方面，由 $B \lhd G$，从而 $aba^{-1} \in B$，进而 $aba^{-1}b^{-1} \in B$，同理另一方面有 $a(ba^{-1}b^{-1}) \in A$，进而可知 $aba^{-1}b^{-1} \in A \cap B$. ♣

2.证明 若 $H \lhd G$，故可知 $H \subseteq \bigcup_{h \in H} C_h$，又由正规性，$C_h \subseteq H$，从而 $H = \bigcup_{h \in H} C_h$，即为 G 的一些共轭类的并；

若 H 是 G 的一些共轭类的并，反证若 H 不是 G 的正规子群，即存在 $g \in G, h \in H$，使得 $ghg^{-1} \notin H$，从而 C_h 不为 H 的子集，这与 $H = \bigcup_{h \in H} C_h$ 矛盾! ♣

3.证明 不难证明封闭性与结合律，有注意到幺元为 (e_H, e_K)，(h, k) 的逆元为 (h^{-1}, k^{-1})，从而可知 $H \times K$ 为群. 用定义不难证明 H_1, K_1 为正规子群，略去. ♣

4.证明 若 R 是一个同余关系，为了证明可以定义运算，即证明运算的合理性，若 $a\mathrm{R}c$，$b\mathrm{R}d$，则 $\bar{a} \circ \bar{b} = \bar{c} \circ \bar{d}$，从而由 R 为同余关系可知 $ab\mathrm{R}cd$，则有 $\overline{a \circ b} = \overline{c \circ d}$，故这个运算良定义. ♣

7.证明 考虑关系 R: $a\mathrm{R}B$ 当且仅当 $C_a = C_b$，则一方面不难证明其为等价关系，且若 $C_a \cap C_b \neq \varnothing$，从而可知存在 $g, h \in G$ 使得 $gag^{-1} = hbh^{-1}$，这即 $b = (h^{-1}g)a(h^{-1}g)^{-1}$，从而 $C_a = C_b$，这即蕴含着不同的共轭类不交，从而为 G 为一个划分. ♣

8.解 我们可以考虑 $\mathbb{Z}_2 \lhd K_4 \lhd S_4$，这为同构意义下的表示，其中均用置换群可表示为

$$\mathbb{Z}_2 = \{(1), (12)\}, \quad K_4 = \{(1), (12)(34), (13)(24), (14)(23)\},$$

从而任意 $\sigma \in S_4, \pi = (ij)(st) \in K_4$，有 $\sigma\pi\sigma^{-1} = (\sigma(i)\sigma(j))(\sigma(s)\sigma(t)) \in K_4$，从而 $K_4 \lhd S_4$，另一方面不难验证 $\mathbb{Z}_2 \lhd K_4$，且注意到 $(1234)(12)(4321) = (23) \notin \mathbb{Z}_2$，从而不为正规子群. ♠

9.证明 由 $H \lhd G$，$K \lhd G$，从而任意 $h \in H, k \in K$，有 $ghg^{-1} \in H, gkg^{-1} \in K$，对任意 $g \in G$，从而 $ghkg^{-1} = (ghg^{-1})(gkg^{-1}) \in HK$，即证 $HK \lhd G$. ♣

10.证明 设 $H = \{h_1, \cdots, h_m\} < G$，若 H 不为 G 的正规子群，则不妨设存在 $gh_1g^{-1} \notin H$，则考虑 $H' = gHg^{-1}$，则易见 $gHg^{-1} \neq H$，且 $|gHg^{-1}| = m$，并且任意 $gh_ig^{-1}, gh_jg^{-1} \in H'$，有 $(gh_ig^{-1})(gh_jg^{-1})^{-1} = gh_ih_j^{-1}g^{-1} \in H'$，从而 $H' < G$，这与 H 的唯一性矛盾! ♣

12.证明 由 $[G : H] = 2$，从而可知 $G = H \cup gH$，则我们考虑右陪集 Hg，则易见 $Hg \cap H = \varnothing$，否则 $g \in H$，从而有 $gH = Hg$，即 $H \lhd G$. ♣

13.证明 假设 G 有 n 阶子群 H, H_1，从而一方面由 lagrange 定理 $|G| = |H|[G : H] = mn$，则我们考虑 G 对 H, H_1 的双陪集分解

$$G = \bigcup_{g \in G} HgH_1,$$

则我们不难发现，由 $H \lhd G$，则由习题 1.2 的问题 24，我们有每个双陪集的元素个数均有

$$|HgH_1| = |H|[H_1 : g^{-1}Hg \cap H_1] = |H|[H_1 : H \cap H_1] = \frac{|H||H_1|}{|H \cap H_1|},$$

从而每个双陪集的元素个数均为 $\dfrac{n^2}{|H \cap H_1|}$，则由双陪集分解为不交并，且每个双陪集元素个数一样，故成立

$$\frac{n^2}{|H \cap H_1|} = \frac{|H||H_1|}{|H \cap H_1|} \Bigg| |G| = mn,$$

又 $(m, n) = 1$，从而有 $n||H \cap H_1|$，这意味着 $|H \cap H_1| = n$，从而 $H = H_1$，即证 H 是 G 的唯一 n 阶子群. ♣

14.证明 (2) 若 H 的两个共轭子群相等，即 $g_1Hg_1^{-1} = g_2Hg_2^{-1}$，等价于任意 $h \in H$，$g_2^{-1}g_1hg_1^{-1}g_2 \in H$，也即等价于 $g_2^{-1}g_1 \in N_G(H)$，从而考虑 G 对 $N_G(H)$ 的左陪集空间，则可知共轭子群的个数即为 $[G : N_G(H)]$，而又有 $H \lhd N_G(H) < G$，从而由推广的 Lagrange 定理 (习题 1.2 的问题 23)，可知

$$[G : N_G(H)] = \frac{[G : H]}{[N_G(H) : H]} = \frac{n}{[N_G(H) : H]},$$

这即意味着 H 的共轭子群的个数有限且为 n 的因数，即证. ♣

15.证明 设 H 的共轭子群的并为 $\sigma = \cup gHg^{-1}$，下面估计 σ 中的元素个数，由 14 题可知，共轭子群的个数为 $[G : N_G(H)]$，又对任意 g，gHg^{-1} 均有 $|H|$ 个元素，且考虑到幺元在每个共轭子群中都会出现一次，所以我们考虑更细致的估计为

$$|\sigma| \leq (|H| - 1)[G : N_G(H)] + 1 = |H|[G : N_G(H)] - [G : N_G(H)] + 1,$$

又注意到

$$|H|[G : N_G(H)] - [G : N_G(H)] + 1 = \frac{|G||H|}{|N_G(H)|} - \frac{|G|}{|N_G(H)|} + 1 = |G|\left(\frac{|H| - 1}{|N_G(H)|}\right) + 1,$$

且我们结合 $H \lhd N_G(H) < G$，不难得到 $|H| \leq |N_G(H)| \leq |G|$，进而我们有估计

$$|\sigma| \leq |G| \cdot \frac{|N_G(H)|-1}{|N_G(H)|} + 1 \leq |G| \cdot \frac{|G|-1}{|G|} + 1 = |G|.$$

从而若有 $\sigma = G$，则可知上述不等式均取等号，意味着 $H = N_G(H) = G$，这与 H 为 G 的真子群矛盾！即证.

若考虑无限群，则熟知任一复矩阵都相似于上三角矩阵，从而我们考虑 $G = \mathrm{GL}(n,\mathbb{R})$，$H$ 为全体上三角可逆矩阵，则我们不难得到 G 为 H 的共轭子群之并，从而对无限阶群不成立. ♣

Remark. 虽然在 1.1 中已经证明了一个群不能写为两个真子群的并，但是这并不能推广到任意有限个，比如考虑 Klein 四元群 K_4，则易见其有子群 $\{e,a\},\{e,b\},\{e,c\}$，则 K_4 可以写为三个真子群的并，因此本题并不能通过证明上述假设来完成.

17.解 当 n 为奇数时，$\mathrm{SL}(n,\mathbb{R})$ 为单群；

当 n 为偶数时，$\mathrm{SL}(n,\mathbb{R})$ 有唯一非平凡正规子群 $\{I,-I\}$. ♠

Remark. 查了挺多资料，貌似都要借助 Lie 代数或者其他后续知识.

1.4 群的同态与同构

1.4.1 Notes

定义 1.4.1: 同态、同构

设 G 和 G' 是两个群，如果映射 $f: G \to G'$ 满足 $f(ab) = f(a)f(b), \quad \forall a, b \in G$, 则称 f 是 G 到 G' 的一个**群同态**，若 f 是双射，则称 f 是**群同构**，此时称 G 与 G' 是**同构**的，记为 $G \simeq G'$，特别地，成群 G 到自身的同构为 G 的一个**自同构**.

不难看见，同态是保持幺元与逆元性质的，这是一个很重要的基本性质.

命题 1.4.1: 思考题

若一个群 G 到自身的映射 $a \mapsto a^2$ 是一个同态，则 G 是 Abel 群.

证明 不难得到 $(ab)^2 = a^2b^2$，这即 $ba = ab$，即证. ♣

定义 1.4.2: 自同构群

设 G 的自同态全体记为 $\mathrm{Hom}(G)$，自同构的全体记为 $\mathrm{Aut}(G)$，则不难证明为 $\mathrm{Hom}(G)$ 为一个幺半群，$\mathrm{Aut}(G)$ 为一个群，成为 G 的**自同构群**.

事实上，更进一步，类比高代里矩阵相似的概念，我们不难得到一类更重要的同构：

定义 1.4.3: 内自同构群

设 G 为群，$a \in G$，定义映射 $\mathrm{Ad}_a: G \to G$ 为

$$\mathrm{Ad}_a(g) = aga^{-1}, \quad \forall g \in G,$$

则 $\mathrm{Ad}_a \in \mathrm{Aut}(G)$，成为由 a 决定的**内自同构**. 记 $\mathrm{Inn}(G) = \{\mathrm{Ad}_a | a \in G\}$，则 $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$，成为 G 的**内自同构群**，商群 $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ 称为 G 的**外自同构群**.

上述定义中的内容是不难通过定义证明的.

命题 1.4.2: 思考题

存在群 G 使得 $\mathrm{Inn}(G) \neq \mathrm{Aut}(G)$.

证明 考虑 $G = K_4$，则 $\mathrm{Aut}(K_4)$ 有 6 个元素，但 $\mathrm{Inn}(K_4) = \{\mathrm{id}\}$，因此不同. ♣

定理 1.4.1: 核与像的性质

设 $f: G \to G'$ 为群同态，则 $\mathrm{Im}f < G'$，$\mathrm{Ker}f \lhd G$.

证明 任意 $f(a), f(b) \in \mathrm{Im}f$，有 $f(a)(f(b))^{-1} = f(ab^{-1}) \in G'$，从而为子群. 对任意 $k \in \mathrm{Ker}f$，有 $f(k) = e'$，且任意 $g \in G$，有 $g(gkg^{-1}) = f(g)e'(f(g))^{-1} = e'$，从而可知为正规子群. ♣

定理 1.4.2: 群的同态基本定理

设 $f : G \to G'$ 是群的满同态，则 $G/\mathrm{Ker}f \simeq G'$(也可写为 $G/\mathrm{Ker}f \simeq \mathrm{Im}f$).

证明 我们考虑建立 $G/\mathrm{Ker}f$ 到 G' 的映射：$a\mathrm{Ker}f \mapsto f(a)$，这么联想是自然的，那么为了验证这个映射是一个群同构，我们一般需要顺次验证如下几点：良定义 (商空间上的映射像不依赖于代表元的选取)，是群同态，是双射，三部曲一步不可遗漏.

我们记 $N = \mathrm{Ker}f$，我们定义映射 $\overline{f} : G/N \to G'$，$gN \mapsto f(g)$，我们先证第一步：若 $gN = hN$，则 $g^{-1}h \in N$，从而 $f(g^{-1}h) \in f(N) = \{e\}$，从而 $f(g) = f(h)$，因此 $\overline{f}$ 良定义.

我们再证第二步：任意 $g, h \in G$，

$$\overline{f}(gN \cdot hN) = \overline{f}(ghN) = f(gh) = f(g)f(h) = \overline{f}(gN)\overline{f}(hN),$$

这即证明了 $\overline{f}$ 是群同态.

我们最后再证明 $\overline{f}$ 是双射，其中满射是平凡的，另一方面，若 $\overline{f}(gN) = \overline{f}(hN)$，则有 $f(g) = f(h)$，这即意味着 $f(g^{-1}h) = e$，从而 $g^{-1}h \in \mathrm{Ker}f = N$，即 $gN = hN$，从而这是单射，综上我们证明了 $\overline{f}$ 是 G/N 到 G' 的一个群同构，从而我们完成了证明. ♣

群的同态基本定理给我们的启发就是：我们如果想要研究一个群 G 的所有同态像，感觉好像会很多，但事实上，每个同态像都会同构于 G 的一个商群，这即找出所有正规子群，从而这就完全转化到了去刻画 G 本身的性质上.

定理 1.4.3: 同态基本定理的进一步讨论

设 $f : G \to G'$ 是满同态，$N = \mathrm{Ker}f$，则

(1)f 建立了 G 中包含 N 的子群与 G' 中的子群间的双射；

(2)f 把包含 N 的正规子群对应到 G' 的正规子群；

(3) 若 $H \lhd G$，$N \subseteq H$，则 $G/H \simeq G'/f(H)$.

证明 (1) 显然对任意 $N \subseteq H < G$，有 $f(H) < G'$，而对任意 $H' < G'$，从而满射也是平凡的，我们主要考虑单射，即若 $f(H_1) = f(H_2)$，从而任意 $f(h_1)$，存在 $h_2 \in H_2$ 使得 $f(h_1) = f(h_2)$，从而 $h_1^{-1}h_2 \in N \subseteq H_2$，从而 $h_1 \in H_2$，从而 $H_1 \subseteq H_2$，同理 $H_2 \subseteq H_1$，则有 $H_1 = H_2$，故 f 为单射，从而两个群的子群之间存在一个对应；

(2) 直接照搬定义证明即可，略去；

(3) 由 (2) 可知 $H \lhd G$，则 $f(H) \lhd G'$，从而我们希望能照搬同态基本定理，从而我们希望构造一个从 $G \to G'/f(H)$ 的一个映射 f' 使得 $\mathrm{Ker}f' = H$，这么看或许不知道该如何定义 f'，但我们从 $G \to G'/f(H)$ 不难考虑 $\pi' \circ f$，这显然是一个满同态，下证 $\mathrm{Ker}(\pi' \circ f) = H$.

不难注意到

$$\mathrm{Ker}(\pi' \circ f) = f^{-1} \circ \pi'^{-1}(e' f(H)) = f^{-1}(f(H)) = H,$$

其中利用了 $N \subseteq H$，利用了 (1) 中的一一对应，从而由同态基本定理即可证明. ♣

Remark. 本题给我们了一个证明商群同构的模板，即考虑选取某一个正规子群为核，构造同构.

定理 1.4.4: 同态基本定理另一推论

我们如果对正规子群 $N \lhd G$ 与其自然同态 π，运用同态第二定理，则对 $N \subseteq H \lhd G$，有

$$G/H \simeq (G/N)/(H/N).$$

事实上，我们可以把任意满同态都转化为到一个商群的自然同态，由同态基本定理的同构作保证，这并不会损失任何信息，因此从这个角度出发，我们可以的到另一种表述语言：

定理 1.4.5: 同态基本定理的另一表述

射 G 是群，$N \lhd G$，π 是 G 到 G/N 的自然同态，$H < G$，则

(1)HN 是 G 中包含 N 的子群，且 $N \lhd HN$，$HN = \pi^{-1}(\pi(H))$；

(2)$\mathrm{Ker}(\pi|_H) = H \cap N$，从而 $(H \cap N) \lhd H$；

(3)$HN/N \simeq H/(H \cap N)$.

证明 (1) 不难发现 $\pi(HN) = \pi(H)$，而 HN 为包含 N 的子群，又自然满同态诱导了包含 N 的子群 HN 与 $\pi(H)$ 的一一对应，从而 $HN = \pi^{-1}(\pi(H))$；

(3) 由 $\pi(H) = \pi(HN) = HN/N$，从而 π 是 H 到 HN/N 的满同态，因此结合 $\mathrm{Ker}(\pi|_H) = H \cap N$，由同态基本定理，即可知

$$HN/N \simeq H/(H \cap N),$$

综上我们完成了证明. ♣

1.4.2 Exercises From Z.Fh

1.证明 **Case I.** 若 G 中存在 6 阶元 g，从而 $G = \langle g \rangle$，从而 $G \simeq \mathbb{Z}_6$；

Case II. 若 G 中无 6 阶元，从而熟知偶数阶群一定有 2 阶元，则若 G 中仅有二阶元，从而对 $a \neq b$，则 $(ab)^2 = e$，从而 $\{a, b, ab, e\} < G$，则 $4|6$，与 Lagrange 定理矛盾！从而存在三阶元，不妨设 a 为 2 阶元，b 为三阶元，则不难得到 $G = \{e, a, b, b^2, ab, ab^2\} \simeq S_3$.

综上我们证明了六阶群 G 必与 $\mathbb{Z}_6$ 或 S_3 同构. ♣

4.解 设 $f \in \mathrm{Aut}K_4$，则 $f(e) = e$，且 f 为单射，则考虑所有 $\{a, b, c\}$ 上的置换共六个，下证其均为自同构.

由对称性可知 $f(a)f(b) = f(c) = f(ab)$，从而 f 为同态，又显然是双射，从而为同构，即 $\mathrm{Aut}K_4 = \{f : K_4 \to K_4 | f(e) = e, f|_{\{a,b,c\}} \in S_{\{a,b,c\}}\}$. ♠

5.证明 若 $(k,|G|)=1$，从而可知若 $g^k=h^k$，设 g,h 的阶为 s,t，则可知 $(s,k)=(t,k)=1$，从而可知 $g^{st}=h^{st}=e$，故有 Bezout 定理，结合 $(st,k)=1$，则不难得到 $g=h$，从而为单射，进而为群同构.

若 φ_k 为群同构，且若 $(k,|G|)=d>1$，从而由 $\frac{k}{d}$ 与 $|G|$ 互素，则 $\varphi_{\frac{k}{d}}$ 为群同构，而注意到对任一阶为 $m||G|$ 的元 g，有 $(m,k)|d$，从而 $\left(g^{\frac{m}{(m,k)}}\right)^d=e$，则有 h 使得 $a=h^{\frac{k}{d}}=g^{\frac{m}{(m,k)}}\neq e$，则 $a^k=e$，与 φ 是单射矛盾！从而可知 $(k,|G|)=1$. ♣

8.证明 显然满足封闭性，又任意 $g_1,g_2,g_3\in G$，$h_1,h_2,h_3\in H$，一方面有

$$\begin{aligned}&((g_1,h_1)(g_2,h_2))(g_3,h_3)\\=&(g_1g_2,\varphi(g_2^{-1})(h_1)h_2)(g_3,h_3)\\=&(g_1g_2g_3,\varphi(g_3^{-1})\left(\varphi(g_2^{-1})(h_1)h_2\right)h_3)\\=&(g_1g_2g_3,\varphi(g_3^{-1}g_2^{-1})(h_1)\varphi(g_3^{-1})(h_2)h_3)\end{aligned}$$

另一方面也不难同理算出 $(g_1,h_1)((g_2,h_2)(g_3,h_3))=(g_1g_2g_3,\varphi(g_3^{-1}g_2^{-1})(h_1)\varphi(g_3^{-1})(h_2)h_3)$，从而可知满足结合律.

另一方面由 $\varphi(e_G^{-1})=\varphi(e_G)=\mathrm{id}$，从而易证 (e_G,e_H) 为幺元. 且对任意 $g\in G,h\in H$，存在逆元 $(g^{-1},\varphi(g)(h^{-1}))$，从而不难得知 $G\ltimes H$ 为群，余下的用定义不难验证. ♣

9.证明 任意 $f(a)=g(a)$，$f(b)=g(b)$，则显然 $f(ab^{-1})=g(ab^{-1})$，从而 $D<G$. ♣

10.证明 设 $a,f(a)$ 的阶分别为 k,l，从而结合 $a^k=e$，则 $e=f(a^k)=(f(a))^k$，从而 $l|k$，同理 $k|l$，故 $k=l$，也即 a 与 $f(a)$ 有同样的阶.

若 f 为群同态则不一定成立，如考虑 $\mathbb{Z}_4=\{e,a,a^2,a^3\}\to\mathbb{Z}_2=\{e,a^2\}$，其中 $f(a)=a^2$，从而可知 a 的阶为 4，但 $f(a)$ 的阶为 2，从而命题不再成立. ♣

11.证明 显然 $K\lhd G$，考虑 $G\to\mathbb{R}^*$ 的满同态 $f:(a,b)\mapsto a$，从而不难验证 $K=\mathrm{Ker}f$，从而由同态基本定理 $G/K\simeq\mathbb{R}^*$，即证. ♣

13.解 我们考虑 $G=G'=\{\mathbb{Z},+\}$，$N=2\mathbb{Z}\simeq\mathbb{Z}$，$N'=3\mathbb{Z}\simeq\mathbb{Z}$，从而 $N\simeq N'$，但显然 $G/N=\mathbb{Z}_2\not\simeq\mathbb{Z}_3=G'/N'$，从而既是一个反例. ♠

14.解(1) 若 $f(g)=f(h)$，从而 $\sigma(g)g^{-1}=\sigma(h)h^{-1}$，这即 $\sigma(h^{-1}g)=h^{-1}g$，从而 $h^{-1}g=e$，即 $h=e$，从而 σ 为单射；

(2) 由 G 为有限群，从而 f 为单射，进而为双射，因此为满射.

(3) 对任意 $g\neq e$，存在 $h\neq g$ 使得 $\sigma(g)=h$，$\sigma(h)=g$，则可知能两两配对，因此 G 一定为奇数阶，由 (2) 有对任意 $g\in G$ 存在 h 使得 $g=\sigma(h)h^{-1}$，从而 $\sigma(g)=h\sigma(h^{-1})=g^{-1}$，从而任意 $a,b\in G$，存在 $a=\sigma(s),b=\sigma(t)$，则 $ab=\sigma(st)=t^{-1}s^{-1}=\sigma(t)\sigma(s)=ba$，从而 G 为 Abel 群，即证. ♠

15.解 我们称两个幺半群 S_1,S_2 同构，如果存在双射 $f:S_1\to S_2$，且满足 $f(a)f(b)=f(ab)$，对任意 $a,b\in S_1$，则考虑 $f:\{\mathbb{Z},*\}\to\{\mathbb{Z},\cdot\}$，$a\mapsto 1-a$ 对任意 $a\in\{\mathbb{Z},*\}$，从而不难验证这是一个幺半群同构. ♠

16.解 考虑满同态 $f(z)=|z|$，从而取 $N=\mathrm{Ker}f=\{z\in\mathbb{C}^*||z|=1\}$ 即可. ♠

17. 只是第五题换了一个表述.

18.证明 (1) 我们先证明这是满射，显然 $\varphi(1)=1$，且若假设不存在 $\varphi(a)=-1$，从而任意 $a\in\mathbb{Z}_p^*$，存在 b_a 使得 $a\equiv b_a^2(\mathrm{mod}\ p)$，从而 $(\mathbb{Z}_p^*)^2=\mathbb{Z}_p^*$，但注意到 $1^2\equiv(p-1)^2(\mathrm{mod}\ p)$，从而可知矛盾，因此一定存在 a 使得 $\varphi(a)=-1$.

下证其是一个同态，我们考虑证明如下的 Euler 判别法，即成立

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(\mathrm{mod}\ p),\quad \forall a\in\mathbb{Z}_p^*.$$

(i) 若 a 可被平方表示，从而有 $a^{\frac{p-1}{2}}\equiv(b^2)^{\frac{p-1}{2}}1(\mathrm{mod}\ p)$，其中用到了 Fermat 小定理；

(ii) 若 a 不可被平方表示，从而有任意 $i\in\mathbb{Z}_p^*$，有 $i\not\equiv i^{-1}a(\mathrm{mod}\ p)$，从而可将 $\{1,2,\cdots,p-1\}$ 两两配对，且一对 (i,j) 满足 $ij\equiv a(\mathrm{mod}\ p)$，则可知所有对乘积则得

$$a^{\frac{p-1}{2}}\equiv(p-1)!\equiv-1(\mathrm{mod}\ p),$$

其中用到了 Wilson 定理，从而综上可知 Euler 判别法成立.

因此利用 Euler 判别法，不难看到 φ 为一个同态，进而为满同态.

(2) 由 (1) 可知 φ 为满同态，且 $\ker\varphi=\mathrm{Im}f_2$，故由同态基本定理 $\mathbb{Z}_p^*/\mathrm{Im}f_2\cong\{-1,1\}$. ♣

19.证明 由习题 1.2-13 可知，$\mathrm{SL}(2,\mathbb{Z})=\langle S,R\rangle=\left\langle\begin{pmatrix}0&-1\\1&0\end{pmatrix},\begin{pmatrix}0&-1\\1&1\end{pmatrix}\right\rangle$，从而对任意 $\chi\in\mathrm{Hom}(\mathrm{SL}(2,\mathbb{Z}),\mathbb{C}^*)$，由 $\mathbb{C}^*$ 具有交换性，因此不难得到

$$\chi(S^{n_1}R^{m_1}\cdots S^{n_k}R^{n_k})=\chi(S^{n_1+\cdots+n_k}R^{m_1+\cdots+m_k})=(\chi(S))^{n_1+\cdots+n_k}(\chi(R))^{m_1+\cdots+m_k},$$

也即 $\mathrm{SL}(2,\mathbb{Z})$ 的所有同态像均有 $\chi(S)$ 与 $\chi(R)$ 生成，又 $S^4=I_2$，$R^6=I_2$，从而 $(\chi(S))^4=1$，$(\chi(R))^6=1$，则不妨设 $\chi(S)=\zeta_4$，$\chi(R)=\zeta_6$ 为单位根，从而同态像为 $\langle\zeta_4,\zeta_6\rangle=\langle\zeta_{12}\rangle$，因此像均在 12 次单位根中.

另一方面，对任意四次单位根 ζ_4，六次单位根 ζ_6，其均可构成一个同态像，因此也即所有这样的同态共 24 个，即 $\mathrm{Hom}(\mathrm{SL}(2,\mathbb{Z}),\mathbb{C}^*)=\{f|f(S)=\zeta_4,f(R)=\zeta_6\}$. ♣

20.证明 (1) 我们只需证明 φ_q 是保持模长的，而注意到

$$(\varphi_q(A),\varphi_q(A))=\frac{1}{2}\mathrm{tr}(qAq^HqA^Hq^{-1})=\frac{1}{2}\mathrm{tr}(AA^H)=(A,A),$$

因此可知 φ_q 为正交变换.

又注意到 $W=L(i,j,k)$。从而 $W^\perp=L(1)$，则由 $W^\perp$ 为不变子空间，从而由 φ_q 为正交变换，进而为正规变换，从而 $W=(W^\perp)^\perp$ 为不变子空间，即证.

(2) 由 W 可视为三维欧氏空间 $\mathbb{R}^3$，从而 $\varphi_q|_W$ 作为 W 上的正交变换，从而 $\Phi(q)\in O(3)$，又注意到对任意 $q_1,q_2\in\mathrm{SU}(2)$，$\Phi(q_1q_2)$ 表示 $\varphi_{q_1q_2}|_W$ 的表示矩阵，则不难知道可看作正交变换 φ_{q_1} 与 φ_{q_2} 的复合，从而其可表示为 $\Phi(q_1)\Phi(q_2)$，因此 Φ 是一个群同态，后面可参考知乎文章.

♣

22. 只是第 14 题换了个表述.

23.证明 注意到 $\varphi(AB)=\overline{AB}$，则 $\overline{AB}_{ij}=\overline{\sum a_{ik}b_{kj}}=\sum\overline{a_{ik}}\cdot\overline{b_{kj}}=(\overline{A}\cdot\overline{B})_{ij}$，从而 $\varphi(AB)=\varphi(A)\varphi(B)$，因此 φ 为群同态.

(满同态还不会，哭)

♣

1.5 循环群

1.5.1 Notes

命题 1.5.1: 思考题

存在有限群 G 及 $|G|$ 的因子 m，使得 G 中不存在 m 阶子群.

证明 考虑正六边形的二面体群 D_{12}，可知其元素阶为 2 或 6，从而不难证明其无 4 阶子群. ♣

定理 1.5.1: 循环群子群的结构

循环群 $G=\langle a\rangle$ 的任一子群都形如 $\langle a^l\rangle$，$l\in\mathbb{N}$，从而也是循环群.

证明 由 G 同构于某个整数加群，从而我们只考虑证明 $\mathbb{Z}$ 的情形，其余本质类似. 设 $H<\mathbb{Z}$，从而有 $m\in H\subseteq\mathbb{Z}$ 且 $m\neq 0$，则不妨设 $m>0$(否则用 $-m$ 代替). 且不妨设 m 为 H 中绝对值最小的数，从而由归纳法不难证明 $mn\in H$ 对任意 $n\in\mathbb{Z}$，从而 $m\mathbb{Z}\subseteq H$，又若存在 $n\in H$ 且 $m\nmid n$，则考虑 $d=\gcd(m,n)$，则由 Bezout 定理，存在 $a,b\in\mathbb{Z}$，使得 $d=am+bn\in H$，而 $0<d<m$，这与 m 的最小性矛盾！从而 $H=m\mathbb{Z}$，即证. ♣

定理 1.5.2: 循环群的子群

设 G 是 n 阶循环群，$k\mid n$，则存在 G 的唯一的 k 阶子群.

证明 一方面存在性，不难发现对任意 $k\mid n$，有子群 $\left\langle a^{\frac{n}{k}}\right\rangle<G$ 为 k 阶子群. 另一方面唯一性，若 G 有 k 阶子群 H，则其一定形如 $\langle a^l\rangle$，且 a^l 的阶为 k，从而设 $l=\min\{m\in\mathbb{N}^*|a^m\in H\}$，从而由 $n|kl$，则 $\left.\frac{n}{k}\right|l$，从而 $\langle a^l\rangle\subseteq\left\langle a^{\frac{n}{k}}\right\rangle$，而两者元素个数相等，从而 $\langle a^l\rangle=\left\langle a^{\frac{n}{k}}\right\rangle$，即证唯一性. ♣

定理 1.5.3: 一类简单的单群

设 G 是 n 阶 Abel 群，则 G 为单群当且仅当 G 为素数阶群.

1.5.2 Exercises From Z.Fh

1.证明 显然，若有四阶元，则同构于 $\mathbb{Z}_4$，若无四阶元，则全为二阶元即同构于 K_4. ♣

3.证明 我们考虑映射 $f:\mathbb{Z}_m\times\mathbb{Z}_n\to\mathbb{Z}_{mn},(a^r,b^t)\mapsto c^{nr+mt}$，其中我们不妨 $\mathbb{Z}_m=\langle a\rangle$，$\mathbb{Z}_n=\langle b\rangle$，$\mathbb{Z}_{mn}=\langle c\rangle$,我们先证明这是一个群同态,注意到 $f(r,t)f(r',t')=(a^r,b^t)(a^{r'},b^{t'})=(a^{r+r'},b^{t+t'})=f(r+r',t+t')$，这即表明这是群同态，而另一方面，我们证明这是单同态，若存在 $nr+mt=nr'+mt'$，也即 $n(r-r')=m(t'-t)$，从而由 $(m,n)=1$，则 $n|t'-t$，又 $0\leq t,t'\leq n$，从而 $t=t'$，同理 $r=r'$，因此可知这是单射，因此可知 f 为群同构，即证. ♣

4.证明 不难注意到 $\mathrm{Hom}(G)=\{\varphi:G\to G|a|\mapsto a^l,l\in\mathbb{Z}\}$，从而由习题 1.4-5 可知为群同构当且仅当 l 与 $|G|$ 互素，因此可知 $\mathrm{Aut}(G)=\{\varphi:G\to G|a|\mapsto a^l,(l,|G|)=1\}$，特别地，若 $|G|=\infty$，则其不存在非平凡自同构. ♣

5.解 不一定，如考虑 K_4，其任意真子群均为二阶循环群. ♠

7.解 G 的生成元为 a 或 a^{-1}，若其有生成元 a^l 且 $|l|>1$，则任意 $a^{nl}\neq a$，否则 a 阶有限，与无限阶群矛盾.

设 r 满足 $(r,m)=1$，则可知 $\langle b^r\rangle$ 的阶为 m，从而其为一个生成元，若 $(k,m)=d>1$ 则任意 $b^l\in\langle b^k\rangle$，有 $d|l$，从而 $b\notin\langle b^k\rangle$，故其不为生成元. ♠

8.证明 若 $H=\mathrm{Im}f$，其中 f 是从 G 到 H 的同态，从而由同态基本定理可知 $H\cong G/\ker f$，则

$$n=\frac{|G|}{\mathrm{Ker}f}=\frac{m}{\mathrm{Ker}f},$$

从而可知 $n\mid m$，即证. ♣

9.证明 ($\Rightarrow$) 若 G 为循环群，则存在 $a\in G$ 使得 $G=\langle a\rangle$，则 a 为 n 阶元，且任一元素阶不超过 n，从而 $n=\min K$；

($\Leftarrow$) 若 $n=\min K$，从而下证存在 $a\in G$ 使得其阶为 n，设 G 中元素可能的阶为 $d_1,d_2,\cdots,d_k$，且存在 $a_i^{d_i}=e(1\leq i\leq k)$，从而由 1.2-9 可知存在阶为 $[d_1,\cdots,d_k]$ 阶元，进而由 $[d_1,\cdots,d_k]\in K$，从而 $n\leq[d_1,\cdots,d_k]\leq n$，从而存在 n 阶元，即为循环群. ♣

10.证明 对任意有限生成子群 $S=\left\langle\frac{q_1}{p_1},\cdots,\frac{q_n}{p_n}\right\rangle$，设

$$P=p_1\cdots p_n,\quad Q=\gcd(q_1p_2\cdots p_n,\cdots,q_np_1\cdots p_{n-1}),$$

下证 $S=\left\langle\frac{Q}{P}\right\rangle$，一方面，任一 $g\in S$，可知其可表示为

$$g=\sum_{i=1}^n k_i\cdot\frac{q_i}{p_i}=\frac{1}{P}\sum_{i=1}^n k_iq_ip_1\cdots\widetilde{p_i}\cdots p_n=K\cdot\frac{Q}{P}\in\left\langle\frac{Q}{P}\right\rangle,$$

从而 $S\subseteq\left\langle\frac{Q}{P}\right\rangle$，另一方面由 Bezout 定理，可知 $\frac{Q}{P}\in S$，从而 $S=\left\langle\frac{Q}{P}\right\rangle$，即证任一有限生成子群为循环群. ♣

11.证明 设 $H<\mathbb{P}^*$，且 $|H|=n<\infty$，则任意 $h\in H$，从而有 $h^n=1$，则 H 中的元素均为 n 次单位根，又其互不相同，故 H 恰为全体 n 次单位根，即为循环群. ♣

12.证明 若 $|G|<\infty$，则 $|G|$ 至多 $2^{|G|}$ 个子群，从而只有有限个子群；

若 $|G|=\infty$，若每个元素阶有限，则一定有无穷多个子群，否则每个元素都能生成一个有限子群，则元素个数有限；若有无限阶元 g，从而考虑 $g\in G$，$\langle g^p\rangle$ 对任意素数 p 均为其子群，且互不相同，因此有无限个子群，综上即证. ♣

13.证明 若 a^l 的阶为 m，从而 $m=\frac{n}{(n,l)}$，从而 $l=\frac{n}{m}\cdot k$，且 $(k,n)=1$，$1\leq k\leq m$，则进而有 $(k,m)=1$，从而阶为 m 的元至少有 $\varphi(m)$ 个，若存在 $(k,m)=d>1$，从而不难发现此时 a^l 的阶为 $\frac{m}{d}$，因此 $(k,m)=1$ 是充要条件，因此阶为 m 的元恰好有 $\varphi(m)$ 个.

因此由循环群中每个元素的阶唯一且为 n 的因子，我们有 $\sum_{m|n}\varphi(m)=n$. ♣

14.证明 注意到：

$$y(xy)^3=yxyxyxy=(yx)^3y,$$

且 $(xy)^3=\varphi(xy)=\varphi(x)\varphi(y)=x^3y^3$，$(yx)^3=y^3x^3$，则代入有 $yx^3y^3=y^3x^3y$，即 $x^3y^2=y^2x^3$，这即意味着

$$\varphi(xy^2)=x^3(y^2)^3=x^3(y^3)^2=(y^3)^2x^3=\varphi(y^2x),$$

因此由 φ 为单同态，则 $xy^2=y^2x$，从而 $x^2y^2=xy^2x=y^2x^2$，又由 $x^3y^3=(xy)^3$，则 $y^2x^2=x^2y^2=yxyx$，从而 $xy=yx$，因此可知 G 为 Abel 群，即证. ♣

Remark. 手动 @ 想出这个做法的凯佬.

15.证明 设 G 中元素阶的全体为 $d_1,\cdots,d_t$，从而对任一阶 d，若有 a,b 阶均为 d，从而由 d 阶子群的唯一性，可知 $\langle a\rangle=\langle b\rangle$，则存在 $1\leq k<d$，$(k,d)=1$ 使得 $b=a^k$，从而 b 有 $\varphi(d)$ 个，这表明按元素的阶划分，阶为 d_i 的元素个数有 $\varphi(d_i)$ 个，因此我们成立

$$\sum_{i=1}^{t}\varphi(d_i)=n=\sum_{m|n}\varphi(m),$$

又 d_i 均为 n 的因子，从而 $d_1,\cdots,d_t$ 恰为 n 的因子全体. 进而可知存在 $d_i=n$，因此 G 存在 n 阶元，这即表明 G 为循环群，即证. ♣

16.证明 与上一题类似，我们可证明对任一元素 a，若其阶为 d，则阶为 d 的元素形如 a^k，其中 $1\leq k<d,(k,d)=1$(因为 d 阶子群唯一). 从而考虑所有可能的阶 $d_1,\cdots,d_t$，成立上一题一样的等式，从而 $d_1,\cdots,d_t$ 恰为 n 的因子全体，因此 G 为 n 阶群. ♣

Remark. 第 15 题的证法就已经足够强大到证明本题，这里只是浪费生命的重复一遍.

17. 没看懂这个题要我干什么。。。。

1.6 对称群与交错群

1.6.1 Notes

定理 1.6.1: S_n 中元素的刻画

S_n 中的任何元素 σ 都可表为 S_n 中一些不相交轮换之积，如果不计次序，则表法唯一.

Sketch: 存在性就不断对一个文字做 σ 复合，直到回到 a，从而形成一个轮换，由有限步即可完成. 而对唯一性，可知每个对换间都有对应，因此即可说明.

命题 1.6.1: S_p 的性质

若 p 为素数，求 S_p 中 p 阶元的个数.

解 若 σ 为 p 阶元，从而其一定为 p 轮换，因为 σ 可以表为一些不相交的轮换之积，从而若可被分解成至少两个轮换的乘积，则其阶为若干小于 p 的正整数的最小公倍数，一定不为 p，因此下面只需考虑不同的 p 轮换，易见这有 $p!/p = (p-1)!$ 个. ♠

下面的部分，我们考虑 S_n 共轭类的划分，内容部分选自《近世代数引论》.

设 $\sigma \in S_n$，将 σ 表示成没有公共元素的轮换之积，设长为 r 的轮换共有 λ_r 个 $(1 \leq r \leq n)$，则称置换 σ 的**型**为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$.

引理 1.6.1. *S_n 中任何两个轮换共轭当且仅当它们的长度一样.*

证明 一方面，对任意 $\sigma \in S_n$ 与 r 轮换 $(i_1 i_2 \cdots i_r)$，从而考虑 $\sigma(i_1 \cdots i_r)\sigma^{-1}$，对 $i \neq i_k$，则 $\sigma(i) \to i \to i \to \sigma(i)$，对 $\sigma(i_k) \to i_k \to i_{k+1} \to \sigma(i_{k+1})$，因此我们有

$$\sigma(i_1 i_2 \cdots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_k)),$$

因此共轭的对换有相同的长度.

另一方面，对任意 $(i_1 i_2 \cdots i_r)$ 与 $(j_1 j_2 \cdots j_r)$，考虑 $\sigma(i_k) = j_k (1 \leq k \leq r)$，其他有 $\sigma(i) = i$，因此由前面论述可知满足 $\sigma(i_1 \cdots i_r)\sigma^{-1} = (j_1 \cdots j_r)$，即证. ♣

定理 1.6.2: 共轭类的划分

S_n 中两个置换共轭，当且仅当它们有相同的型.

证明 一方面若对置换 $(ab\cdots c)\cdots(xy\cdots z)$，其共轭类为

$$\sigma(ab\cdots c)\cdots(xy\cdots z)\sigma^{-1} = \sigma(ab\cdots c)\sigma^{-1}\cdots\sigma(xy\cdots z)\sigma^{-1},$$

由引理可知每个轮换的长度共轭不变，因此共轭类有相同的型.

另一方面，若有相同的型，从而对 $(ab\cdots c)\cdots(xy\cdots z)$ 与 $(a'b'\cdots c')\cdots(x'y'\cdots z')$，其有

相同的型，则每个轮换都可以对应一个 σ_i 进行共轭，因此将这些置换作乘积，即可 σ 成立

$$\sigma(ab\cdots c)\cdots(xy\cdots z)\sigma^{-1}=\sigma(a'b'\cdots c')\cdots(x'y'\cdots z')\sigma^{-1},$$

这个证明是粗糙的，其本质在于由于轮换不交，则对应之间转换的 σ_i 是不交的，故可交换. ♣

定理 1.6.3: 共轭类的元素个数

S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换共有 $\dfrac{n!}{\prod\limits_{i=1}^{n}\lambda_i!\cdot i^{\lambda_i}}$ 个.

证明 考虑 $\{1,2,\cdots,n\}$ 的一个排列 $(p_1,\cdots,p_n)$，共有 $n!$ 种，按照从前往后分配 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$，则可知，对其他排列，与这种分配后得到的置换相同的全体满足 (1)λ_r 个 r 阶轮换可交换顺序，重复 $\lambda_r!$ 次，(2) 对给定 $(s_1\cdots s_r)$，$(s_k\cdots,s_{k+r-1})$ 本质一样，重复 r^{λ_r} 次，因此综上一样的置换重复 $\prod\limits_{i=1}^{n}\lambda_i!\cdot i^{\lambda_i}$ 次，即证. ♣

我们熟知 S_n 的正规子群是由若干共轭类拼成的，但更本质的，我们有

定理 1.6.4: S_n 的非平凡正规子群

对 $n\geq 5$，A_n 为 S_n 的唯一非平凡的正规子群.

证明 设 $\{1\}\neq N\lhd S_n$，则我们考虑

Case I. 若 $N\leq A_n$，从而由 $N\lhd S_n$ 可知 $N\lhd A_n$，但由 $n\geq 5$，A_n 为单群，因此 $N=A_n$.

Case II. 若 N 种包含奇置换，从而由 $N\cap A_n\lhd A_n$，因此可知 $N\cap A_n=A_n$ 或 $\{1\}$，若为前者，则由 $[S_n:A_n]=2$，从而 $[S_n:N]=1$，即有 $N=S_n$；若为后者，从而 N 中除了 1 均为奇置换，则由奇置换乘积为偶置换，从而任意 $\sigma,\tau\in S_n$，$\sigma\tau=1$，则可知 $N=\{1,\sigma\}$，但此时可知任意 $\tau\in S_n$，$\tau\sigma\tau^{-1}=\sigma$，因此 $\sigma\in C(S_n)=\{1\}$，矛盾！从而不存在这种情况.

因此综上我们有 $N=S_n$ 或 A_n 即证. ♣

1.6.2 Exercises From Z.Fh

1.证明 我们考虑 $\mathrm{Ad}:S_3\to \mathrm{Inn}S_3$，$\sigma\mapsto \mathrm{Ad}_\sigma$ 为一满同态，且由 $\mathrm{KerAd}=C(S_3)=\{1\}$，从而可知这也是单同态，故有 Ad 为 S_3 与 $\mathrm{Inn}S_3$ 间的同构，因此 $S_3\cong \mathrm{Inn}S_3$.

另一方面，注意到 $S_3=\{1,(12),(13),(123),(132)\}$，且任一 $f\in \mathrm{Aut}S_3$，f 将 2 阶元映为 2 阶元，3 阶元映为 3 阶元，且 $(123)=(23)(13)$，$(132)=(12)(13)$，从而 3 阶元的像由 2 阶元的像决定，因此 f 由 2 阶元的排列决定，从而

$$6=\mathrm{Inn}S_3\leq|\mathrm{Aut}S_3|\leq 6,$$

因此这表明 $\mathrm{Aut}S_3=\mathrm{Inn}S_3\cong S_3$，即证. ♣

2.证明 由 Notes 中的定理 1.6.2、1.6.3，我们有 S_5 的共轭类元素个数为：$[1^5]:1$，$[1^32^1]:\dfrac{5!}{2!3!}=10$，

$[1^12^2]:\dfrac{5!}{2^2\cdot 2!}=15$，$[1^23^1]:\dfrac{5!}{2!\cdot 3}=20$，$[2^13^1]:\dfrac{5!}{2\cdot 3}=20$，$[1^14^1]:\dfrac{5!}{1\cdot 4}=30$，$[5^1]:\dfrac{5!}{5}=24$.
由定理 1.6.4 可知非平凡正规子群只有 A_5. ♣

4. 引理 1.6.1

5.证明 一方面 $\pi_1=\langle\{(12),\cdots,(1n)\}\rangle\subseteq S_n$，另一方面，任意 $\sigma\in S_n$，其可分解成若干不交的 r 轮换乘积，对任一 r 轮换 $(i_1i_2\cdots i_r)=(i_1i_r)\cdots(i_1i_3)(i_1i_2)$，而不难注意到 $(i_1i_k)=(1i_1)(1i_k)(1i_1)$，因此 $(i_1i_2\cdots i_r)$ 可由 π_1 中的元素生成，进而 $\sigma\in\pi_1$，从而 $S_n=\pi_1$.

再考虑 $H_n=\langle\{(12),(12\cdots n)\}\rangle\subseteq S_n$，注意到 $(12)(12\cdots n)=(23\cdots n)$，从而 $(1n)=(n\cdots 21)(23\cdots n)=(12\cdots n)^{n-1}(2\cdots n)\in H_n$，进而 $(12\cdots n-1)=(1n)(12\cdots n)\in H_n$，因此不难归纳得到 $(12),\cdots,(1,n-1)$ 均在 H_n 中，因此由上面论述可知 $\pi_1\subseteq H_n$，进而 $H_n=S_n$.

而对于 A_n，熟知当 $n\geq 3$ 时，A_n 可由所有 3 轮换生成，而对于任意 $j\neq k$，$(1jk)=(12k)(12j)(12j)$，从而同理对互不相同的 i,j,k，有 $(ijk)=(jki)=(j1i)(j1k)(j1k)=(1ij)(1kj)(1kj)$，从而任一 3 轮换可由 $(123),\cdots,(12n)$ 生成，从而可知 $A_n=\langle\{(123),\cdots,(12n)\}\rangle$，即证. ♣

6.证明 我们仅证明 S_4 全体非平凡正规子群为 A_4 和 K_4，注意到任一正规子群都是由共轭类拼成的，且 S_4 的共轭类为 $[1^4]:1$，$[1^22^1]:6$，$[1^13^1]:8$，$[2^2]:3$，$[4^1]:6$.

设 $N\lhd S_4$ 且非平凡，则 $|N|\mid 24$，且 $N=2,3,4,6,8,12$，且 N 中一定含 (1) 即共轭类 $[1^4]$，从而上述共轭类只能拼出偶数 $1+3=4$，$1+3+8=12$，因此 $|N|$ 只能为 $4,12$，即 $K_4=[1^4]\cup[2^2]$，$A_4=[1^4]\cup[2^2]\cup[1^13^1]$，容易验证这均为正规子群，综上即证. ♣

7.证明 注意到当 $n\geq 5$，A_n 可由三轮换 (ijk) 生成，而 $(ijk)=(ij)(mn)(mn)(ik)$，即证. ♣

8.证明 由定理 1.6.2 可知 S_n 的共轭类为形如 $[1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}]$，其中 $\lambda_1\cdot 1+\lambda_2\cdot 2+\cdots+\lambda_n\cdot n=n$，即与 n 的划分之间有一一对应.

又考虑幂零矩阵的相似等价类代表元为 Jordan 标准型，其中特征值全为 0，从而 Jordan 块均为 $J_k(0)=\begin{pmatrix}0&1&&\\&\ddots&1&\\&&0\end{pmatrix}$，其中一共 n 阶，则可知对于每一组分划 $\lambda_1\cdot 1+\lambda_2\cdot 2+\cdots+\lambda_n\cdot n=n$ 唯一对应一个 Jordan 标准型

$$\mathrm{diag}\{\underbrace{J_1(0),\cdots,J_1(0)}_{\lambda_1},\cdots,\underbrace{J_k(0),\cdots,J_k(0)}_{\lambda_k},\cdots,\underbrace{J_n(0),\cdots,J_n(0)}_{\lambda_n}\},$$

综上我们可知 S_n 的共轭类与 n 的分划、幂零矩阵的相似等价类之间存在一一对应. ♣

9.证明 设 $\sigma\in S_n$ 且 $\sigma\neq 1$，从而存在指标 i 使得 $\sigma(i)=j\neq i$，从而考虑 $\tau=(jk)$，从而 $\tau\sigma(i)=\tau(j)=k$，$\sigma\tau(i)=\sigma(i)=j$，从而 $\sigma\tau\neq\tau\sigma$，即 $\sigma\notin C(S_n)$，从而即证. ♣

10.证明 考虑 $H<G$ 为 G 中所有偶置换构成的子群，不难验证 $H\lhd G$，从而有对奇置换 τ，有 $G=H\cup\tau H$，从而 $[G:H]=2$，即为指数为 2 的正规子群. ♣

11.证明 由 Caley 定理，$G\cong S$，$g\mapsto L_g$，其中 $S<S_{2n}$ 为一 $2n$ 阶置换群，又由 S 为偶数阶群，从而一定有二阶元 L_h，进而有 L_h 一定为若干不相交的对换之积，又任意 $g\in G$，$L_hg=hg\neq g$，因此每个元素均在对换中出现，也即为 n 个不相交的对换之积，从而为奇置换，因此由 T10 即

可得到 S 有指数为 2 的正规子群，即 G 有指数为 2 的正规子群，即证. ♣

12. 参考 GTM 163-*Permutation Groups* Thm 8.1 A.

1.6.3 S_n 的自同构群 $\mathrm{Aut}(S_n)$

注：以下材料基本上摘抄自知乎文章.

我们将要证明的是如下主定理：

定理 1.6.5

当 $n \geq 3$ 且 $n \neq 6$ 时，$\mathrm{Aut}S_n = \mathrm{Inn}S_n \cong S_n$.

我们先证明后者，这个同构是与 $n = 3$ 类似的：

引理 1.6.2. *当 $n \geq 3$ 时，$S_n \cong \mathrm{Inn}S_n$.*

证明 易知 $\mathrm{Ad} : S_n \to \mathrm{Inn}S_n$ 为满同态，且由 $\mathrm{Ker}\,\mathrm{Ad} = C(S_n) = \{1\}$，因此这也为单同态，进而为同构，因此我们证明了 $S_n \cong \mathrm{Inn}S_n$. ♣

下面我们证明 $\mathrm{Aut}S_n = \mathrm{Inn}S_n$ 的思路与 $n = 3$ 的情形类似，即去估计 $|\mathrm{Aut}S_n| \leq n!$，而我们熟知 S_n 可由 $(12), (13), \cdots, (1n)$ 生成，因此我们希望证明任一自同构 σ 可以将对换映为对换，首先我们还需要一些基本的引理：

引理 1.6.3. *设 $g \in S_n$ 阶为 m，则对 $\sigma \in \mathrm{Aut}S_n$，$\sigma(g)$ 阶也为 m.*

引理 1.6.4. *设 $\mathcal{N}$ 为 S_n 的一个共轭类，则 $\sigma(\mathcal{N})$ 也为一个共轭类.*

证明 注意到任意 $g, h \in \mathcal{N}$，即存在 $a \in S_n$ 使得 $aga^{-1} = h$，即两者共轭，从而有 $\sigma(a)\sigma(g)\sigma(a)^{-1} = \sigma(h)$，即 $\sigma(g)$ 与 $\sigma(h)$ 共轭，因此 $\sigma(\mathcal{N})$ 中的元素两两共轭.

另一方面，若有 $\sigma(g)$ 与 h 共轭，即 $b\sigma(g)b^{-1} = h$，则设 $b = \sigma(c)$，则 $h = \sigma(cgc^{-1}) \in \sigma(\mathcal{N})$，因此与 $\sigma(\mathcal{N})$ 共轭的元素全在其中，综合两方面我们即可断言，$\sigma(\mathcal{N})$ 为共轭类. ♣

定理 1.6.6: 自同构将对换映为对换

设 $\sigma \in \mathrm{Aut}S_n$ 且 $n \geq 3$，$n \neq 6$，则对任一对换 g，$\sigma(g)$ 也为对换.

证明 易见，所有对换为型 $\mathcal{H} = [1^{n-2}2^1]$，为一个共轭类，因此 $\sigma(\mathcal{H})$ 也为一个共轭类，又 $\mathcal{H}$ 中元素阶均为 2，则可知 $\mathcal{H}' = \sigma(\mathcal{H})$ 阶为 2，因此 $\mathcal{H}'$ 中元素为 m 个不相交 2 轮换的乘积，因此有其型为 $[1^{n-2m}2^m]$，因此我们有

$$\frac{n(n-1)}{2} = |\mathcal{H}| = |\mathcal{H}'| = \frac{n!}{(n-2m)! \cdot m! \cdot 2^m},$$

这里用到了定理 1.6.3 的计算公式. 化简即可得到

$$4 \cdot 6 \cdots (2m-2) \cdot 2m = (n-2m+1)(n-2m+2) \cdots (n-2),$$

注意到左侧为 $m-1$ 项，且公差为 2，右侧为 $2m-2$ 项且公差为 1，则不难有 $n-2m+1\leq 4$ 或 $n-2\geq 2m$，即可知 $0\leq n-2m\leq 3$，因此若 $n=2m$，则有 $m=(2m-3)!!$，只有 $m=3$，此时 $n=6$ 舍弃 (这也是排除 6 的原因)；而同理对 $n-2m=1,2,3$，类似可导出 m 无解.

综上 m 仅能取平凡解 1，这也意味着对任一对换 g，$\sigma(g)$ 也为对换. ♣

引理 1.6.5. 设 $n\geq 3$ 且 $n\neq 6$，对 S_n 的一组生成元 $(12),(13),\cdots,(1n)$，我们有 $a,b_2,\cdots,b_n$ 为 $1,2,\cdots,n$ 的一个排列，且满足

$$\sigma:(12)\mapsto(ab_2),(13)\mapsto(ab_3),\cdots,(1n)\mapsto(ab_n).$$

证明 一方面，我们由定理 1.6.8，可不妨设 $\sigma:(1k)\mapsto(a_kb_k)$，从而由 $(12)(13)=(132)$ 为 3 轮换，则 $(a_2b_2)(a_3b_3)$ 也为 3 轮换，这是因为若 a_2,b_2,a_3,b_3 两两不同，则其阶为 2，不会为 3，因此可知 (a_ib_i) 与 (a_jb_j) 四者中恰有 3 个元素.

另一方面，由 $(a_2,b_2),\cdots,(a_nb_n)$ 能生成 S_n，因此其中元素包含 $1,2,\cdots,n$，因此不难得到其形式如题所述. ♣

综上我们可知 $\mathrm{Aut}S_n$ 完全由 $\{a,b_2,\cdots,b_n\}$ 决定，因此 $|\mathrm{Aut}(S_n)|\leq n!$，综上可知 $\mathrm{Aut}S_n=\mathrm{Inn}S_n$，即证定理 1.6.5.

定理 1.6.7: S_6 的自同构群

对于 $n=6$ 的情形，我们有 $[\mathrm{Aut}S_6:\mathrm{Inn}S_6]=2$.

更详细的内容可参考论文.

1.7 群的扩张与 John—Hölder 定理

1.8 可解群和幂零群

1.8.1 Notes

可解群

1.9 群在集合上的作用

1.9.1 Notes

定义 1.9.1: 群在集合上的作用

设 G 是一个群，X 是一个非空集合. 若映射

$$f : G \times X \to X, \quad (g, x) \mapsto f(g, x)$$

满足对任何 $x \in X$，$g_1, g_2 \in G$ 都有

$$f(e, x) = x, \quad f(g_1 g_2, x) = f(g_1, f(g_2, x)),$$

则称 f 决定了 G 在 X 上的一个**作用**. 通常，我们将 $f(g, x)$ 简记为 $g(x)$ 或 gx.

定理 1.9.1: 为什么要研究作用？

群 G 在集合 X 上的作用的全体与 G 到 S_X 的同态的全体存在一一对应.

对于作用，我们有如下分类：

定义 1.9.2: 作用的分类

设群 G 作用在集合 X 上，则

- 若对任意 $x, y \in X$，存在 $g \in G$ 使得 $gx = y$，则称 G 在 X 上的作用**可递**，这时称 X 为 G 的**齐性空间**；
- 若对 $g \in G$，由 $gx = x$，任意 $x \in X$ 可以推出 $g = e$，则称 G 在 X 上的作用**有效**；
- 若对任意 $g \in G, x \in X$ 都有 $gx = x$，则称 G 在 X 上的作用**平凡**.

Remark. 注意到，若 G 在 X 上的作用有效，即满足 g 对应的 S_X 中元素是 id 则 $g = e$，也即考虑 $\pi : G \to S_X$，则 $\mathrm{Ker}\pi = e$，即 π 为单射 (注意！不是 $g(\cdot)$ 在 X 上是单射)，同理另一方面 π 是单射也蕴含作用是可递的.

为了研究作用，往往集合 X 过于庞大不好研究清楚，类比研究不变子空间的思想，我们也希望能够找到 X 的“不变子集合”，使得我的作用可以限制在这样的子集合上，那么如果在子集合上的作用研究清楚了，自然整体就不存在问题了.

定义 1.9.3: 轨道

设群 G 作用在集合 X 上，$x \in X$. 称 X 的子集 $O_x = \{gx | g \in G\}$ 为 x 的**轨道**.

命题 1.9.1: 轨道的性质

(1)$x, y \in X$，在 $O_x \bigcap O_y = \varnothing$ 或者 $O_x = O_y$，即可以将轨道看作 X 的一个划分或者等价类；

(2)G 在 O_x 上的作用可递.G 在 X 上的作用可递当且仅当 X 中仅有一个轨道.

证明 (1) 设 $gx \in O_y$，则存在 $h \in G$ 使得 $gx = hy$，从而有任意 $sx \in O_x$，有 $sx = sg^{-1}hy \in O_y$，即 $O_x \subseteq O_y$，同理另一边也成立，综上有 $O_x = O_y$，反之则交集为空，即证.

(2) 这个证明是 trivial 的，略去. ♣

那么下面我们就希望去研究群在单个轨道上的作用，与原来作用不同，是在两个都在变化的里面研究结构，也与原来 $G \to S_X$ 中固定 g 研究 X 上的自映射也不同，轨道的很大一个好处就是它可以看成 $G \times \{x\}$ “生成的”，因此这个视角下，我们是固定 x 来看的 (这里就产生了对偶的观点！)，因此对比映射 π，我们也希望研究 $G \to O_x$ 上的映射 φ_x.

定义 1.9.4: 对偶观点看问题

固定 $x \in X$，考虑 G 在 O_x 上的作用，有如下映射

$$\varphi_x : G \to O_x, \quad \varphi_x(g) = gx.$$

显然 φ_x 是满射，从而我们自然考虑 O_x 中元素的原像，而为了研究原像，本质上可以转化为研究 x 的原像：

定义 1.9.5: 迷向子群

记 F_x 为 x 的原像，即

$$F_x = \{g \in G | gx = x\}.$$

注意到 F_x 是 G 的子群，称为 x 的**迷向子群**.

Remark. 为什么这里叫“迷向”子群捏？事实上，我们把集合 X 看成一个研究对象，对群里的每个元素，作用一下，相当于让 X 中一个点跑到另一个点，且这些点都落在初始点的“轨道”上！如果作用不来自迷向子群，那么就可以**沿着轨道这个方向一直往下走**，但是如果不小心作用来自迷向子群，就只能在原地打转，出不去了，也就“迷失了方向”.

命题 1.9.2: 轨道上不同元素迷向子群的关系

设 $y = gx \in O_x$，则 $F_y = gF_xg^{-1}$.

证明 注意到

$$F_y = \{h \in G | hy = y\} = \{h \in G | hgx = gx\} = \{h \in G | g^{-1}hgx = x\},$$

从而即有 $F_y = gF_xg^{-1}$. ♣

我们回过头来再看看 φ_x，我们研究清楚 x 的原像后，再来看一般的元素 gx，则由于

$$\varphi_x^{-1}(gx) = \{h \in G | hx = gx\} = \{h \in G | g^{-1}hx = x\} = gF_x,$$

从而我们会发现，对于轨道中不同的元素 gx，其原像事实上就是迷向子群 F_x 的左陪集 gF_x，从而如果我们把 G 中元素关于 F_x “捏起来”，即得到左商集 $G \setminus F_x$，因此有一个一一对应 $\varphi : G \setminus F_x \to O_x$(注意！这里不存在商群，$X$ 也不为群，从而这里仅是对应，不是同构).

因此我们研究两个集合间的关系以及映射 φ，我们发现对群 G 中的元素，作用在两个集合上效果是 “等价” 的，设对元素 gF_x 与对应的 gx，如果考虑作用 h，则有：

$$\varphi(h(gF_x)) = \varphi(hgF_x) = hgx = h(gx) = h\varphi(gF_x),$$

也即有如下交换图成立

$$\begin{array}{ccc} G \setminus F_x & \xrightarrow{\varphi} & O_x \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h} \\ G \setminus F_x & \xrightarrow{\varphi} & O_x \end{array}$$

据此，我们发现研究轨道上的作用可以进一步转化为研究与轨道等价的商集上的作用，从而我们可以抽象出下面这个概念

定义 1.9.6: 等价

设群 G 作用在集合 X 与 X' 上，若有 X 到 X' 的一一对应 φ 使得

$$g(\varphi(x)) = \varphi(g(x)), \quad \forall g \in G, x \in X,$$

则称 G 在 X 与 X' 上的作用**等价**.

进而我们就不难得到如下定理：

定理 1.9.2

设 $G \curvearrowright X$，则对任意 $x \in X$，有 G 在 O_x 上的作用与 G 在 G/F_x 上的左平移作用等价.

推论 1.9.1. $|O_x| = |G/F_x| = [G : F_x]$，进而 $|O_x| \mid |G|$.

1.9.2 Exercises From Z.Fh

1.解 考虑 S_9 在 $X = \{1, 1, 1, 2, 2, 2, 2, 3, 3\}$ 上的作用，从而有三个轨道，元素个数分别为 $3, 4, 2$，从而可能的排列数为 $\dfrac{9!}{3!4!2!}$. ♠

2.证明 设 $H < A_5$，且 $[A_5 : H] = k \in \{2, 3, 4\}$，因此考虑 $A_5 \curvearrowright A_5/H$ 即一个左平移作用，这诱导出了一个 $A_5 \to S_k$ 的一个同态 f，因此由 $\ker f \lhd A_5$，且 A_5 为单群，则若 $\ker f = A_5$，则任意

$g\in A_5$，有 $gH=H$(对应的置换均为单位置换)，即 $H=A_5$，指数为 1，矛盾；若 $\ker f=\{e\}$，从而 f 为单射，即 $A_5\cong \mathrm{Im}f<S_k$，则 $60=|A_5|\leq |S_k|\leq 4!=24$，矛盾！综上，不存在指数为 2，3，4 的子群. ♣

3.证明 我们考虑 $H\times K\curvearrowright G$，其中 $(h,k)g=hkg$，从而易见 $HK=O_e$，则有 $|HK|=|O_e|=|H\times K/F_e|$，又 $F_e=\{(h,k)\in H\times K|(h,k)e=hke=e\}=\{(h,k)|hk=e\}$，一方面由 $hk=e$，有 $h\in H\cap K$，另一方面任意 $h\in H\cap K$，存在唯一 k 使得 $hk=e$，因此 $|F_e|=|H\cap K|$，因此我们即有 $|HK|=|H\times K|/|F_e|=|H|\cdot|K|/|H\cap K|$，即证. ♣

7.证明 设 $\varphi_1,\varphi_2\in \mathrm{GL}(E)$，从而有 $(\varphi_1\varphi_2)(xy)=\varphi_1(\varphi_2(x)\varphi_2(y))=(\varphi_1\varphi_2)(x)(\varphi_1\varphi_2)(y)$，又 $\varphi_2^{-1}\varphi_1^{-1}$ 为 $\varphi_1\varphi_2$ 的逆，从而可知 $\varphi_1\varphi_2\in \mathrm{GL}(E)$，另一方面不难验证其满足结合律，且幺元为恒等映射，逆元即考虑表示矩阵的逆即可，因此 $\mathrm{Aut}(E)$ 为群.

注：这里题目有误，应当加上 $f(x)$ 无重根的限制条件.

由 φ 为线性映射，对任意 $f(x)=a_nx^n+\cdots+a_0\in\mathbb{Q}[x]$，从而 $\varphi(f(x))=\varphi(a_nx^n+\cdots+a_0)=a_n\varphi(x^n)+\cdots+a_0$，又由 $\varphi(xy)=\varphi(x)\varphi(y)$，因此 $\varphi(x^k)=(\varphi(x))^k$，因此有 $\varphi(f(x))=a_n(\varphi(x))^n+a_0=f(\varphi(x))$，从而若 $r\in E$ 为 $f(x)$ 的根，从而 $\varphi(r)$ 也为其根，从而若 $f(x)=f_1(x)f_2(x)$ 可约，则若 x_1 为 $f_1(x)$ 的根，由作用可递，从而存在 φ 使得 $\varphi(x_1)=x_2$ 为 $f_2(x)$ 的根，而 $\varphi(x_1)$ 为 $f_1(x)$ 的根，因此 $f(x)$ 有重根，矛盾，因此 $f(x)$ 不可约，即证.

注：凯佬给我讲的，*mod*，代数的神中神. ♣

8.解 显然 $\boldsymbol{I}_2\circ z=z$，且不难剥蒜验证 $g_1g_2\circ z=g_1\circ(g_2\circ z)$，由此可知这决定了一个 $\mathrm{SL}(2,\mathbb{R})\curvearrowright\mathbb{H}$，下面证明这个作用在 $\mathbb{H}$ 上是可递的，即 $\mathbb{H}$ 是作用的齐性空间，我们先证明任意 $z=x+y\sqrt{-1}$，存在 g 使得 $g\circ\sqrt{-1}=z$，不难发现有 $g=\begin{pmatrix}\frac{x}{\sqrt{y}} & -\sqrt{y}\\ \frac{1}{\sqrt{y}} & 0\end{pmatrix}$，即满足，从而 $O_{\sqrt{-1}}=\mathbb{H}$，进而可知 $\mathbb{H}$ 是作用的齐性空间，从而在 $\mathbb{H}$ 上作用可递.

另一方面，若存在 g 使得 $g\circ z=z$，对任意 $z\in\mathbb{H}$ 均成立，则可知有 $az+b=z(cz+d)$，若这方程恒成立，则 $c=b=0$，且 $a=d$，又 $\det(g)=ad=1$，且 $d>0$，则 $g=\boldsymbol{I}_2$，从而说明作用在 $\mathbb{H}$ 上是有效的.

我们再考虑 $F_{\sqrt{-1}}=\{g\in\mathrm{SL}(2,\mathbb{R})|g\circ\sqrt{-1}=\sqrt{-1}\}$，即有 $(a-d)\sqrt{-1}=-b-c$，从而 $a=d$，$b=-c$，又 $ad-bc=a^2+b^2=1$，因此其迷向子群为全体 $\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}$ 构成的集合，其中 $\theta\in[0,2\pi]$. ♠

9.证明 由 $[G:H]\leq 4$，从而显然 $m=[G:H]\geq 2$，若 $m=2$，则熟知 $H\lhd G$，与单群矛盾；

若 $m=4$，从而考虑 $G\to S_{G/H}\cong S_4$ 的同态，则由 $\mathrm{Ker}f\lhd G$，且 G 为单群，从而 $\mathrm{Ker}f=\{e\}$，因此为单同态，从而 $G\cong\mathrm{Im}f$，即 G 同构于 S_4 的子群. 由 $|S_4|=24$，从而 $|G|=2,3,4,6,8,12$，而 12 阶群不为单群，8 阶群为 $p-$ 群有非平凡的中心元素进而不为单群，从而 $|G|\neq 8,12$. 而若 $|G|=6$，则由 $4=[G:H]\mid|G|=6$ 矛盾. 对 $|G|=4$，则 $G\cong K_4$ 或 $\mathbb{Z}_4$，这两者均不为单群，因

此 $|G| \leq 3$.

若 $m = 3$，则 G 同构于 S_3 的子群，而 $G \neq S_3$，因为 S_3 不为单群，从而 $G < S_3$，即有 $|G| \leq 3$，综上当 $[G : H] \leq 4$ 时，成立 $|G| \leq 3$，即证. ♣

10.证明 考虑 $G \curvearrowright G/H$ 即左平移作用，诱导出 $G \to S_n$ 的同态 f，从而 $\ker f \lhd G$，且任意 $g \in \ker f$，有 $gH = H$，从而 $g \in H$，因此 $N := \ker f \subseteq H$，且为 G 的正规子群，另一方面 G/N 同构于 S_n 的子群，因此 $|G/N| \leq |S_n| = n!$，即 $[G : N] \leq n!$，即证. ♣

11.证明 考虑 $G \curvearrowright G/H$ 即左平移作用诱导出的 $G \to S_p$ 的同态 f，从而 $\ker f \lhd G$，且 $G/\ker f \cong S < S_p$，这表明 $|G/\ker f| \mid |S_p| = p!$，而 $|G/\ker f| \mid |G|$，从而最小素因子即为 p，这表明 $|G/\ker f| = p = [G : H]$，而在上一问中我们已经得到 $\ker f < H$，因此 $H = \ker f \lhd G$，综上我们完成了证明. ♣

12.证明 我们设 $X = \{H | H < G\}$，则考虑 $G \curvearrowright X$ 为伴随作用，从而 H 的共轭子群的个数即为 $|O_H| = \{gHg^{-1} | g \in G\} = |G/F_H|$，而 $F_H = \{g \in G | gHg^{-1} = H\} = N_G(H)$，从而 $|O_H| = [G : N_G(H)]$，即证. ♣

13.证明 设 H 的共轭子群的并为 $\sigma = \cup gHg^{-1}$，下面估计 σ 中的元素个数，由 12 题可知，共轭子群的个数为 $[G : N_G(H)]$，又对任意 g，gHg^{-1} 均有 $|H|$ 个元素，且考虑到幺元在每个共轭子群中都会出现一次，所以我们考虑更细致的估计为

$$|\sigma| \leq (|H| - 1)[G : N_G(H)] + 1 = |H|[G : N_G(H)] - [G : N_G(H)] + 1,$$

又注意到

$$|H|[G : N_G(H)] - [G : N_G(H)] + 1 = \frac{|G||H|}{|N_G(H)|} - \frac{|G|}{|N_G(H)|} + 1 = |G|\left(\frac{|H| - 1}{|N_G(H)|}\right) + 1,$$

且我们结合 $H \lhd N_G(H) < G$，不难得到 $|H| \leq |N_G(H)| \leq |G|$，进而我们有估计

$$|\sigma| \leq |G| \cdot \frac{|N_G(H)| - 1}{|N_G(H)|} + 1 \leq |G| \cdot \frac{|G| - 1}{|G|} + 1 = |G|.$$

从而若有 $\sigma = G$，则可知上述不等式均取等号，意味着 $H = N_G(H) = G$，这与 H 为 G 的真子群矛盾！即证. ♣

14.证明 这里的同态应该理解为左平移/右平移作用所对应的那个同态.

考虑 $G \curvearrowright G/H$ 即左平移作用，诱导出 $G \to S_{G/H}$ 的同态 f，从而 $\ker f = \{g \in G | gaH = aH \ , \forall a \in G\}$，因此我们有任意 $a \in G$，$a^{-1}ga \in H$，也即 $g \in \bigcap_{a \in G} aHa^{-1}$，从而 $\ker f \subseteq \bigcap_{a \in G} aHa^{-1} := N$，另一方面任意 $g \in N$，显然有 $gaH = aH$，对任意 $a \in G$，从而 $N \subseteq \ker f$，综上即证 H 的所有共轭子群之交为 $G \to S_{G/H}$ 的同态核. ♣

15.证明 显然 G 为一个群，且 $e = \mathrm{diag}\{I, I\}$，因此有 $(e, x) = x$，且 $(\mathrm{diag}(g_1, h_1), x) = g_1 g_2 x h_1^{-1} h_2^{-1} = (\mathrm{diag}(g_1, h_1), (\mathrm{diag}(g_2, h_2), x))$，从而可知 π 为群作用.

轨道分解不会捏。。。。 ♣

16.证明 考虑 $G=\mathrm{GL}(n,\mathbb{R})\times\mathrm{GL}(n,\mathbb{R})$，以及 $G\curvearrowright M_n(\mathbb{R})$，其中作用具体为 $(P,Q)M=PMQ$，不难验证这是一个群作用，且注意到任意 $\mathrm{rank}(M)=r$，则存在 (P,Q) 使得 $PMQ=\boldsymbol{I}_r$，因此所有的轨道即为 $O_{\boldsymbol{I}_r}$，其中 $0\leq r\leq n$. ♣

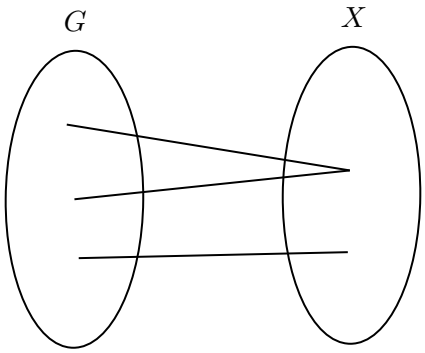
17.解 一方面，$(e\cdot f)(x)=f(ex)=f(x)$，从而有 $e\cdot f=f$，另一方面，$g_1g_2\cdot f(x)=f(g_1g_2x)=(g_1\cdot(g_2\cdot f))(x)$，从而可知这为一个群作用. ♠

18.证明 考虑 $\varphi:G\to G$，$x\mapsto x^{-1}$，从而有对右平移作用 g，有 $g(\varphi(x))=\varphi(x)g^{-1}=x^{-1}g^{-1}$，而 $\varphi(g(x))=\varphi(gx)=x^{-1}g^{-1}$，从而 $\varphi g=g\varphi$，因此即左平移作用等价于右平移作用. ♣

20.证明 凯佬锐评：这不经典算两次嘛. 我们不难注意到如下等式

$$\sum_{g\in G}F(g)=\sum_{x\in X}F_x,$$

这个观察事实上是平凡的，这里采用凯佬的观察，考虑一个二部图 (G,X)，把每个 G 和 X 中元素视作一个点，且两点连边当且仅当 $gx=x$，因此这就构做了一个图



因此我们事实上有两个表达式均为这个图的边数，因此我们进一步结合轨道公式，有

$$\sum_{x\in X}F_x=\sum_{x\in X}\frac{|G|}{|O_x|}=\sum_{O_x}\sum_{y\in O_x}\frac{|G|}{|O_x|}=\sum_{O_x}|G|=t|G|,$$

综上我们完成了证明，核心就是那个算两次的观察. ♣

19.证明 又是凯佬教我的一题，不动点个数计算难度感觉有点大，这里就直接证明后者的结论.

我们先证明 φ_1,φ_2 是 $\mathbb{Z}_2\curvearrowright X$ 上的作用，这事实上即证 $\varphi_1^2=\varphi_2^2=\mathrm{id}$，一通非本质的剥蒜即可证明. 从而两个映射为群作用，下面我们证明当 $p=4k+1$ 时 $x^2+y^2=p$ 有解，又 x,y 中恰有一个为偶数，因此不妨考虑 $x^2+4y^2=p$，进而易见其解即 φ_1 在 X 上的不动点.

我们先考虑 φ_2 的不动点，易见 $F(\overline{0})=|X|$，下面考虑 $F(\overline{1})$，即 $\varphi_2(x,y,z)=(x,y,z)$，不难求得这即 $x=y$，进而代入有 $x^2+4xz=p$，则 $x\mid p$，显然 $x\neq p$，从而 $x=y=1$，$z=k$，从而 $F(\overline{1})=|\{(1,1,k)\}|=1$，由 Bureside 引理，从而我们有 $|X|+1=t|\mathbb{Z}_2|=2t$，因此 $|X|$ 为奇数，同理我们类似考虑 φ_1 其对应的不动点个数为 $F'(\overline{1})$，则也不难看见 $F'(\overline{0})=|X|$，从而有 Bureside 引理，$F'(\overline{1})+|X|=2t'$，因此 $F'(\overline{1})$ 为奇数，进而 $F'(\overline{1})\geq 1$，也即 φ_1 在 X 上有非平凡不动点，也即 $x^2+4y^2=p$ 有解，即证. ♣

1.10 Sylow 定理

1.10.1 Notes

为了研究群的结构，一个很基本的问题就是寻找群的子群，Lagrange 定理告诉我们，如果 $H < G$，则有 $|H|$ 为 $|G|$ 的因子，借助这个定理，我们很自然的会想，是否对 $|G|$ 的任何一个因子，都能找到对应的子群呢？很遗憾，这么强的结论是不正确的，因为有如下反例：

例 1.10.1 (Lagrange 定理的逆命题不一定成立)**.**

一方面我们考虑 5 元交错群 A_5，则可知 $|A_5| = \dfrac{5!}{2} = 60$，则若其有 30 阶子群 H，从而 $[G : H] = 2$，即 H 的左陪集仅有 $eH = H$ 和 aH，同理右陪集仅有 $He = H$ 和 Ha，而陪集是对群中元素的分划，从而 $aH = Ha$，即 H 为正规子群.

又熟知 $n \geq 5$，有 A_n 为单群，既没有非平凡的正规子群，则 A_5 没有正规子群，更不可能有 30 阶子群，从而这就是一个反例.

Remark. 这个反例用到的核心结论就是指数为 2 的子群一定是正规的.

尽管对一般的因子命题不一定成立，但是数学的世界总是黑暗与曙光并存，Cauchy 指出若因子为素数，那么对应的子群是存在的，我们下面证明这一断言：

定理 1.10.1: Cauchy 定理

设素数 p 是 $|G|$ 的因子，则 G 中存在 p 阶元，则自然其生成的循环子群阶即为 p.

证明 事实上，我们可以证明更强的结论，不仅有 p 阶元，而且 p 阶元的个数可以写成

$$(p-1)(pt+1), \quad t \geq 0.$$

为了找到 p 阶元，不妨先扩大研究范围 (拟对象逼近——冯跃峰)，我们考虑连续 p 个元素相乘为幺元的这些数组，看看其上有没有什么好的性质，定义：

$$X = \{(a_1, \cdots, a_p) | a_i \in G, a_1 \cdots a_p = e\}.$$

从而我们容易观察到，当我们任意从 G 中选取 $p-1$ 个元素填进该数组的 $p-1$ 个位置时，最后一个元素就是这些元素乘积的逆元，从而唯一确定，因此可知 $|X| = |G|^{p-1}$，自然 $p||X|$.

下面我们考察 p 阶循环群 $\langle\sigma\rangle$ 在 X 上的作用，其中 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & p \\ 2 & 3 & \cdots & 1 \end{pmatrix}$，则我们断言，对任意 $\mathcal{A} = (a_1, \cdots, a_p) \in X$，$\mathcal{A}$ 的轨道恰为 $\{\mathcal{A}, \sigma\mathcal{A}, \cdots, \sigma^{p-1}\mathcal{A}\}$ 当且仅当 $\mathcal{A}$ 中没有两个元素相等.

注意到若 $\sigma^k\mathcal{A} = \sigma^l\mathcal{A}$，即存在正整数 i 使得 $a_j = a_{i+j}$(任意 $1 \leq j \leq p$，下标模 p 理解)，易见 $\{i, i+j, i+2j, \cdots, i+(p-1)j\}$ 恰好构成模 p 的完全剩余系，则此时所有元素都相等，即断言成立.

我们记 σ 在 X 上作用的不动点全体为 X_0，则不动点全部形如 $(a,a,\cdots,a)$，且其余的轨道 $O_{\mathcal{A}}$ 均恰有 p 个元素，故结合 $p||X|$，故有 $p||X_0|$，而显然 $(e,e\cdots,e)\in X_0$，故 $|X_0|=np(n\geq 1)$，则有 p 阶元的个数为 $np-1>0$，从而存在 p 阶元.

更进一步，我们注意到若 g 为 p 阶元，则 $g^k(1\leq k\leq p-1)$ 均为 p 阶元，从而 $(p-1)||X_0\backslash\{e\}|$，即 $(p-1)|np-1$，则显然此时 p 阶元的个数可以表示成 $(p-1)(pt+1)$，即证. ♣

Remark. 上述证明材料来自知乎. 证明的关键在于考虑在集合 X 上的作用，从而根据作用**将 X 划分成不交轨道与不动点集合的并**，载结合素数 p 的特性可知轨道元素个数的特殊性，进而倒逼出不动点集合的特殊性.

推论 1.10.1: 上述结果的漂亮推论

若群 G 的阶为 pq，且满足 $p<q$，p、q 均为素数，$p\nmid q-1$，则 G 为循环群.

证明 反证法，若 G 不为循环群，即一定没有阶为 pq 的元素，从而任意元素的阶为 p 或 q，而由前述定理结果可知，p 阶元的个数可以表示为 $(p-1)(pt+1)$，q 阶元的个数可以表示为 $(q-1)(qs+1)$，从而可知 G 的阶可写为 $(p-1)(pt+1)+(q-1)(qs+1)+1=pq$.

而 $(q-1)(qs+1)\leq pq-1<q^2-1$，从而 $s<1$，即 $s=0$，从而即有 $(p-1)(pt+1)=(p-1)q$，则有 $pt=q-1$，即 $p|q-1$，矛盾！故 G 为循环群，即证. ♣

解决了素数因子情形的逆命题，我们自然会去探索 p 的幂次是否依然满足？更一般地，如果 $|G|=p^lm$，其中 $(p,m)=1$，那么对于因子 $p^k(1\leq k\leq l)$，是否存在 G 的子群使得其阶恰好为 p^k？为了回答这一问题，我们先从 Cauchy 定理的证明过程中分离出一些有价值的一般结果.

定义 1.10.1: p-群

设 p 是一个素数，若群 G 的阶为 $p^k(k\in\mathbb{N})$，则称 G 是一个***p*-群**.

这里将原证明中的 p 阶循环群进行了推广，那么其中不动点的结论也可以推广：

定理 1.10.2: 群作用的不动点

设 $p-$ 群 G 作用在集合 X 上，$|X|=n$. 记 G 作用的不动点集为

$$X_0=\{x\in X|gx=x,\quad \forall g\in G\},$$

且记 $t=|X_0|$，则有 $t\equiv n(\mathrm{mod}\ p)$；特别地，当 $(n,p)=1$ 时，$t\geq 1$，即 G 在 X 上的作用存在不动点.

证明 设 X 在群 G 的作用下的轨道分解为

$$X=X_0\bigcup O_1\bigcup\cdots\bigcup O_k.$$

其中 $|O_i|>1(1\leq i\leq k)$，于是由 $|O_i|=|O_x|=[G:F_x]=|G|/|F_x|=p^s(0<s<v_p(|G|))$，即 $p||O_i|$，故又 $|X|=|X_0|+\sum_{i=1}^{k}|O_i|$，知 $p|(|X|-|X_0|)$，从而 $t\equiv n(\mathrm{mod}\ p)$，即证. ♣

考虑 G 上的特殊作用，我们可以得到下面这个结论：

推论 1.10.2: $p-$ 群的中心也为 $p-$ 群

设 G 是一个 $p-$ 群，则 G 的中心也是一个 $p-$ 群. 由此可以得到 p^2 阶群一定是 Abel 群.

证明 我们考虑 G 在自身上的伴随作用 $\mathrm{Ad}_g:a\mapsto gag^{-1}$，从而可知作用的不动点恰好为 G 的中心 $C(G)$，从而 $p||C(G)|$，又 $C(G)$ 为子群，从而 $|C(G)|=p^l$，即为 $p-$ 群.

下面考虑 p^2 阶群，从而若存在元素阶为 p^2，则可知其为循环群，即证；若不然，则可知每个非幺元的元素阶均为 p，进一步由 $C(G)$ 中有 p 或 p^2 个元素，从而取 $a\in C(G)$ 且 $a\neq e$，则考虑 $b\in G\setminus\langle a\rangle$，从而 $ab=ba$，下证 $G=\langle a,b\rangle=\{a^mb^n|1\leq m\leq p,1\leq n\leq p\}$.

一方面显然 $\langle a,b\rangle\subseteq G$，而另一方面，任意 $(m,n)\neq(k,l)$，若 $a^mb^n=a^kb^l$，则可知 $a^i=b^j$，从而 $b\in\langle a\rangle$，矛盾！故可知 $|\langle a,b\rangle|=p^2$，即 $G=\langle a,b\rangle$，从而显然 G 为 Abel 群，即证. ♣

在有了上述铺垫之后，我们终于可以回到主线剧情上来，探讨 p^l 阶子群的存在性，这个工作主要由挪威数学家 Sylow 完成，可表述为如下定理：

定理 1.10.3: Sylow 第一定理

设 $|G|=p^lm$ 且 $(p,m)=1$，其中 p 为素数，$l\geq 1$，$(p,m)=1$，则对任意 $k\leq l$，G 中存在 p^k 阶子群.

证明 由 Cauchy 定理可知 G 一定有 p 阶子群，从而我们下面用数学归纳法证明命题，假设 G 中已经找到 $p^n(0<n<l)$ 阶子群 H，下面去构建 p^{n+1} 阶子群，那么自然地，我希望在 H 的基础上进行构造，那么怎么样才会使得在 p^n 上再来个 p 呢？自然想到如果有个**商集**为 $[*:H]=|*|/|H|$ 也能被 p 整除，那么自然就可以找到了！

进一步联想，什么样的集合的阶会有因子 p，这让我们想到了群在集合上作用的不动点集. 从而考虑子群 H 在商集 $G\setminus H$ 上的左平移作用，并记其不动点集为 X_0，从而由 $n<l$ 可知 $p||X|$，从而 $p||X_0|$. 而事实上，我们注意到，$X_0=\{gH|h(gH)=gH,\forall h\in H\}$，也即 $g^{-1}hg\in H$ 对任意 $h\in H$，从而 $g\in N_G(H)$ 即 H 的正规化子. 反之对正规化子 g 也有 $gH\in X_0$，从而 $X_0=N_G(H)\setminus H$.

又显然 $H\lhd N_G(H)$，从而 $N_G(H)\setminus H$ 为商群，且其阶有因子 p，从而由 Cauchy 定理，可知商群 $N_G(H)\setminus H$ 有 p 阶子群，从而倒推过去，借助群到商群的自然同态，则有 $N_G(H)$ 中有 p^{n+1} 阶子群，综上我们完成了证明. ♣

Remark. 这个证明的想法比较朴素，主要是借助 Cauchy 定理，构造更大的子群，从而可以归纳下去，此外还有一种证法，与 Cauchy 定理最初的想法比较类似，都是通过构造一个拟对象，

然后考虑特殊群在集合上的作用：

证明 为了找到 $p^k(k \leq l)$ 阶的子群，我在所有元素个数为 p^k 的子集里搜索，从而定义 $X = \{A \subseteq X||A| = p^k\}$，我们自然考虑群 G 在 X 上的作用，$G \times X \to X, gA = \{ga|a \in A\}$.(其中这个定义是良好的，因为 $|gA| = |A|$，从而仍在 X 中)

进而我们考虑 A 的迷向子群 $F_A = \{g \in G|gA = A\}$，从而其是群，故再考虑 F_A 在集合 A 上的作用：$F_A \times A \to A, (g, a) \mapsto ga$，从而显然 $a \in A$ 在此作用下的轨道为 F_Aa，故 A 可划分成若干不交轨道的并，即 $A = \bigcup_{i=1}^{n} F_Aa_i$，从而可知 $|F_A||A| = p^k$，故 $F_A(A \in X)$ 的阶均为 p 的幂次，从而假设若均小于 p^k，则考虑第一次作用下 A 的轨道 O_A，则其是 X 的一个划分，且 $|O_A| = [G : F_A] = |G|/|F_A|$.

故有

$$\binom{p^lm}{p^k} = |X| = \sum_{i=1}^{m} |O_{A_i}| = \sum_{i=1}^{m} \frac{|G|}{|F_{A_i}|} \Rightarrow p^{l-k+1} \left| \binom{p^lm}{p^k} \right.$$

而事实上，由 Kummer 定理，

$$v_p\left(\binom{p^lm}{p^k}\right) = \#\left\{(\cdots m'\underbrace{0\cdots0}_{l个})_p - (1\underbrace{0\cdots0}_{k个})_p\text{的借位次数}\right\} = l - k,$$

其中 m' 为 m 在 p 进制下的末尾数字，则可知 $|X|$ 的 p 的幂次恰好为 $l - k$，故可知矛盾！从而一定存在一个迷向子群 F_A 的阶恰为 p^k. ♣

Remark. 第二个证明过程相当精彩，反复寻找群在集合上的作用，从而进行轨道划分，然后再进行统一的计数，两次作用的过程比较抽象，需要仔细体会，反复理解.

定义 1.10.2: Sylow $p-$ 子群

设 $|G| = p^lm$ 且 $(p, m) = 1$，其中 p 为素数，$l \geq 1$，$(p, m) = 1$，则称 G 的 p^l 阶子群为 G 的**Sylow $p-$ 子群**.

Sylow 第一定理证明了 Sylow p-子群的存在性，从而一个自然的问题就是，这样的子群是否唯一，如果不唯一，他们之间是否存在一定联系？下面的 Sylow 第二定理一定程度上回答了这个问题：

定理 1.10.4: Sylow 第二定理

设 P 是 G 的一个 Sylow p-子群，H 是 G 的一个 p^k 阶子群，$k \leq l$，则存在 $g \in G$ 使得 $H \subseteq gPg^{-1}$. 特别地，G 的 Sylow p-子群是相互共轭的.

证明 考虑群 H 在集合 $G \setminus P$ 上的左平移作用 $(h, gP) \mapsto h(gP)$，又由 $p \nmid |G \setminus P|$，从而可知 $G \setminus P$ 中有不动点 gP，对任意 $h \in H$，均有 $h(gP) = gP$，从而 $h \in gPg^{-1}$，即 $H \subseteq gPg^{-1}$，即证. ♣

命题 1.10.1: Sylow p 子群的个数

设 P 是群 G 的一个 Sylow $p-$ 子群，则 $n_p = [G : N_G(P)]$，这里 $n_p = |X_p| = \{P|P < G, |P| = p^l\}$，即 Sylow $p-$ 子群的个数.

证明 考虑 $G \curvearrowright X_p$ 即共轭作用，又 Sylow 第二定理可知这个作用在 X_p 上可递，也即 X_p 为齐性空间，从而 $n_p = |X_p| = |O_P| = [G : F_P]$，而 $F_P = \{g \in G|gPg^{-1} = P\} = N_G(P)$，从而即证 $n_p = [G : N_G(P)]$，即证. ♣

利用这个刻画，我们就不难得到 Sylow 第三定理，也被称为计数定理：

定理 1.10.5: Sylow 第三定理

(1)G 的 Sylow $p-$ 子群 $P \lhd G$ 当且仅当 $n_p = 1$，即 Sylow $p-$ 子群唯一；

(2)$n_p|m$，$n_p \equiv 1(\mathrm{mod}\ p)$.

证明 (1) 这是不言自明，不言而喻，不难看出，自然成立的；

(2) 注意到 $n_p = [G : N_G(P)] = |G|/|N_G(P)|$，从而有

$$n_p \cdot \frac{|N_G(P)|}{|P|} = \frac{|G|}{|P|} = m,$$

而由 $P < N_G(P)$ 可知 $|N_G(P)|/|P|$ 为整数，进而有 $n_p \mid m$.

为了证明 $n_p \equiv 1(\mathrm{mod}\ p)$，回想我们在哪见过这玩意，不难想到在证明 p 群作用的轨道公式时，有这样一个结果产生，因此我们自然会去考虑一个 p 群在 X_p 上的作用，更自然地，不妨取 $P \in X_p$，考虑 $P \curvearrowright X_p$ 一个共轭作用，因此有 $n_p \equiv |X_0|(\mathrm{mod}\ p)$，这里 X_0 为不动点集.

若任意 $g \in P$，有 $gP_1g^{-1} = P_1$，即 $P_1 \in X_0$，从而 $P < N_G(P_1)$，则 P 与 P_1 均为 $N_G(P_1)$ 的 Sylow p 子群，且 $P_1 \lhd N_G(P_1)$，从而 $P = P_1$，因此不动点个数恰为 1，即 $n_p \equiv 1(\mathrm{mod}\ p)$. ♣

命题 1.10.2: 思考题——Sylow 定理的小应用

对任何素数 p 和正整数 m，$(p, m) = 1$，则当 l 满足

$$l > v_p((m-1)!) = \sum_{n=1}^{\infty} \left[\frac{(m-1)!}{p^n}\right]$$

就一定有 $p^l m$ 阶群不是单群.

证明 考虑 $|G| = p^l m$，则设其 Sylow $p-$ 子群的个数为 n_p，则有 $n_p|m$ 且 $n_p \equiv 1(\mathrm{mod}\ p)$，从而若 $n_p = 1$，则显然 Sylow $p-$ 子群即为 G 的一个正规子群，进而不为单群；

若 $d = n_p > 1$ 且为 m 的因子，则设 $X_p = \{P_1, P_2, \cdots, P_d\}$ 为 G 的 Sylow $p-$ 子群的集合，从而 G 在 X_p 上的共轭作用可递，进而这个作用对应 $G \to S_d$ 的一个同态 π，又因为一方面作用可递，从而 $\ker \pi \neq G$，否则任意 g，有 $gP_kg^{-1} = P_k$，不会和别的子群联系起来；另一方面，由 $v_p(|G|) = l > v_p((m-1)!) = v_p(m!) > v_p(|S_d|)$，从而 $|G| \nmid |S_d|$，进而 $\ker \pi \neq \{e\}$ 为单同态，

从而 $\ker\pi \lhd G$ 且非平凡，这表明 G 不为单群. 综上即证. ♣

1.10.2 Exercises From Z.Fh

1. 见定理 1.10.3 的第二个证明.

2.证明 若 p^2 阶群 G 有 p^2 阶元，则 $G \cong \mathbb{Z}_{p^2}$，从而为 Abel 群；

若 G 中无 p^2 阶元，即全为 p 阶元，则由 p 群有非平凡的中心元素，设 $a \in C(G)$，且 a 的阶为 p，则有 $b \notin \langle a\rangle$，从而有 $ab = ba$，进而 $G = \langle a, b\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_{\text{l}}$，从而也为 Abel 群.

综上，我们有 p^2 阶群的同构类为 $\mathbb{Z}_{p^2}$ 和 $\langle a, b\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_{\text{l}}$. ♣

3.解 由 $|S_4| = 24 = 3 \times 2^3$，从而 $n_3 \mid 8$ 且 $n_3 \equiv 1(\text{mod } 2)$，则 $n_3 = 1$ 或 4，而易见 $\langle(123)\rangle$，$\langle(124)\rangle$，$\langle(134)\rangle$，$\langle(234)\rangle$ 均为 Sylow 3 子群，因此 $n_3 = 4$.

又 $n_2 \mid 3$，且 $n_2 \equiv 1(\text{mod } 2)$，从而 $n_2 = 1$ 或 3，又若 $n_2 = 1$，则说明 sylow 2 子群为 S_4 的 8 阶正规子群，而熟知 S_4 的非平凡正规子群仅有 A_4 和 K_4，从而矛盾，因此 $n_2 = 3$.

综上 S_4 的 Sylow 子群有 4 个 Sylow 3 子群，3 个 Sylow 2 子群. ♠

Remark. 事实上，我们“不难”求出所有的 Sylow 2 子群：

$$\{1, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}$$
$$\{1, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\},$$
$$\{1, (14), (23), (12)(34), (13)(24), (14)(23), (1243), (1342)\}.$$

4.解 由 $|S_p| = p!$，从而一方面有 $n_p \equiv 1(\text{mod } p)$，且由 p 阶群均为循环群，可知 Sylow p 子群均为 p 阶元生成；另一方面，易见 p 阶元一共 $(p-1)!$ 个，而每个循环子群需要 $(p-1)$ 个 p 阶元，故 $n_p = (p-2)!$，因此我们有 $(p-2)! \equiv 1(\text{mod } p)$，即证 wilson 定理：$(p-1)! \equiv -1(\text{mod } p)$. ♠

5.证明 设 X 为 G 的所有子群构成的集合，考虑 $G \curvearrowright X$ 上的共轭作用，记 $X_0 = \{H \in X | gHg^{-1} = H, \quad \forall g \in G\}$ 为全体正规子群构成的集合，又由 $|X| \equiv |X_0|(\text{mod } p)$(由 G 为 p 群)，从而结合非正规子群的个数为 $|X| - |X_0|$ 为 p 的倍数，即证. ♣

6.证明 由 $N \lhd G$，从而可以考虑 $G \curvearrowright N$ 上的共轭作用，从而由 G 为 p 群，故设共轭作用的不动点集为 X_0，从而 $|X| \equiv |N|(\text{mod } p)$，进而 $p||X|$，又显然 $|X| \geq 1$，因此 $|X| = p$，故 N 中每个元素均为不动点，从而 $N \subseteq C(G)$，即证. ♣

7.证明 显然 $P \leq N_G(P)$，且 $P \lhd N_G(P)$，从而考虑 $P \curvearrowright G/P$ 即左平移作用，则有不动点 $X_0 = \{gP | pgP = gP, \forall g \in G\} = N_G(P)/P$，从而有 $|X_0| = |N_G(P)|/|P|$，则又由 P 为 p 群从而 $|X_0| \equiv |G/P| \equiv 0(\text{mod } p)$，从而结合 $|N_G(P)|/|P| \geq 1$，从而可知 $|N_G(P)|/|P| \geq p$，因此 P 为 $N_G(P)$ 的真子群，即证. ♣

8.证明 (1) 由 $56 = 7 \times 2^3$，从而有 $n_7 \equiv 1(\text{mod } 7)$，且 $n_7|8$，从而 $n_7 = 1$ 或 8，若 $n_7 = 1$，则 Sylow 7 子群即为一个非平凡正规子群，从而不为单群；

若 $n_7 = 8$，从而有 8 个 Sylow 7 子群，则由 7 阶群一定为循环群，因此我们有每个非幺元均为 7 阶元，且每个 Sylow 7 子群交集仅为幺元，进而可知恰有 $8 \times (7-1) = 48$ 个 7 阶元，从

而可知恰有一个 8 阶的 Sylow 2 子群，进而为非平凡的正规子群，从而也不为单群.

(2) 由 $72 = 2^3 \times 3^2$，从而 $n_3 \equiv 1(\text{mod } 3)$，且 $n_3|4$，则有若 $n_3 = 1$，从而可知其有唯一的 Sylow 3 子群，进而为非平凡正规子群，从而不为单群；

若 $n_3 = 4$，从而考虑 $X_3 = \{P_1, P_2, P_3, P_4\}$ 为 Sylow 3 子群构成的集合，考虑 $G \curvearrowright X_3$ 上的共轭作用，对应 $G \to S_{X_3} = S_4$ 的同态 π，则由作用可递，因此 $\text{Ker}\pi \neq G$，又若 $\text{Ker}\pi = \{e\}$，从而 $G \cong \text{Im}\pi < S_4$，而 $|G| = 73 > 24 = |S_4|$，矛盾，因此 $\text{Ker}\pi$ 为 G 的非平凡正规子群，从而不为单群，即证. ♣

9.证明 这个题的结论弱于命题 1.10.2，不难由那个推导出本题. ♣

11.证明 考虑 $G \curvearrowright G/H$ 即左平移作用诱导出的 $G \to S_p$ 的同态 f，从而 $\ker f \lhd G$，且 $G/\ker f \cong S < S_p$，这表明 $|G/\ker f| \mid |S_p| = p!$，而 $|G/\ker f| \mid |G|$，从而最小素因子即为 p，这表明 $|G/\ker f| = p = [G : H]$，而在上一问中我们已经得到 $\ker f < H$，因此 $H = \ker f \lhd G$，综上我们完成了证明. ♣

12.证明 一方面不难注意到 $N_G(P)N \subseteq G$，因此我们下面证明任意 $g \in G$ 可以分解，注意到 $gPg^{-1} \leq gNg^{-1} = N$，而 gPg^{-1} 也为 N 的 Sylow 子群，从而可知存在 $n \in N$ 使得 $gPg^{-1} = nPn^{-1}$，也即 $n^{-1}g \in N_G(P)$，从而 $g \in N_G(P)N$，即证 $G \subseteq N_G(P)N$，综上我们即可证明 $G = N_G(P)N$. ♣

13.证明 显然 $N_G(P) \lhd N_G(N_G(P))$，则任取 $h \in N_G(N_G(P))$，有任意 $g \in N_G(P)$，有 $hgh^{-1} \in N_G(P)$，也即 $hgh^{-1}Phg^{-1}h^{-1} = P$，从而 $gh^{-1}Phg^{-1} = h^{-1}Ph$，也即 $N_G(P) \subseteq N_G(h^{-1}Ph)$，而这两者均为 Sylow p 子群，从而 $|N_G(P)| = |N_G(hPh^{-1})| = |G|/n_p$，因此 $N_G(P) = N_G(h^{-1}Ph)$，又 $P \lhd N_G(P)$ 为唯一 Sylow 子群，因此又 $h^{-1}Ph$ 为 Sylow 子群，进而 $h^{-1}Ph = P$，进而 $h \in N_G(P)$，从而可知 $N_G(P) = N_G(N_G(P))$，即证. ♣

14.证明 一方面显然 $H \lhd N_G(H)$，另一方面任意 $g \in N_G(H)$，有 $gPg^{-1} \leq gN_G(P)g^{-1} \leq gHg^{-1} = H$，从而 gPg^{-1} 与 P 为 H 的 Sylow 子群，则存在 $h \in H$ 使得 $gPg^{-1} = hPh^{-1}$，从而 $h^{-1}g \in N_G(P) \subseteq H$，从而 $g \in H$，进而可知 $N_G(H) = H$，综上即证.

注：本题是上一题的推广版本，这里取 $H = N_G(P)$ 即可证明上一题. ♣

15.证明 一方面，若群中有 pq 阶元则命题显然成立，另一方面，假设群中不存在 pq 阶元，则除了幺元，每个元的阶为 p 或 q，因此若设 Sylow p 子群与 Sylow q 子群的个数分别为 n_p 和 n_q，则我们有

$$n_p(p-1) + n_q(q-1) + 1 = pq,$$

进而不难知道该不定方程的整数解仅有 $(1, p)$ 和 $(q, 1)$，而利用 $n_p \equiv 1(\text{mod } p)$ 和 $n_q \equiv 1(\text{mod } q)$ 不难知道均不符合，进而可知矛盾，综上可知其一定为循环群. ♣

16.证明 因为 $p \nmid [G : H]$，因此可知 H 与 G 有公共的 Sylow p 子群 P，又任意 G 的 Sylow p 子群 P_1，存在 g 使得 $P_1 = gPg^{-1} \leq gHg^{-1} = H$，其中用到了 $H \lhd G$，因此可知 P_1 为 H 的 Sylow 子群，综上可知 H 包含 G 的所有 Sylow p 子群. ♣

17.证明 我们设 G 的 Sylow p 子群全体为 $\{P_1,\cdots,P_k\}$，则考虑 $H=\bigcap_{i=1}^{k}P_i$，则由所有 Sylow 子群均为互相共轭的，因此不难证明 $H\lhd G$，另一方面，有 H 可视为 P_1 的所有共轭子群之交，因此由习题 1.9 题 14，不难知道 H 为 $\pi:G\to S_{G/P_1}=S_k$ 的同态核，从而 $|H|=\ker\pi$.

若 $k=1$，则可知 G 有唯一的 Sylow p 子群；若 $k>1$，则有 $K|m$，且 $k\equiv 1(\mathrm{mod}\ p)$，因此只有 $k=m=p+1$，从而可知 $G/H=G/\mathrm{Ker}\pi\cong\mathrm{Im}\pi<S_{p+1}$，也即存在 $d|(p+1)!$ 使得

$$\frac{|G|}{|H|}=\frac{p^l(p+1)}{|H|}=\frac{(p+1)!}{d},$$

因此我们有 $|H|\cdot(p-1)!=d\cdot p^{l-1}$，则有 $p^{l-1}\mid|H|$，从而可知 $|H|=p^{l-1}$ 或 p^l，即证 G 中有正规的 Sylow 子群或正规的 p^{l-1} 阶阶子群. ♣

1.10.3 p-群的性质

我们这里简要汇总一下关于 p-群的性质，材料来自 Dummit，下面如果不特殊说明，p 为素数，P 是一阶为 p^a 的群，$a\geq 1$.

定理 1.10.6: p-群的中心

P 有非平凡的中心元素，即 $1<C(P)\lhd P$.

证明 我们考虑类方程 (class equation)，即考虑 P 在 P 上的共轭作用，有

$$|P|=|C(P)|+\sum_{i=1}^{k}|O_i|,$$

这里 O_i 表示共轭作用下的轨道，值为 $[P:F_i]$，F_i 为轨道 O_i 代表元对应的迷向子群，因此不难有 $p\mid C(P)$，对于正规性则是直接的，即证. ♣

定理 1.10.7: p-群的正规子群

H 为 P 的非平凡正规子群，则 $H\cap C(P)\neq 1$，特别地，任意 p 阶正规子群在 $C(P)$ 中.

证明 我们这里依然希望得到上一证明中的等式，但这需要一点更细致的讨论，我们容易发现在考虑共轭作用下，每个轨道 O_i，设其有代表元 a_i，则若 $a_i\in H$，则由 H 正规性，任意 $g\in P$，$ga_ig^{-1}\in H$，进而 $O_i\subseteq H$，因此也可以在 H 内实现轨道的“子分解”，即有

$$|H|=|H\cap C(P)|+\sum_{i=1}^{k}|O_i\cap H|,$$

进而不难看见 $|O_i\cap H|$ 为 0 或 $|O_i|$，因此仍有 $p\mid|H\cap C(P)|$. ♣

定理 1.10.8

$H\lhd P$，若 $p^b\mid|H|$，则 H 存在 p^b 阶子群 K 使得 $K\lhd P$.

1.11 群的直积

1.11.1 群的直积

本节的目的是回忆群的直积，并且揭示一些基本的性质，并不加证明的引入有限生成 Abel 群的基本定理.

命题 1.11.1: 有限群的直积的阶

设 $G_1,\cdots,G_n$ 为有限群，则群 $G_1\times\cdots\times G_n$ 的阶为

$$|G_1|\cdots|G_n|.$$

下面这个性质对我们理解直积与其分量间关系有着重要意义，我们也将意识到，直积模掉一个分量就完全可以视为把它拿走，非常的轻松愉快.

命题 1.11.2: 直积的分量

设 $G_1,\cdots,G_n$ 为群，群 $G=G_1\times\cdots\times G_n$，则我们有

$$G_i\cong\{(1,\cdots,g_i,\cdots,1)|g_i\in G\},$$

并且不难发现 $G_i\lhd G$，且

$$G_i\cong G_1\times\cdots\widehat{G_i}\times\cdots G_n.$$

因此在同构的意义下，对任意 $x\in G_i\lhd G$，$y\in G_j\lhd G$，有 $xy=yx$，即为交换的.

注：上述命题可以做进一步的推广，如果我们设 $I\cup J=\{1,2,\cdots,n\}$ 且 $I\cap J=\varnothing$，则对 $I=(n_1,\cdots,n_i)$，我们如果定义

$$G_I=\{(\cdots,g_{n_1},\cdots,g_{n_2},\cdots,g_{n_i},\cdots)|g_k\in G_k\}$$

即除了 n_k 位，其余均为 1. 那么有 $G_I\cong G_{n_1}\times\cdots\times G_{n_i}$，且 $G_I\lhd G$，$G\cong G_I\times G_J$.

另外一个值得一提但很平凡的事实是，对群 $G=G_1\times\cdots\times G_n$，我们有 G 的全体子群形如 $H_1\times\cdots\times H_n$，这里每个 H_i 均为 G_i 的子群.

下面我们区分两种直积，一种是内直积，一种是外直积，其区别主要体现在如下定义上：

定义 1.11.1: 内直积和外直积

设 $H,K<G$，称 $H\times K$ 为 H,K 的**外直积**，如果特别地 $H\lhd G$，$K\lhd G$ 且 $H\cap K=1$，则我们称 HK 为 H,K 的**内直积**.

为什么我们痴迷于 $H\lhd G$，$K\lhd G$ 且 $H\cap K=1$ 这个条件呢？因为我们有下面这个 Recongniton Theorem：

定理 1.11.1: Recongniton Theorem

设 $H \lhd G$，$K \lhd G$ 且 $H \cap K = 1$，则 $HK \lhd G$ 且 $HK \cong H \times K$.

证明 我们熟知 $HK \lhd G$，这是之前一道熟知的习题，我们更关心 $HK \cong H \times K$ 的证明，一个基本且自然的映射是长成这样的

$$\varphi : HK \to H \times K, \quad hk \mapsto (h, k),$$

这样定义又自然伴生了两个问题，一个是良定义问题，即任意元素 $hk \in HK$ 表示方法是否唯一？另一个则是这样的映射是否是同态以及双射.

我们容易看到一个基本的事实是 $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K| = |H \times K|$，因此良定义以及双射的问题不证自明. 那么关于同态，只需注意到 $HK = KH$ 这一信息，进而不难证明. ♣

下面我们来简单看一下这个定理的一个运用：

例 1.11.1 (置换的中心 $C_{S_n}(\sigma)$)**.** 设 $\sigma \in S_n$，我们关心 $C_{S_n}(\sigma)$，这里考虑 σ 作用的不动点集

$$I = \{i \in \{1, 2, \cdots, n\} | \sigma(i) = i\}.$$

我们若记 $C = C_{S_n}(\sigma)$，那么容易看见 $C < \mathrm{Stab}I = \{\sigma \in S_n | \sigma(i) \in I, \forall i \in I\}$，因此设 $J = \{1, \cdots, n\} - I$，易见 $C < \mathrm{Stab}J$，又注意到 $G = \mathrm{Stab}I = \mathrm{Stab}J$，故考虑

$$\begin{aligned} H &= \{\sigma \in G | \sigma(i) = i, \quad \forall i \in I\} \\ K &= \{\sigma \in G | \sigma(j) = j, \quad \forall j \in J\} \end{aligned},$$

则不难发现 $H, K \lhd G$ 且 $H \cap K = 1$，因此 $HK \cong H \times K$，而事实上，容易看见 $G = HK$，故 $G \cong H \times K \cong S_J \times S_I$，这是因为不难看见 $H \cong S_J$，$K \cong S_I$.

这表明 C 为 $H \times K$ 的子群，其可表示为 $H_1 \times K_1$，容易看见任意 $\tau \in K$，τ 与 σ 可交换，因此 $K_1 = K$，故对 H_1，不难看到其同构于 $C_H(\sigma)$，因此我们事实上有

$$C_{S_n}(\sigma) \cong C_H(\sigma) \times K \cong C_{S_J}(\sigma) \times S_I.$$

最后，为了便于半直积中行文的叙述，我们这里给出一个看似唐突且平凡但实际意义非凡的一个小结论：

定理 1.11.2: 群的直积与自同构群

设 $H < G$，称 H 为 G 的**特征子群**，如果任意 $\sigma \in \mathrm{Aut}(G)$，均有 $\sigma(H) = H$，往往记作 $G \mathrm{Char} H$. 现若有 $G = HK$ 且 H, K 均为 G 的特征子群，$H \cap K = 1$，则有

$$\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K).$$

证明 容易看见特征子群均为正规子群 (考虑内自同构)，因此有 $HK \cong H \times K$(回忆 Recongnition Theorem)，因此任意 $\sigma \in \mathrm{Aut}(G)$，$g = hk$，则 $\sigma(g) = \sigma(h, k) = (h', k')$，其中 $h' \in H, k' \in K$(这

是由特征子群之定义)，因此定义 $\sigma_1 \in \mathrm{Aut}(H)$，$\sigma_2 \in \mathrm{Aut}(K)$，满足 $\sigma_1(h) = h'$，$\sigma_2(k) = k'$，不难证明 $\sigma \mapsto (\sigma_1, \sigma_2)$ 为一个同构. ♣

1.11.2 有限生成的 Abel 群

我们这里仅给出有限群的版本，因为有限 Abel 群一定是有限生成的：

定理 1.11.3: 有限 Abel 群基本定理

设 G 为 n 阶 Abel 群，从而存在整数 $n_1, n_2, \cdots, n_s$ 使得

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s},$$

其中 $n_j \geq 2$ 对任意 $1 \leq j \leq s$，$n_{i+1} \mid n_i$，对任意 $1 \leq i \leq s-1$，以及 $n_1 n_2 \cdots n_s = n$.

注：这里正整数数 $n_1, n_2, \cdots, n_s$ 称为 G 的**不变因子**.(你想到了什么？) 回忆高等代数中的相似标准型理论，矩阵相似的其中一个不变量是其 λ 矩阵的不变因子，即把 λ 矩阵化为法式

$$\mathrm{diag}\{d_1(\lambda), \cdots, d_n(\lambda)\},$$

且满足 $d_{i+1}(\lambda) \mid d_i(\lambda)$，且 $d_1(\lambda) \cdots d_n(\lambda) = D(\lambda)$，从而对比即可看出具有完全类似的结构，进而不变因子在同构意义下的不变性也好理解了.

那么下面一个自然的问题就是，给定一个正整数 $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$，如何求出它所有可能的 Abel 群呢？当然这便不再是一个群论问题，而是一个饶有趣味的组合问题了.

首先我们需要铭记在心里的一个基本事实是，对 $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$，我们有

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}},$$

这个结论不难由 $(m, n) = 1$ 则 $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ 得到. 因此我们类比相似标准型中初等因子与不变因子间的关系，我们

1.12 群的半直积

首先让我们回忆一下群论研究中的核心目标，我们想得到群，我们想分解群，在上一节群的直积中，**任意**给定两个群 H,K(可能毫不相关)，我们可以构造出 $G=H\times K$，使得 H,K 为 G 的正规子群，并且 $H\cap K=1$(当然这里的 H,K 相交是站在 G 的子群角度来看的).

这个角度是站在生成的观点来看的，且仅从生成角度，直积已经达到我们的一个设想了. 现在反过来看群的分解，上述构造对应了一个分解，把给定的群分成其两个正规子群的直积，这样一看这种分解便显得十分苛刻.

因此我们不由产生一种设想，如果仅要求一个子群是正规的，那这种分解或许更容易实现? 这个问题放宽一下，我们便会去问给定 G 以及其正规子群 H，若有 $K\lhd G$ 且 $H\cap K=1$，那么首先毋庸置疑 HK 是 G 的子群 (利用 H 的正规性)，且任意 $g\in HK$，g 能被唯一分解成 hk，这样看起来我们又得到了一个 $hk\mapsto(h,k)$ 的映射，但是注意，相较于直积，**乘法运算法则**发生了改变.

在 K 也是正规子群的假设下，我们很快能得到

$$(h_1k_1)(h_2k_2)=(h_1h_2)(k_1k_2),$$

这是利用了交换化子 $h^{-1}k^{-1}hk\in H\cap K=1$ 从而实现的，但是在失去 K 正规的假设下，我们虽然仍有

$$(h_1k_1)(h_2k_2)=h_1(k_1h_2k_1^{-1})(k_1k_2):=h_3k_3,$$

但这里 $h_3=h_1(k_1h_2k_1^{-1})$ 不再是单纯的 h_1h_2，而是 $h_1\ k_1\cdot h_2$，这里 $k\cdot h$ 表示 $K\curvearrowright H$ 即共轭作用. 因此我们可以考虑把这个共轭作用推广至一般群作用，从而得到**半直积**的概念.

定理 1.12.1: 半直积的构造

设 H,K 为群，φ 为群 K 到 $\mathrm{Aut}(H)$ 的同态，记 $\cdot$ 表示 φ 诱导的群作用，也即 $k\cdot h=\varphi(k)(h)$，设 G 是全体 (h,k) 构成的集合，定义 G 上的乘法

$$(h_1,k_1)(h_2,k_2)=(h_1\ k_1\cdot h_2,k_1k_2).$$

1. G 是阶为 $|H||K|$ 的群;
2. $H\cong\{(h,1)|h\in H\}$，$K\cong\{(1,k)|k\in K\}$，并在这个意义下，$H\cap K=1$;
3. 任意 $h\in H,k\in K$，$khk^{-1}=k\cdot h=\varphi(k)(h)$，进一步 $H\lhd G$.

证明 只有最后一条略显不平凡，注意到 $(h,k)^{-1}=(k^{-1}\cdot h^{-1},k^{-1})$，因此 $(1,k)(h,1)(1,k)^{-1}=(k\cdot h,k)(1,k^{-1})=(k\cdot h,1)$，这表明 $K\le N_G(H)$，也表明 $khk^{-1}=k\cdot h$. 又注意到 $G=HK$，从而 $N_G(H)=G$，这即 $N_G(H)=G$ 从而 $H\lhd G$. ♣

接下来我们就可以定义半直积的概念了:

定义 1.12.1: 半直积

设 H, K 为群，φ 为群 K 到 $\mathrm{Aut}(H)$ 的同态，则我们把按上一定理所构造得到的群 G 叫做 H 和 K 的**半直积**，记作 $H \rtimes_\varphi K$，这里 $\rtimes$ 的方向遵循正规子群的方向.

1.13 2021 伯苓班抽象代数 I 期中考试

Problem 1. (20 分) 判断下列命题是否正确, 如果正确请给出证明，不正确请举出反例.

1. 幺半群 G 里，元素 a 有左逆元和右逆元，则 a 是可逆元.
2. 群 G 中 a 的阶有限而 ab 的阶无限，那么 b 的阶无限.
3. $n \in \mathbb{N}^*$，$G < S_n$，则 G 中要么只有偶置换，要么奇置换和偶置换各占一半.
4. G 是群，$H \subseteq G$，且 $\forall g \in G, h \in H$，$ghg^{-1} \in H$，则 $H \lhd G$.

解 1. 正确，设 $ba = ac = e$，从而有 $b = be = bac = ec = c$，则 b 为 a 的逆元，从而 a 为可逆元.

2. 错误, 定义群 G 满足幺元为 e, 且 $a^2 = b^2 = e$, 定义 ab 为无限阶元素, 则 $G = \{e, a, b, a*b\}$ 则为一个群，这里 $a * b$ 表示 a, b 生成的自由群，且显然是一个反例.

3. 正确，若置换群 G 中有奇置换 τ，从而设 H 为 G 中所有偶置换组成的集合，则对每个奇置换 σ，$\tau^{-1}\sigma$ 为偶置换，进而在 H 中，因此 $G = H \cup \tau H$，也即奇置换和偶置换各占一半.

4. 错误，考虑 $G = \mathrm{GL}(n, \mathbb{R})$，考虑 H 为全体行列式为 2 的 n 阶实矩阵构成的集合，则不难见到 $ghg^{-1} \in H$，但显然 H 不为群，更不为 G 的正规子群. ♠

Problem 2. (20 分) 设 G 是群. 证明:

1. $a \to a^{-1}$ 是群 G 的自同构等价于 G 是 Abel 群.
2. 若存在 $a \to a^3$ 是群 G 的单同态，则 G 是 Abel 群.

证明 1. 若群 G 为 Abel 群，从而对 $\pi : a \mapsto a^{-1}$，有 $\pi(ab) = b^{-1}a^{-1} = a^{-1}b^{-1} = \pi(a)\pi(b)$，从而 π 为群同态，又不难看到其为双射，因此其为群 G 的自同构.

若 π 为自同构，从而任意 $a, b \in G$，有 $ab = \pi(b^{-1}a^{-1}) = \pi(b^{-1})\pi(a^{-1}) = ba$，因此 G 为 Abel 群，综上即证.

2. 设 $\sigma : x \mapsto x^3$，由 $(xy)^3 = x^3y^3$，则 $x^2y^2 = yxyx$，由 $(yx)^3 = y^3x^3$，则 $y^2x^2 = xyxy$，进而 $y^2x^3 = xyxyx = x(x^2y^2) = x^3y^2$，因此 x^3 与 y^2 可交换，进而我们有

$$\varphi(xy^2) = x^3y^6 = y^6x^3 = \varphi(y^2x),$$

因此由 φ 为单同态可知 $xy^2 = y^2x$，进而 $xy^2x = y^2x^2 = xyxy$，也即 $xy = yx$，从而群 G 为 Abel 群，即证. ♣

Problem 3. (20 分) 求解下列问题：

1. 求元素
$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 12 & 1 & 8 & 6 & 4 & 2 & 7 & 5 & 10 & 15 & 11 & 13 & 14 & 3 & 9 \end{pmatrix}$$
的阶.

2. 求 S_{15} 的 7 阶元的个数.

解 1. 易见 φ 可分解为 (1 12 13 14 3 8 5 4 6 2)(9 10 15)，一个 11 阶轮换和 3 阶轮换的乘积，因此其阶为 $[11,3]=33$.

2. 设 7 阶元可分解成若干不相交的轮换之积，则每个轮换的阶只能为 1 或 7，进而可知 7 阶元一定为全体 7 轮换或者为两个不相交的 7 轮换乘积，因此元素个数即 $\mathrm{C}_{15}^7\cdot\frac{7!}{7}+\mathrm{C}_{15}^7\cdot\frac{7!}{7}\cdot\mathrm{C}_8^7\cdot\frac{7!}{7}=26691865200$ 个. ♠

Problem 4. (15 分) 证明 455 阶群是循环群.

证明 易见 $455=5\times7\times13$，考虑 G 的 Sylow 5，7，13 子群，则可知
$$n_5|91,\ n_5\equiv1(\mathrm{mod}\ 5),\ n_7|65,\ n_7\equiv1(\mathrm{mod}\ 7),\ n_{13}|35,\ n_{13}\equiv1(\mathrm{mod}\ 13),$$
因此不难得到 $n_7=n_{13}=1$，$n_5=1$ 或 91，若为前者，则可知 G 有三个正规的 Sylow 子群 P_5，P_7，P_{13}，故由其均为循环群，则相交为幺元，可知 $G=P_5\times P_7\times P_{13}$ 为 455 阶循环群，即证；

若 $n_5=91$，从而一共有 $91\times4=364$ 个 5 阶元，而由 P_7 与 P_{13} 正规，且相交为幺元，则有 $P_7\times P_{13}<G$，为一 91 阶循环群，从而与 Sylow 5 子群相交为幺元，恰好拼凑为 455 阶群 G，即 G 中元素为 5，7，13，91 阶，但我们任取一个 5 阶循环群 P_5，则有 $|P_5P_7|=|P_5||P_7|/|P_5\cap P_7|=35$，从而 P_5，P_7 分别是 P_5P_7 的唯一正规 Sylow p 子群，进而可知这为直积 $P_5\times P_7$，为 35 阶循环群，说明 G 中有 35 阶元，矛盾！

综上可知，455 阶群一定是循环群. ♣

Problem 5. (15 分) 设有限群 G 的所有 Sylow $p-$ 子群都是正规子群，则 G 可以分解成若干个 Sylow $p-$ 子群的直积.

证明 设 $|G|=p_1^{\alpha_1}\cdots p_t^{\alpha_t}$，从而设 G 的 Sylow 子群为 $P_1,\cdots,P_t$，则我们下面归纳证明 $P_1\times P_2\times\cdots\times P_t$，由 $P_1\cap P_2=\{e\}$(因为相交为两者的子群，从而由 Lagrange 定理可知一定为幺元)，则由 Sylow 子群的唯一性，可知 $P_1\lhd G$，$P_2\lhd G$，则 $P_1\times P_2$，又任意 $g\in G$，$h_1\in P_1$，$h_2\in P_2$，

则 $gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} \in P_1 \times P_2$，从而 $P_1 \times P_2 \lhd G$，进一步也有 $P_1 \times P_2 \cap P_3 = \{e\}$，因此可知 $P_1 \times P_2 \times P_3$，因此可得 $P_1 \cdots P_t = P_1 \times \cdots \times P_t$.

另一方面，显然 $P_1 \times \cdots \times P_t < G$，且 $|P_1 \times \cdots \times P_t| = p_1^{\alpha_1} \cdots p_t^{\alpha_t} = |G|$，因此 $G = P_1 \times \cdots \times P_t$，即证其为所有 Sylow 子群的直积. ♣

Problem 6. (10 分) 求 A_4 的自同构群 $\mathrm{Aut}(A_4)$.

证明 不难验证 $A_4 = \langle (123), (12)(34) \rangle$，又自同构 $f \in \mathrm{Aut}(A_4)$ 保持元素的阶，且 $f((123))$ 与 $f((12)(34))$ 可以生成 A_4，故自同构由 (123) 与 $(12)(34)$ 的像决定，而三阶元共 8 个，二阶元共 3 个，因此 $|\mathrm{Aut}(A_4)| \leq 24$.

另一方面，考虑 S_4 在 A_4 上的共轭作用，其诱导出一个同态 $\pi : S_4 \to \mathrm{Aut}(A_4)$，$\sigma \mapsto \mathrm{Ad}_\sigma$，由 $A_4 \lhd S_4$ 可知这是良定义的. 又 $\mathrm{Ker}\pi = C_{S_4}(A_4)$，且有 $S_4 = A_4 \cup (12)A_4$，若 $\tau \in A_4$，则若 $\tau = (abc)$ 或 $(ab)(cd)$，则对前者，有 $(abc)(abd) \neq (abd)(abc)$，从而 $(abc) \notin C_{S_4}A_4$，对后者，有 $(ab)(cd)(abc) \neq (abc)(ab)(cd)$，从而可知 $(ab)(cd) \notin C_{S_4}A_4$. 若 $\tau \in (12)A_4$，不妨设 $\tau = (12)\sigma$，则若 $\tau \in C_{S_4}A_4$，且 $\sigma = (abc)$，考虑 $\tau\sigma^{-1} = \sigma^{-1}\tau$，即 $(12)\sigma = \sigma(12)$，又一定存在 $c \neq 1, 2$，则显然不成立；若 $\sigma = (ab)(cd)$，则 “不难” 找到一个 A_4 中元与其不可交换. 综上有 $\mathrm{Ker}\pi = \{e\}$，因此 $S_4 \leq \mathrm{Aut}(A_4)$.

综合两方面可知 $\mathrm{Aut}(A_4) \cong S_4$，即证. ♣

1.14 2022 伯苓班抽象代数 I 期中考试

Problem 1. (20 分) 判断下列命题是否正确, 如果正确请给出证明，不正确请举出反例.

1. 群 G 中 ab 无限，那么 a, b 的阶都无限.
2. 设 G 是奇数阶群，$H < G$，且 $[G : H] = 3$，则 $H \lhd G$.
3. 设 Z 是群 G 的中心，若 $H < G$，则 $Z \cap H$ 为 H 的中心.
4. 任意 12 阶群均有 6 阶子群.

Problem 2. (20 分) 证明：复数域加群 $\{\mathbb{C}, +\}$ 与非零复数乘法群 $\{\mathbb{C}^*, \cdot\}$ 不同构.

Problem 3. (15 分) 设 p 为素数，G 为 p^n 阶群，$n \geq 1$，证明：群 G 存在指数为 p 的正规子群.

Problem 4. (20 分) 设 G 为群，$N \lhd G$，若 H，G/N 均为有限生成群，证明：G 为有限生成群.

Problem 5. (15 分)

(1) 分别计算 $\mathrm{SO}(n)$ 和 $\mathrm{O}(n)$ 在其二阶元构成集合上的共轭作用的轨道个数；

(2) 证明：$\mathrm{SO}(n)$ 与 $\mathrm{O}(n)$ 不同构.

Problem 6. (10 分) 证明 455 阶群是循环群.

2 环论

2.1 环的定义与基本性质

2.1.1 Notes

定义 2.1.1: 环

一个非空集合 R 称为一个**环**，如果其关于加法构成 Abel 群，关于乘法构成半群，且乘法与加法之间满足左、右分配律：

$$a(b+c)=ab+ac,\quad (b+c)a=ba+ca,\quad \forall a,b,c\in R.$$

如果关于乘法还有幺元，则称 R 为**幺环**，若交换，则成为**交换环**.

命题 2.1.1: 关于乘法运算的限制条件

如果一个环对于乘法也构成群，则其为零环.

证明 设关于乘法，加法的幺元为 $e,0$，从而设 0 关于乘法有逆元 a，则 $0=0a=e$，从而 $e=0$，进而任意 $r\in R$，有 $r=er=0r=0$，也即 R 为零环. ♣

定义 2.1.2: 零因子与消去律

设 R 为一个环，$a,b\in R$，且 $a\neq 0,b\neq 0$，若 $ab=0$，则称 a 为 R 中的一个**左零因子**，称 b 为 R 中的一个**右零因子**. 如果在环 R 中，由 $ax=ay$，$a\neq 0$，可以推出 $x=y$，则称 R 满足**左消去律**；如果由 $xa=ya$，$a\neq 0$，可以推出 $x=y$，则称 R 满足**右消去律**.

定理 2.1.1: 无零因子与消去律

一个环 R 没有零因子的充分必要条件为 R 满足左右消去律.

证明 (“必要性”) 若 R 没有零因子，从而由 $ax=ay$，有 $a(x-y)=0$，又 $a\neq 0$，从而 $x-y=0$，进而 $x=y$，从而成立左消去律，同理成立右消去律；

(“充分性”) 反证法，若 R 有零因子 $ab=0$，从而由左右消去律可知 $a=0=b$，矛盾！♣

定理 2.1.2: 无零因子环的重要性质

设 R 为无零因子环，令 $R^*=R-\{0\}$，则 R^* 中元素对于 R 中的加法具有相同的阶，且当这一共同的阶有限时，必为素数.

证明 显然，若 R^* 中所有元素关于加法的阶均为无穷则命题自然成立. 下假设存在 $a\in R^*$，且有

有限阶 n，即有 $na=0$，从而对任意 $b\in R^*$，有 $(na)b=a(nb)$，因此可知 b 的阶整除 n，设为 m，则不难证明 $m=n$，因此我们可知 R^* 中元素阶均相等.

若 n 不为素数，从而存在 $n_1,n_2<n$，且 $n=n_1n_2$，则由 $0=na^2=(n_1a)(n_2a)$，而 $n_1a,n_2\neq 0$，因此可知矛盾，进而可知每个元素的阶相等且为素数. ♣

定义 2.1.3: 无零因子环的特征

设 R 为无零因子环，若其中所有非零元素都是无穷阶的，则称环 R 的**特征**为 0；若其中所有非零元素都是 p 阶的，则称 R 的特征为 p，我们将环 R 的特征记为 $\mathrm{Ch}R$.

2.1.2 Exercises From Z.Fh

1.解 (1) 易见 R 关于普通加法构成 Abel 群，且乘法满足

$$(a_1+b_1\sqrt{m})(a_2+b_2\sqrt{m})=(a_1a_2+mb_1b_2)+(a_1b_2+a_2b_1)\sqrt{m}\in R,$$

上式成立是注意到 $a_1a_2+mb_1b_2,a_1b_2+a_2b_1\in\mathbb{Q}$. 从而满足乘法封闭性，又分配律是平凡的，从而可知 R 是环.

(2) 关于加法，注意到封闭性与交换性是显然的，且显然有零元 1，即对任意 $a\in R$，均有 $a\oplus 1=1\oplus=a+1-1=a$，且对 a，有负元 $2-a$ 使得 $a\oplus(2-a)=1$，从而关于加法构成 Abel 群.

另一方面，显然乘法满足封闭性，下验证分配律，注意到

$$(a\oplus b)\otimes c=(a+b-1)\otimes c=a+b-1+c-ac-bc+c=(a\otimes c)\oplus(b\otimes c),$$

从而同理有 $a\otimes(b\oplus c)=(a\otimes b)\oplus(a\otimes c)$，综上可知 R 为环.

(3)R 是环，这个证明是平凡的.

(4)R 是环，因为显然关于乘法是一个平凡群，且又关于加法是交换群，从而即是环.

(5) 注意到乘法不一定满足封闭性：

$$\boldsymbol{CD}=\boldsymbol{C}^{\mathsf{T}}\boldsymbol{D}^{\mathsf{T}}\neq-\boldsymbol{D}^{\mathsf{T}}\boldsymbol{C}^{\mathsf{T}}.$$

从而不构成环.

(6)R 是环，这个证明也是平凡的，因为运算内蕴着满足性质，只需验证封闭性，而封闭是平凡的. ♠

2.证明 若 $|R|=2$，则 R 交换显然 $(0\cdot a=0=a\cdot 0)$.

设 $|R|=p\geq 3$ 且为素数，则可知 $\{R,+\}$ 无非平凡子群，从而考虑非 0 元素 $a\in R$，则可知 $\langle a\rangle=R$，即 R 可以看作 a 生成的循环群，即有

$$R=\{a,2a,\cdots,pa=0\},$$

从而任意 $r_1,r_2\in R$，有 $r_1\cdot r_2=(sa)\cdot(ta)=sta^2=r_2r_1$，即交换. ♣

3.解 容易验证关于加法构成群，其中零元为 a，且关于乘法满足封闭性，但注意到

$$c\cdot(b+b)=c\cdot c=a,\quad c\cdot b+c\cdot b=b+b=c,$$

而又 $a\neq c$ 可知 $c\cdot(b+b)\neq c\cdot b+c\cdot b$，从而不满足分配律，不构成环. ♠

4.解 考虑 $M(\mathbb{Z})$ 为整数 $\mathbb{Z}$ 的所有变换组成的集合，在加法和复合运算下构成含幺环，分别构作

$$f(n)=\begin{cases}\dfrac{n}{2} & \text{如果}n\text{为偶数}\\ 0 & \text{如果}n\text{为奇数}\end{cases},\quad g_k(n)=\begin{cases}2n & n\neq 0\\ 2k+1 & n=0\end{cases},$$

其中 k 可取任意整数，进而易见 $f\circ g_k(n)=n$，因此任意 g_k 均为其右逆元. ♠

5.证明 注意到 $-a$ 也为幂零元，从而

$$(e+a)(e-a+\cdots+(-a)^{m-1})=e^m-(-a)^m=e,$$

故可知 $e+a$ 为可逆元. ♣

6.证明 注意到 a 为幂零元，故由上一题的结论可知，$e-a$ 为可逆元，且 $(e-a)^{-1}=e+a+\cdots+a^{m-1}$，则由 $a+b=ab$ 可知 $ab-a-b+e=e$，即 $(e-a)(e-b)=e$，从而 $e-b=e+a+\cdots+a^{m-1}$，则代入显然有

$$ab=-a^m-\cdots-a^2-a=ba,$$

即证. ♣

7.证明 (1) 由 $ab-ba=(ab-ba)^2=ab+ba-aba-bab$，从而可知 $aba+bab=2ba$，又 $a=a^2=(-a)^2=-a$，因此有 $aba=-bab=bab$，从而 $ab=abab=babb=bab$，$ba=baba=bbab=bab$，因此可知 $ab=ba$，进而 R 必为交换环.

(2) 设 a 为 R 的幂等元，从而对任意 $b\in R$，设 $ab=c$，则有 $a^2b=ac$，即 $ab=ac$，从而 $a(b-c)=0$，则由 R 为无零因子环，且 $a\neq 0$，故 $b=c$，从而 $ab=b$，同理有 $ba=b$，由 b 的任意性可知 a 为幺元.

进而若 r 为幂等元。从而 $r^2=r=ra$，即 $r(r-a)=0$，即 $r=a$，综上 R 为幺环，且有唯一幂等元. ♣

8.证明 设 e 为左幺元，从而任意 $a\in R$，有 $ae-a+e$ 因为左幺元，因为 $(ae-a+e)b=ab-ab+b=b$，从而由左幺元唯一可知 $ae-a+e=e$，进而 $ae=a$，从而由 a 的任意性可知，因此可知 e 为右幺元，因此 R 为幺环. ♣

9.证明 设 e 为无零因子环 R 的左幺元，从而对任意非零元素 $a\in R$，设 $ae=a'$，则有 $aea=a'a$，即 $a^2=a'a$，也即 $(a-a')a=0$，则由 R 无零因子，故 $a'=a$，从而 e 为右幺元，综上 e 必为 R 的幺元，即证. ♣

10.证明 由 $aba=a$，从而 $aba\cdot ab=a^2b$，即 $a^2b=aba^2b=a=aba$，则 $baba=ba^2b=e$，则 ba 可逆，进一步 $ba=ab$，又由 $aba\cdot b=ab$，由元素可逆知 $ab=e$，从而 $ba=e$，故 a,b 均为可逆元且互为逆元. ♣

Remark. 事实上本题不需要环的限制，对含幺半群即成立.

11.证明 注意到有 $u(vu-e+v)u=uvu^2-u^2+uvu=uvu=u$，且 $u(uv-e+v)u=u$，进而可知结合唯一性 $uv=vu=e$，从而其互为逆元，即证. ♣

12.解 前面的验证是直接的，我们只讨论最后一个.

这个命题显然不成立，如我们考虑整数环，则易见 $\mathbb{Z}+\mathbb{Z}$，有 $(1,0)(0,1)=(0,0)$，但 $(0,1)$ 与 $(1,0)$ 均不为 0，因此 R_1+R_2 不一定为无零因子环. ♠

14.证明 我们任取 $a\neq 0$，考虑证明任意 b，$a+b=b+a$，注意到

$$\begin{aligned}&(a+b-a-b)a\\=&a^2+ba-a^2-ba\\=&a^2+ba+a(-a)+b(-a)\\=&(a+b)a+(a+b)(-a)\\=&(a+b)(a-a)=0,\end{aligned}$$

从而结合 R 为无零因子环，因此可知 $a+b-a-b=0$，即 $a+b=b+a$，若 $a=0$，则命题平凡，即证 R 为环. ♣

13.证明 这个证明本质和 11 没有区别，注意到有 $u^k(vu-e+v)u^l=u^kvu^{l+1}-u^{k+l}+u^kvu^l=u^{k+l-1}$，同理 $u^k(uv-e+v)u^l=u^{k+l-1}$，从而由唯一性可知 $uv=vu=e$，从而互为逆元. ♣

15.证明 我们只证明一侧，另一侧同理，不妨假设 $e-ab$ 可逆，从而我们断言

$$(e-ba)^{-1}=e+b(e-ab)^{-1}a.$$

注意到 $(e-ba)(e+b(e-ab)^{-1}a)=e-ba+(e-ba)b(e-ab)^{-1}a=e-ab+(b-bab)(e-ab)^{-1}a=e-ba+ba=e$，从而是右逆. 而进一步 $(e+b(e-ab)^{-1}a)(e-ba)=e-ba+b(e-ab)^{-1}(a-aba)=e-ba+ba=e$，从而为左逆，因此为逆元，即 $e-ba$ 可逆. ♣

Remark. 本题的逆元是如何得到的呢？简单的来讲，可以很“粗糙”的做下面这样的分析：

$$\frac{1}{e-ba}=e+ba+ba\cdot ba+\cdots=e+b(e+ab+\cdots)a=e+b(e-ab)^{-1}a.$$

我们可以借助这个形式上的幂级数展开去猜测出逆元，那么我们所需要的工作就是验证这个确实是逆元，这个就是所谓的 Jacobson 引理，可以理解为“过河拆桥”. 当然这种形式上的论断确实有严谨的解释，不过我不懂我也就不乱说了 (.

16.证明 显然 $(a-b^{-1})^{-1}=[(ab-e)b^{-1}]^{-1}=b(ab-e)^{-1}$，从而反过来验证是容易的. 而 $[(a-b^{-1})-a^{-1}](aba-a)=[b(ab-e)^{-1}-a^{-1}](ab-e)a=ba-(ba-e)=e$，从而可知 $(a-b^{-1})-a^{-1}$ 也可逆，且逆元为 $aba-a$. ♣

17.证明 我们给出一个“构造性”的证明，主要利用了 $e-uv+v$ 这种结构.

设 $X=\{x\in R|ax=e\}$，则 $|X|\geq 2$，若 X 为有限集，不妨设为 $X=\{x_1,x_2,\cdots,x_n\}$，从而我们考虑 $y_i=e-x_ia+x_1$，因此有 $ay_i=a-ax_ia+ax_1=e$，从而 $y_1,\cdots,y_n$ 也为 a 的右逆

元，若 $y_i = y_j$，则 $x_i a = x_j a$，进而 $x_i = x_i a x_i = x_j a x_i = x_j$，因此可知 $y_1, \cdots, y_n$ 为 X 的一个置换，因此存在 $y_i = e - x_i a + x_1 = x_1$，即 $x_i a = e$，从而 x_i 为 a 的逆元，因此 $|X| = 1$，矛盾，综上可知 X 为无限集. ♣

Remark. 本质上采用的思路就是，若有 x_1, x_2 为不同的右逆元，则可考虑 $e - x_1 a + x_2$，$e - x_2 a + x_2$ 等结构，就可以构做出许多右逆元.

2.2 理想与商环

2.2.1 Notes

这一节主要研究环的子体系和商体系：

定理 2.2.1: 判断子环的充要条件

设 R 为环，R_1 为 R 的非空子集，则 R_1 为 R 的子环的充要条件为对任何 $a,b\in R_1$，有 $a-b\in R_1$，$ab\in R_1$.

证明 核心就在于 $a-b\in R_1$ 刻画了加法子群，$ab\in R_1$ 刻画了乘法封闭性. ♣

利用加法自然可以定义出商集，但仅满足加法下，一般也满足不了乘法，比如

命题 2.2.1: 商集上自然定义的乘法不一定合理

存在 R_1 为 R 的子环，$a,b,a',b'\in R$ 在商群 R/R_1 上 $a+R_1=a'+R_1$，$b+R_1=b'+R_1$，但是 $ab+R_1\neq a'b'+R_1$.

解 考虑 $R=C(\mathbb{R})$，$R_1=C^\infty(\mathbb{R})$，从而考虑 $a=x+x\sin\dfrac{1}{x}$，$a'=x\sin\dfrac{1}{x}$，$b=x^2+x\sin\dfrac{1}{x}$，$b'=x\sin\dfrac{1}{x}$，则容易看见这是一个反例. ♠

因此为了使得上述乘法定义合理，我们需要给子环增加一些限制条件：

定义 2.2.1: 理想

设 R 为环，I 为 R 的子环，如果 I 满足条件 “$a\in I,x\in R$ 有 $xa\in I$”，则称 I 为 R 的**左理想**；如果 I 满足条件 “$a\in I,x\in R$ 有 $ax\in I$”，则称 I 为 R 的**右理想**. 若一个子环既是左理想，又是右理想，则称为**双边理想**.

我们沿用 F.H Zhu 的书上的约定，以后理想均指双边理想，但是一般情况下左理想和右理想也不一定相等，比如

命题 2.2.2

存在环 R 的子环 I，使得 I 是左理想而不是右理想；同样存在环 R 的子环 I，使得 I 是右理想而不是左理想.

解 我们考虑所有二阶矩阵构成的环 $M_2(\mathbb{R})$，从而易见形如 $\begin{pmatrix}a&0\\b&0\end{pmatrix}$ 的二阶矩阵全体构成一个左理想，且不难验证其不为右理想，同样的，$\begin{pmatrix}a&b\\0&0\end{pmatrix}$ 为右理想，不为左理想. ♠

验证环 R 的理想只需验证加法子群与左右吸收律两个条件：

定理 2.2.2: 理想的判别方法

设 R 为环，I 为 R 的非空子集，则 I 为 R 的**理想**的充分必要条件为 $a-b\in I, ax, ya\in I$，对任意 $a,b\in I, x,y\in R$.

为了给出一般的构造理想的方法，我们先不加证明的给出一个引理：

引理 2.2.1 (任意多个理想的交仍为理想).

若 $\{I_\lambda\}_{\lambda\in\Lambda}$ 是环 R 的理想，则有 $\bigcap\limits_{\lambda\in\Lambda} I_\lambda$ 是 R 的理想.

现在设 S 为环 R 的非空子集，则 R 中所有包含 S 的理想之交仍为 R 的理想，称为由 S **生成的理想**，记为 $\langle S\rangle$. 从而我们容易验证这是环 R 中包含 S 的最小理想，其思想可以类比一组基张成的线性空间，下面是一个具体例子：

例 2.2.2 (交换幺环中的特例).

设 R 为交换幺环，则对任一子集 S，我们有 S 生成的理想为

$$\langle S\rangle=\left\{\sum_{i=1}^{n} r_is_i\middle| n\in\mathbb{N}, r_i\in R, s_i\in S, i=1,2,\cdots,n\right\}.$$

证明 我们将上式右边的集合记为 I，从而显然 $S\subseteq I$，又注意到交换性，故 I 满足吸收律，从而可知 I 为包含 S 的理想，进一步对任意包含 S 的理想 I_1，有 $r_is_i\in I_1$，从而 $\sum r_is_i\in I_1$，即 $I\subseteq I_1$，故 I 为包含 S 的最小理想，即证. ♣

定义 2.2.2: 主理想与生成元

设 I 为环 R 的理想，如果存在 $a\in I$，使得 $I=\langle a\rangle$，则称 I 为**主理想**，而 a 称为 I 的一个**生成元**.

例 2.2.3 (特殊环上的主理想).

- 若 R 为幺环，则
$$\langle a\rangle=\left\{\sum_{i=1}^{m} x_iay_i\middle| x_i,y_i\in R, i=1,2,\cdots,m, m\in\mathbb{N}\right\};$$
- 若 R 为交换环，则
$$\langle a\rangle=\{ra+na|r\in R, n\in\mathbb{Z}\};$$
- 若 R 为交换幺环，则
$$\langle a\rangle=\{ra|r\in R\};$$

- 若 R 为环，则

$$\langle a\rangle=\left\{\sum_{i=1}^{m}x_iay_i+ra+as+na\middle|x_i,y_i,r,s\in R,1\le i\le m,n\in\mathbb{Z}\right\}.$$

证明 我们仅证明最一般的情形，即 R 为环时，将上式右边集合记为 I，则容易证明任意 $x,y\in I$，有 $x-y\in I$，且任意 $r\in R$，$rx,xy\in I$，故 I 为包含 a 的理想，且对任意包含 a 的理想 I_1，有 $x_iay_i\in I_1$，且 $ra,as\in I_1$，又注意到不一定是幺环，从而 $na\in I_1$，故综上 $I\subseteq I_1$，即 I 为包含 a 的最小理想，即证. ♣

定义 2.2.3: 商环

设 R 为一个环，I 是 R 的理想. 考虑加法群 $\{R:+\}$ 对于子群 I 的商群 $R\setminus I$，将 a 所在的等价类记为 $a+I$. 则可以在 $R\setminus I$ 上定义乘法：

$$(a+I)(b+I)=ab+I,$$

则集合 $R\setminus I$ 对于商群的加法以及上述乘法运算构成一个环，称为 R 对于理想 I 的**商环**.

Remark. 理想可以看作群中正规子群对应商群的类比.

定义 2.2.4: 单位群与单位

设 R 为幺环，将 $R^*=R\setminus\{0\}$ 中可逆元素的集合记为 U，则 U 构成一个群，称为 R 的**单位群**，U 中的元素称为 R 中的**单位**.

定义 2.2.5: 整环，除环，体与域

- 无零因子的交换幺环称为**整环**；
- 若一个幺环 R 满足 $R^*=U$，即 R^* 关于乘法构成群，则称 R 为**除环**；

(1) 不交换的除环称为**体**； (2) 交换的除环称为**域**.

例 2.2.4 (不是数域的域).

我们考虑模 p 的剩余环 $\mathbb{Z}_p$，其中 p 为素数，则可知

$$\mathbb{Z}_p=\left\{\overline{0},\overline{1},\cdots,\overline{p-1}\right\}.$$

从而我们利用 Bezout 定理容易证明 $\mathbb{Z}_p^*$ 构成 Abel 群，故为域，但显然不包含 $\mathbb{Q}$(元素有限)，故不为数域.

2.2.2 Exercises From Z.Fh

1.证明 (1) 注意到任意 $\frac{a_1}{b_1},\frac{a_2}{b_2}\in S$，有 $\frac{a_1}{b_1}-\frac{a_2}{b_2}=\frac{a_1b_2-a_2b_1}{b_1b_2}$，则由 $(2,b_1b_2)=1$，从而约分后仍有 $2\nmid b'$，即仍在 S 中，且注意到关于乘法封闭，故 S 构成子环.

但显然对 $\frac{1}{2}\in\mathbb{Q}$，有 $\frac{1}{2}\cdot s\notin S$，对任意 $s\in S$ 且 $s\neq 0$，故 S 不构成理想.

(2) 对任意 $2^{n_1}\cdot m_1$ 与 $2^{n_2}\cdot m_2$，不妨 $n_1\leq n_2$，则有 $2^{n_1}\cdot m_1-2^{n_2}\cdot m_2=2^{n_1}(m_1-2^{n_2-n_1}\cdot m_2)\in S$，且满足乘法封闭性，从而构成子环.

又注意到，对 $s=\frac{1}{3}$，有 $r=2^n$ 使得 $sr\notin S$，故不为理想.

(3) 显然 S 为全体二阶反对称矩阵，关于乘法不一定封闭，即不构成子环.

(4) 显然构成子环，但注意到对 $\boldsymbol{I}_2\in S$，显然任意 $\boldsymbol{A}$，不一定有 $\boldsymbol{AI}_2\in S$，即不构成理想.

(5) 是子环但不是理想，证明 trivial.

(6) 显然关于减法封闭，且注意到 $a_1a_2=\left(n_1\cdot\frac{m}{k}\right)\left(n_2\cdot\frac{m}{k}\right)=\overline{\left(n_1n_2\frac{m}{k}\right)}\frac{m}{k}\in S$，故关于乘法封闭，从而构成子环.

从而对任意 $r\in R=\mathbb{Z}_m$，设 $r\equiv r'(\mathrm{mod}\ k)$，则有 $rS=r'S\subseteq S$，故为理想. ♣

2.证明 证明见例 2.2.5 下方. ♣

3.解 若商环 $R\setminus I$ 为无零因子环，即有下面断言恒成立：

$$(a+I)(b+I)=ab+I=I\Rightarrow a+I=I\text{或}b+I=I,$$

即 $ab\in I$ 蕴含 $a\in I$ 或 $b\in I$，对任意无零因子环 R 上的元素 a,b. 而事实上，对于合数 $m=m_1m_2$，考虑 $\mathbb{Z}$ 的理想 $I=m\mathbb{Z}$，则注意到 $m_1,m_2\notin R$，但显然 $m_1m_2=m\in I$，且 $\mathbb{Z}$ 为无零因子环，故上述断言并不恒成立. ♠

4.证明 设 $a\in I$，$b\in J$ 且非零，则显然有 $\langle a\rangle\subseteq I$，$\langle b\rangle\subseteq J$，则又由 $a,b\in R$，故 $ab\in\langle a\rangle\subseteq I$，同理 $ab\in J$，故 $ab\in I\bigcap J$，又 R 为整环，从而无零因子，故 $ab\neq 0$，从而可知 $I\bigcap J\neq\{0\}$. ♣

5.证明 设 R 为无零因子交换幺环，从而对任意 $r\in R$ 且 $r\neq 0$，考虑 $r,r^2,\cdots$，则由为有限整环，从而一定存在 $k<l\in\mathbb{N}$ 使得 $r^k=r^l$，从而由无零因子，可知 $r^{l-k}=e$，即 r 可逆，从而可知 R^* 均可逆，即有 R 为域，即证. ♣

6.证明 若 R 只有有限个理想，从而存在有限个左理想，进而设由 a 生成的左理想记为 $\langle a\rangle$，则由有限可知 $\langle a\rangle$，$\left\langle a^2\right\rangle$，$\cdots$，$\langle a^m\rangle$，$\cdots$ 有限，从而存在 m 使得 $\langle a^m\rangle=\left\langle a^{m+1}\right\rangle$，又 $\left\langle a^{m+1}\right\rangle=\{ra^{m+1}+na^{m+1}|r\in R,n\in\mathbb{Z}\}$，从而存在 $r\in R$ 使得 $a^m=ra^{m+1}+na^{m+1}$，由无零因子，从而 $a=ra^2+na^2$，左乘 a，即 $a^2=ara^2+na^3$，右除 a，即 $a=ara+na^2$，故有 $ara=ra^2$，从而 $ar=ra$.

对任意 $b\in R$，有 $ba=b(ra^2+na^2)$，消去 a 即 $b=b(ra+na)$，有 $ab=(ra^2+na^2)b$，消去 a 即 $b=(ra+na)b$，从而 $e:=ra+na$ 为 R 的幺元，从而 $(r+ne)a=e$，故 a 可逆，进而对 R^* 中任意元素做类似讨论，可知均可逆，综上即证 R^* 为群，从而 R 为除环. ♣

7.解 (1)Gauss 整数环为 $\mathbb{Z}[\sqrt{-1}]=\{a+b\sqrt{-1}|a,b\in\mathbb{Z}\}$，则设 $a+b\sqrt{-1}$ 可逆，则可知其逆元为其共轭，即有 $(a+b\sqrt{-1})(a-b\sqrt{-1})=a^2+b^2=1$，又 $a,b\in\mathbb{Z}$，从而单位群为 $\{1,-1,\sqrt{-1},-\sqrt{-1}\}$；

(2) 我们直接对一般的 m 分析，若 $\overline{k}\in\mathbb{Z}_m$ 可逆，即有 $\overline{k'}\in\mathbb{Z}_m$ 使得 $\overline{k'}\cdot\overline{k}=1$，也即存在整数 q 使得 $k'k+qm=1$，由 Bezout 定理可知 $\gcd(k,m)=1$，从而可知 $\mathbb{Z}_m$ 的单位群为 $\{\overline{k}|\gcd(k,m)=1\}$.

利用这个结论我们可知 $U(Z_7)=\{\overline{1},\cdots,\overline{6}\}$;

(3) 仍然利用结论我们有 $U(Z_{24})=\{\overline{1},\overline{5},\overline{7},\overline{11},\overline{13},\overline{17},\overline{19},\overline{23}\}$. ♠

8.证明 设 I 为 $\mathbb{P}^{n\times n}$ 的理想，且含非零元 $\boldsymbol{A}$，从而存在 $a_{ij}\neq 0$，因此有 $\boldsymbol{E}_{ii}\boldsymbol{A}\boldsymbol{E}_{jj}=a_{ij}\boldsymbol{E}_{ij}\in I$，进而 $\boldsymbol{E}_{ij}\in I$，从而任意 $\boldsymbol{E}_{kl}=\boldsymbol{E}_{ki}\boldsymbol{E}_{ij}\boldsymbol{E}_{jl}\in I$，进而可知任意 $\boldsymbol{B}=\sum b_{ij}\boldsymbol{E}_{ij}\in I$，进而可知 $I=\mathbb{P}^{n\times n}$，从而可知没有非平凡理想. ♣

9.证明 为证明其为除环，只需证明 R^* 为群，又其为有限半群，从而只需证方程 $xa=b$，$ax=b$ 总有解，而任意 $a,b\in R^*$，由 R 无零因子，从而 $aR^*=R^*$，则存在 x 使得 $ax=b$，同理 $xa=b$ 也有解，综上可知 R^* 为群，进而其为除环. ♣

10.证明 任意 $u\in U$，$a\in U_I$，存在 $r\in I$ 使得 $a=e+r$，则 $u^{-1}au=u^{-1}ru+e\in I$，从而 $U_I\lhd U$，即证. ♣

11.证明 我们先证明 $\sqrt{I}$ 为 R 的理想，一方面若 $a\in\sqrt{I}$，$x\in R$，若 $a^n\in I$，则由 R 为交换环，从而 $(xa)^n=x^na^n\in I$，$(ax)^n=a^nx^n\in I$，从而 $ax,xa\in I$，另一方面，任意 $a,b\in\sqrt{I}$，且 $a^n\in I$，$b^m\in I$，则

$$(a-b)^{m+n}=\sum_{k=0}^{m+n}\mathrm{C}_{m+n}^k a^k b^{m+n-k},$$

则对任意 a^sb^t, $s+t=m+n$, $s<n$ 和 $t<m$ 一定不同时成立, 因此 $a^sb^t\in I$, 因此 $(a-b)^{m+n}\in I$, 进而 $a-b\in\sqrt{I}$，从而可知 $\sqrt{I}$ 为 R 的理想.

下面证明 $\sqrt{\sqrt{I}}=\sqrt{I}$，不难注意到 $\sqrt{I}\subseteq\sqrt{\sqrt{I}}$，另一方面，若 $a\in\sqrt{\sqrt{I}}$，则存在 $n\in\mathbb{N}$ 使得 $a^n\in\sqrt{I}$，从而存在 $m\in\mathbb{N}$ 使得 $(a^n)^m\in I$，进而存在 $mn\in\mathbb{N}$ 使得 $a^{mn}\in I$，从而 $a\in\sqrt{I}$，因此 $\sqrt{\sqrt{I}}\subseteq\sqrt{I}$，综上有 $\sqrt{\sqrt{I}}=\sqrt{I}$，即证. ♣

12.证明 设 $a+\mathrm{Rad}R$ 为 $\mathrm{Rad}R$ 的幂零根基，即存在 $n\in\mathbb{N}$ 使得 $(a+\mathrm{Rad}R)^n=0+\mathrm{Rad}R$，又由 Rad 为理想，从而 $a^n+\mathrm{Rad}R=0+\mathrm{Rad}R$，即 $a^n\in\mathrm{Rad}R$，从而存在 m 使得 $a^{mn}=0$，故 $a\in\mathrm{Rad}R$，故可知 $a+\mathrm{Rad}R=\mathrm{Rad}R$，进而没有非零的幂零根基. ♣

13.证明 (1) 注意到 $a\circ(b\circ c)=a\circ(b+c-bc)=a+b+c-bc-ab-ac+abc=(a\circ b)\circ c$，从而可知满足结合律，且 $0\circ a=a$ 是平凡的.

(2) 若 R 为域，从而 R^* 为 Abel 群，从而由 R 关于 $\circ$ 满足结合律与封闭性可知构成半群，又 $0\circ a=a\circ 0=a$，从而 0 为 $R-\{e\}$ 的幺元，另一方面，由 $e\notin R-\{e\}$，从而 $a-e\in R^*$ 可逆，从而任意 $a\in R-\{e\}$，有 $a\circ a(a-e)^{-1}=a+a(a-e)^{-1}-a^2(a-e)^{-1}=a+a(a-e)^{-1}-a(a-e)^{-1}(a-e)-a(a-e)^{-1}=e$，从而可知 $\{R-\{e\},\circ\}$ 中元素可逆，从而构成交换群.

另一方面，若 $\{R-\{e\},\circ\}$ 构成交换群，从而为了证明 R 为域，我们只需证明 R^* 中元素均可逆，注意到设 $(a+e)\circ c=0$，从而 $a+e+c-ac-c=0$，即 $a+e-ac=0$，从而 $a(c-e)=e$，故可知任意 $a\in R^*$，由 $a+e\neq e$，进而其可逆，也即证明 R^* 为交换群，从而 R 为域. ♣

14.证明 这里我们沿用上一题的记号.

显然 0 为一个右逆正则元，下设 R 中只有 a 不为非右逆正则元，我们希望证明 a 为幺元:

Step 1. 若存在 $c\in R$ 使得 $a\circ c\neq a$，从而其为右逆正则元，进而存在 b 使得 $(a\circ c)\circ b=0$，由结

合律, 进而 $a\circ(c\circ b)=0$, 这与 a 不为右逆正则元矛盾! 从而可知 $a\circ c=a$, 这表明 $a=a+c-ac$, 从而 $ac=a$, 即 a 为左幺元.

Step 2. 若存在 $b\in R$ 使得 $b\circ a\neq a$, 即其右逆正则, 故存在 c 使得 $0=(b\circ a)\circ c=b\circ(a\circ c)=b\circ a$, 即 $b+a-ba=0$, 则 $ba+a^2-ba^2=0$, 即 $ba+a-ba=0$, 从而 $a=0$, 矛盾, 进而 $b\circ a=a$, 也即 $ba=b$, 故有 a 为右幺元.

Step 3. 我们再证明任意 $b\in R^*$, 有逆元, 由 $b\neq 0$ 时, $b+e\neq e$, 从而 $b+e$ 为右逆正则元, 即存在 c 使得 $(b+e)\circ c=0$, 故 $b+e-bc=0$, 故 $e=b(c-e)$, 从而 R^* 中任意元均存在右逆元.

综上 R^* 为半群且有右逆元与右幺元, 进而可知 R^* 为群, 从而 R 为除环, 即证. ♣

2.3 四元数体

2.3.1 Notes

定义 2.3.1: Hamilton 四元数体

考虑 $\mathbb{C}^{2\times 2}$ 中的子集

$$\mathbb{H}=\left\{\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}\middle|\alpha,\beta\in\mathbb{C}\right\}.$$

容易验证 $\mathbb{H}$ 构成二阶复矩阵环的子环，且每个非零元素均可逆，且存在幺元，故 $\mathbb{H}^*$ 构成群，但同时容易看出不满足交换性，也即是非交换的除环，我们称为**四元数体**.

四元数体具有数的交换性以外的所有性质，所以可以在其上发展出更广泛的数学体系.

值得一提的是，四元数体之所以叫做“四元”，正是可以依赖于 $\mathbb{H}$ 可以被四个单位所表达，如果我们记

$$\mathbf{1}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad \boldsymbol{i}=\begin{pmatrix}\sqrt{-1} & 0\\ 0 & -\sqrt{-1}\end{pmatrix},\quad \boldsymbol{j}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\quad \boldsymbol{k}=\begin{pmatrix}0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{pmatrix}.$$

则对于任意 $\alpha=a+b\sqrt{-1},\beta=c+d\sqrt{-1}$，有

$$\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}=a\mathbf{1}+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k}.$$

定义 2.3.2: 可除代数

若实数域上的线性空间 $\mathcal{A}$ 上可以定义乘法，满足结合律，且每个非零元素可逆，则称这样的 $\mathcal{A}$ 称为实数域上的**可除代数**.

实数域上的可除代数只有 $\mathbb{R}$，$\mathbb{C}$，$\mathbb{H}$ 三种.

2.3.2 Exercises From Z.Fh

1.证明 任意 $a,b\in C(R)$，有 $(a-b)c=c(a-b)$，$abc=acb=cab$，从而 $a-b,ab\in C(R)$，则 $C(R)$ 为子环，若取 R 为所有上三角矩阵，从而 $C(R)$ 为全体数量矩阵，从而显然不满足吸收律，不为 R 的理想. ♣

2.证明 设 R 为除环，即 R^* 为群，从而由 $C(R)$ 为 R 的子环，则 $C(R)^*$ 为 R^* 的子群，且交换是显然的，进而 $C(R)^*$ 为 Abel 群，故 $C(R)$ 为域.

设 $a\mathbf{1}+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k}\in C(\mathbb{H})$，则由 $\boldsymbol{i}(a\mathbf{1}+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k})=(a\mathbf{1}+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k})\boldsymbol{i}$，这即有 $a\boldsymbol{i}-b\mathbf{1}+c\boldsymbol{k}-d\boldsymbol{j}=a\boldsymbol{i}-b\mathbf{1}-c\boldsymbol{k}+d\boldsymbol{j}$，从而 $c=d=0$，同理与 $\boldsymbol{j}$ 可交换即 $b=d=0$，从而 $C(\mathbb{H})\subseteq\{a\mathbf{1}|a\in\mathbb{R}\}$，又不难验证后者与所有元素可交换，进而可知 $C(\mathbb{H})=\{a\mathbf{1}|a\in\mathbb{R}\}$. ♣

3.证明 直接证明不难，略去，共轭在矩阵表示下即共轭转置 (Hermite 转置). ♣

4.证明 直接利用 $N(x)=a^2+b^2+c^2+d^2$ 逐个验证即可. ♣

5.证明 事实上 $T(x)=x+\overline{x}$，则有 $x^2-T(x)x+N(x)=x^2-(x+\overline{x})x+x\overline{x}=0$. ♣

6.证明 由 Carten-Brauer-华罗庚定理可知成立 (bushi，直接从 $\mathbb{H}$ 出发需要讨论很长，略去. ♣

7.证明 注意到任意 $x,y\in \mathrm{Sp}(1)$，则 $N(x)=x\bar{x}=N(y)=y\bar{y}=1$，则 $N(y^{-1})=y^{-1}\overline{y^{-1}}=\bar{y}y=1$，故 $N(xy^{-1})=N(x)N(y^{-1})=1$，则 $xy^{-1}\in \mathrm{Sp}(1)$，即构成群. ♣

8.证明 对任意 $x=a\mathbf{1}+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k}\in \mathrm{Sp}(1)$，考虑映射 $f:\mathrm{Sp}(1)\to \mathrm{SU}(2)$，

$$a\mathbf{1}+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k}\mapsto \begin{pmatrix} a+b\sqrt{-1} & c+d\sqrt{-1} \\ -c+d\sqrt{-1} & a-b\sqrt{-1} \end{pmatrix},$$

一方面容易验证这是单的群同态，下面验证这是满射，任意 $\boldsymbol{A}\in \mathrm{SU}(2)$，设 $\boldsymbol{A}=\begin{pmatrix} x & y \\ z & w \end{pmatrix}$，则 $|x|^2+|y|^2=|z|^2+|w|^2=1$，$x\bar{z}+y\bar{w}=z\bar{x}+w\bar{y}=0$，$xw-yz=1$，进而 $\bar{w}=\bar{w}(xw-yz)=x\cdot|w|^2-z(-x\bar{z})=x(|w|^2+|z|^2)=x$，故 $x=\bar{w}$，同理 $y=-\bar{z}$，即证 $\boldsymbol{A}\in \mathrm{Sp}(1)$，综上我们证明了 $\mathrm{Sp}(1)$ 同构于 $\mathrm{SU}(2)$. ♣

注：容易证明 $\mathrm{Sp}(1)\cong S^3$，即三维球面，从而可利用 $\mathrm{Sp}(1)\hookrightarrow \mathbb{R}^4$ 上赋予子空间拓扑，故不难证明 $\mathrm{Sp}(1)$ 是一个拓扑群，进而表明可在拓扑空间 S^3 上可以赋予群结构. 但除此之外，在 n 维球面 S^n 中，只有 S^1 和 S^3 上可以赋予拓扑群结构.

9.证明 不存在三维的实数域可除代数不会，只会不存在三元数，求佬浇浇.

假设三元数存在，那么其形式一定是 $a+b\mathrm{i}+c\mathrm{j}$，其中 $a,b,c\in\mathbb{R}$，且 $\mathrm{i}^2=\mathrm{j}^2=-1$. 由乘法的封闭性，有 $\mathrm{ij}=x+y\mathrm{i}+z\mathrm{j}$，其中 $x,y,z\in\mathbb{R}$. 当 $z\neq 0$ 时，移项并除以 z 可得 $\mathrm{j}=\frac{1}{z}(\mathrm{ij}-x-y\mathrm{i})$，两边左乘 i，有 $\mathrm{ij}=\frac{1}{z}(-\mathrm{j}-x\mathrm{i}+y)$. 比较 j 的系数可得 $z=-\frac{1}{z}$，即 $z^2=-1$，这与 $z\in\mathbb{R}$ 矛盾. 当 $z=0$ 时，可得 $\mathrm{ij}=x+y\mathrm{i}$，两边左乘 i，有 $-\mathrm{j}=a\mathrm{i}-b$，这表明 $\mathrm{j}\in\mathbb{C}$，矛盾. ♣

2.3.3 除环的正规子除环

我们这一节讨论华罗庚先生对下面定理的证明

定理 2.3.1: Carten-Brauer-华罗庚定理

一个 D 的子环 $S\subseteq D$ 称为**正规的**，若任意 $x\in S,y\in D^*$，有 $yxy^{-1}\in S$，则若 S 是正规子除环，则 $S=D$ 或 $S\subseteq C(D)$.

我们先依次证明若干引理：

引理 2.3.1 (华罗庚). *若 $a,b\in D$ 且 $ab\neq ba$，则有*

$$a=(b^{-1}-(a-1)^{-1}b^{-1}(a-1))(a^{-1}b^{-1}a-(a-1)^{-1}b^{-1}(a-1))^{-1}.$$

证明 由 $ab \neq ba$，从而 $a, b \neq 0, 1$，故 $a, b, a-1, b-1$ 可逆，一方面注意到 $a(a^{-1}b^{-1}a - (a-1)^{-1}b^{-1}(a-1)) = b^{-1}a - a(a-1)^{-1}b^{-1}(a-1) = b^{-1}a - b^{-1}(a-1) - (a-1)^{-1}b^{-1}(a-1) = b^{-1} - (a-1)^{-1}b^{-1}(a-1)$，另一方面，若 $a^{-1}b^{-1}a - (a-1)^{-1}b^{-1}(a-1)$ 不可逆，则 $a^{-1}b^{-1}a = (a-1)^{-1}b^{-1}(a-1)$，即 $(a-1)a^{-1}b^{-1}a = b^{-1}a - b^{-1}$ 也即 $a^{-1}b^{-1}a = b^{-1}$，从而 $ab = ba$ 矛盾，故 $a^{-1}b^{-1}a - (a-1)^{-1}b^{-1}(a-1)$ 可逆，综上即证. ♣

引理 2.3.2 (华罗庚). *设 S 是正规子除环. 证明：对任何 $a \in D - S$，$b \in S^*$ 有 $ab = ba$.*

证明 反证法，若 $ab \neq ba$，则显然 $a \neq 1, 0$，即 $a, a-1 \in S^*$，结合 $b \in S^*$，从而 $a = (b^{-1} - (a-1)^{-1}b^{-1}(a-1))(a^{-1}b^{-1}a - (a-1)^{-1}b^{-1}(a-1))^{-1} \in S$，矛盾. ♣

利用上面两个引理，我们就不难完成定理 2.3.1 之证明：

证明 若 $S = D$，则命题已成立，若不然，从而 S 中元素均与 $D - S$ 中元素可交换，进而任意 $b, b' \in S$，若 $bb' \neq b'b$，则由 $ab \notin S$，故 $(ab)b' = b'ab = b'ba$，由消去律则 $bb' = b'b$，即矛盾，故可知 S 中元素与 S 可换，故 $S \subseteq C(D)$，即证. ♣

注：这是华罗庚先生的原论文PDF.

2.4 环的同态

2.4.1 Notes

定义 2.4.1: 环的同态

如果映射 $f: R_1 \to R_2$，且 f 保持加法和乘法，则称其为环的同态.

定理 2.4.1: 同态核是理想 (类比同态核是正规子群)

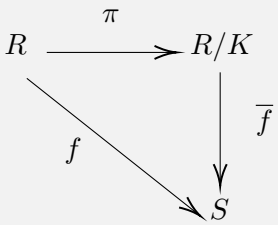
环同态 $f: R_1 \to R_2$，则 $\mathrm{Ker}f$ 为 R_1 的理想.

证明 设 $f(a) = f(b) = 0$，则 $f(a-b) = 0$，任意 $r \in R$，则 $f(ax) = f(a)f(x) = 0 = f(xa)$，从而 ax，$xa \in \mathrm{Ker}f$，进而可知 $\mathrm{Ker}f$ 为环 R 的理想. ♣

定理 2.4.2: 环的同态基本定理

设 f 是环 R 到环 S 的满同态，记 $K = \mathrm{Ker}f$，则有

1. 设 π 为 R 到 R/K 的自然同态，则存在商环 R/K 到环 S 的同构 $\overline{f}$，使得 $f = \overline{f} \circ \pi$，即有交换图



2. f 建立了 R 中包含 K 的子环与 S 的子环之间的一一对应，且将理想对应到理想；

3. 如果 I 是 R 的理想，且包含 K，则有 $R/I \cong S/f(I)$.

证明 (1) 我们考虑定义 $\overline{f}: R/K \to S$，$r + K \mapsto f(r)$，下面证明这是一个同构.

由加法群的同态基本定理，可知 $\overline{f}$ 关于加法是同构，下面只需证明 $\overline{f}$ 保持乘法 (因为加法群中的同构已经保证了 f 为双射)，而又注意到 $\overline{f}((a+K)(b+K)) = \overline{f\pi(a)\pi(b)} = \overline{f}(\pi(ab)) = f(ab) = f(a)f(b) = \overline{f}(a+K)\overline{f}(b+K)$.

(2) 事实上，我们只需要按照定义去依次验证：f 把子环映到子环，S 中的子环的完全原像是 R 中包含 K 的子环，由这两条，我们就不难得到第一条断言.

我们再只需验证：f 把理想映到理想，S 中的理想的完全原像就是 R 中包含 K 的理想，便不难证明第二条断言. 事实上这部分证明的核心在于，S 中的子环 (理想) 一一对应的是其完全原像，借助这个基本的观察，就不难证明.

(3) 我们在第一问的结果支持下，我们只需构做一个满的 $f':R\to S/f(I)$，而且 $\mathrm{Ker}f'=I$，而我们不难发现，设 $\pi'=S\to S/f(I)$ 的自然同态，我们就断言 $f'=\pi\circ f$ 即为所求.

我们只需验证 $\ker f'=I$，如果 $r\in R$ 且 $f'(r)=0+f(I)$，即 $0+f(I)=f(r)+f(I)$，即 $f(r)\in f(I)$，这就表明 $r\in I$(这是因为 $f(I)$ 和 R 中包含 K 的理想有一一对应，而 I 对应的是 $f(I)$)，由此 $\ker f'=I$. ♣

命题 2.4.1: 两个理想的并不一定是理想

我们熟知有限个理想的和仍为理想，但是两个理想的并却不一定是理想，若其为理想，则充分必要条件为 I_1 与 I_2 之间有包含关系.

证明 反例是容易的，我们考虑 $\mathbb{Z}$ 的两个理想 $2\mathbb{Z}$ 和 $3\mathbb{Z}$，那么若 $2\mathbb{Z}\cup 3\mathbb{Z}$ 是理想，则设其为 $n\mathbb{Z}$，则 $n|2,3$ 即 $n=1$，但显然 $2\mathbb{Z}\cup 3\mathbb{Z}\neq\mathbb{Z}$，矛盾!

事实上我们可以证明两个群的并仍为群的充要条件为两群之间存在包含关系，若 G_1 与 G_2 之间无包含关心，则存在 $g_1\in G_1\setminus G_2$，$g_2\in G_2\setminus G_1$，则 $g_1g_2\notin G_1\cup G_2$，矛盾，从而对两个理想其并是子环的充要条件即为两个理想存在包含关系，即证. ♣

定理 2.4.3

设 I,J 为环 R 的理想，则有同构 $(I+J)/I\cong J/(I\cap J)$.

证明 我们利用环的同态基本定理，对任意 $a\in I,b\in J$，考虑 $\varphi:I+J\to J/(I\cap J)$，$a+b\mapsto b+I\cap J$，注意到若 $a+b=a'+b'$，则 $b-b'\in I\cap J$，从而 $b+I\cap J=b'+I\cap J$，即为良定义的，下面验证 $\mathrm{Ker}\varphi=I$，任意 $a+b\in I+J$，若 $\varphi(a+b)=0+I\cap J$，即 $b\in I\cap J$，从而 $a+b\in I$，即证. ♣

定理 2.4.4: 半同态必为同态或反同态

设 f 是 R 到 S 的半同态，那么其要么为同态，要么为反同态.

证明 固定 $a\in R$，考虑 $l_a=\{b\in R|f(ab)=f(a)f(b)\}$，$r_a=\{b\in R|f(ab)=f(b)f(a)\}$，容易证明 l_a 与 r_a 均为 $\{R,+\}$ 的子群，且 $l_a\cup r_a=R$，进而矛盾，因为**群不能写成两个真子群的并**. ♣

2.4.2 Exercises From Z.Fh

1.证明 (1) 由 φ 为满同态，从而任意 $a,b\in R_2$，存在 $a',b'\in R_1$ 使得 $\varphi(a')=a$，$\varphi(b')=b$，则 $ab=\varphi(a')\varphi(b')=\varphi(a'b')=\varphi(b'a')=ba$，即 R_2 为交换环.

(2) 设 R_1 有幺元 e，则对任意 $r\in R_2$，存在 $r'\in R_1$ 使得 $r=f(r')$，则对 $f(e)\in R_2$，有 $rf(e)=f(r'e)=r=f(e)r$，从而 $f(e)$ 为幺元，即证 R_2 为幺环.

(3) 若 R_1 为除环，则 R_1^* 为群，则可知 $\varphi(R_1^*)=R_2^*$ 也为群，即证 R_2 为除环.

(4) 若 R_1^* 为 Abel 群，则由 (2),(3) 可知 $R_2^*=\varphi(R_1^*)$ 为 Abel 群，即证 R_2 为域.

(5)R_2 不一定为整环，如考虑 $R_1=\mathbb{Z}$，取 $R_2=\mathbb{Z}_6$，$\varphi(n)$ 为 n 模 6 的余数，则易见 $\mathbb{Z}$ 为整环，但 $\bar{2}\cdot\bar{3}=\bar{0}$，故 R_2 有零因子，不为整环，从而为一个反例. ♣

2.解 注意到 Ker$\varphi=\{f\in\mathbb{Z}[x]|f(1+\sqrt{2})=0\}$，则 $1+\sqrt{2}$ 为 $f(x)$ 的根，进而 $f(x)$ 有二次因式 x^2-2x-1，从而 $f(x)=(x^2-2x-1)g(x)$，则 Ker$\varphi=\{(x^2-2x-1)g(x)|g(x)\in\mathbb{Z}[x]\}$. ♠

3.证明 设 $f:\mathbb{Z}_p\to\mathbb{Z}_p$，则 $f(0)=0$，设 $f(1)=k\in\{0,1,\cdots,p-1\}$，则 $f(2)=\overline{2k}$，$f(2)=f(1)f(2)=\overline{2k^2}$，即 $2k^2\equiv 2k(\mathrm{mod}\ p)$，则可知 $k=0$ 或 1，故 f 为零同态或恒等同态，即证.

对一般的除环不一定正确，如考虑四元数体，还有自同态 $f(\boldsymbol{i})=\boldsymbol{j},f(\boldsymbol{j})=\boldsymbol{k},f(\boldsymbol{k})=\boldsymbol{i}$，不为零同态和恒等同态. ♣

4.证明 反证法，若 $(R,+)\cong(R^*,\cdot)$，设同构为 f，则 $f(0)=e$，设 $f(a)=-e$，则 $f(a+a)=e$，进而 $2a=0$，若 $a=0$，则 $e=-e$ 即 $2e=0$，若 $a\neq 0$，则 $(2e)a=0$ 即 $2e=0$，综上 $2e=0$，设 $f(e)=b$，则 $e=f(0)=f(2e)=b^2$，则可知 $b=e$ 或 $b=-e=e$，则 $f(0)=f(e)$ 矛盾. ♣

5.证明 由 φ 为满同态，从而其把包含 Kerφ 的子环 (理想) 一一对应到 R 的子环 (理想)，从而存在 $\mathbb{Z}$ 包含 Kerφ 的子环 S 使得其与 R_1 对应，又 $\mathbb{Z}$ 的子环均形如 $m\mathbb{Z}$ 为理想，从而 R_1 为 R 的理想，即证. ♣

6.解 易见 $\mathbb{Q}[\sqrt{-1}]$ 为域，从而设有自同构 f，则 $f(1)=1$，则可知 $f(n)=n$ 对任意 $n\in\mathbb{Z}$，进而 $f\left(\dfrac{q}{p}\right)=\dfrac{q}{p}$，故可设 $f(\sqrt{-1})=c\sqrt{-1}$，则 $f(a+b\sqrt{-1})=f(a)+cf(b)\sqrt{-1}$，故 $f(a-b\sqrt{-1})=f(a)-cf(b)\sqrt{-1}$，且 $f(a^2+b^2)=f^2(a)+c^2f^2(b)=f(a^2+c^2b^2)$，进而 $c^2=1$，又易见当 $c=\pm1$ 时均为同构. 综上自同构为恒等同态或取共轭的同态. ♠

7.证明 类似于上一题，我们可知对任意 $a\in\mathbb{Q}$，均有 $\varphi(a)=a$，且由任意 $x>0$，$\varphi(x)=(\varphi(\sqrt{x}))^2>0$，从而进一步 φ 是单调递增的，进而若有 c 使得 $\varphi(c)\neq c$，那么不妨 $\varphi(c)<c$，那么任取有理数 $d\in(\varphi(c),c)$，则 $d=\varphi(d)<\varphi(c)$ 矛盾！即证. ♣

9.证明 由 R 是特征为 p 的无零因子交换环，从而 $F(a)+F(b)=a^p+b^p=(a+b)^p=F(a+b)$，且 $F(a)F(b)=a^pb^p=(ab)^p=F(ab)$，从而 F 为环同态. 又由 $F(a)-F(b)=(a-b)^p=(a-b)(a-b)^{p-1}=0$，又无零因子，则若 $a-b\neq0$，则 $(a-b)^{p-1}=0$，从而归纳下去可得 $a-b=0$，矛盾，故 $a-b=0$，即 $F(a)=F(b)$ 蕴含 $a=b$，即为单同态.

我们考虑 $\mathbb{Z}_p[x]$，易见其为特征为 p 的交换幺环，且设 $f(x)g(x)=0$，则考虑首项系数可知必有一个多项式为 0，进而无零因子，但显然 $f(x)\mapsto(f(x))^p$ 不为同构，即为一个反例. ♣

10.证明 不难验证 $\mathbb{Z}\times R$ 具有环结构，又注意到对 $(1,0)\in\mathbb{Z}\times R$，其为幺元，进而为幺环. 考虑 $R'=\{(0,a)|a\in R\}\subseteq\mathbb{Z}\times R$，则注意到 $(0,a)-(0,b)=(0,a-b)\in R'$，任意 $(n,b)\in R'$，$(n,b)(0,a)=(0,na+ba)\in R'$，同理 $(0,a)(n,b)\in R'$，故 R' 为 $\mathbb{Z}\times R$ 的理想，显然 $R\cong R'$，综上我们完成了证明. ♣

11.证明 由 $|R|=p$ 为素数，从而 $\{R,+\}$ 为 p 阶循环群，不妨设为 $\{0,a,\cdots,pa\}$，则由 R 无零因子，从而任意 $ka\cdot la\neq0$，故设 $a\cdot a=ka$，则任意 $1\leq l\leq p-1$，$la\cdot a=kla$，则 $k,2k,\cdots,(p-1)k$

模 p 互不同余且不为 0，故设 ks 模 p 余 1，则取 $e=sa$，则任意 $la\cdot sa=sla^2=lska=la=sa\cdot la$，从而为交换幺环，进一步任意 $la\in R$，存在 m 使得 lmk 模 p 余 1，进而 $la\cdot ma=sa$，从而为域，由此不难发现其同构于 $\mathbb{Z}_p$. ♣

12.证明 显然包含 e 的最小子环为 $\{ne|n\in\mathbb{Z}\}$，故根据 e 在加法群中的阶即可证明. ♣

13.解 (1) 是； (2) 是； (3) 不一定是； (4) 不一定是. ♠

14.证明 不难发现若 u 为单位，则 $\varphi(u)\varphi(u^{-1})=\varphi(u^1)\varphi(u)$ 为 R_2 中幺元，故 $\varphi(u)$ 为单位. ♣

15.证明 由 R 为除环，即 R^* 构成群，从而任意非零同态 f，若 $f(a)=f(0)=0$，则若 $a\neq 0$，那么有 $f(e)=f(a\cdot a^{-1})=f(a)f(a^{-1})=0$，进而表明 f 为零同态，矛盾，故 $a=0$，进而说明 f 为单同态，即证. ♣

16.证明 我们先证明 $\{R;\oplus,\cdot\}$ 为交换幺环：关于加法 $\oplus$，结合律、交换性与封闭性是自然的，有零元 -1，任意 a 有负元 $-2-a$，从而构成 Abel 群，关于乘法，结合律、交换性与封闭性也是自然的，且有幺元 0，综上即证 $\{R;\oplus,\cdot\}$ 为交换幺环.

考虑 $\varphi:\{R;+,\cdot\}\to\{R;\oplus,\cdot\}$，$a\mapsto a-1$，则易见这为双射，且有 $\varphi(a)\oplus\varphi(b)=(a-1)\oplus(b-1)=a+b-1=\varphi(a+b)$，保持加法，$\varphi(a)\cdot\varphi(b)=(a-1)\cdot(b-1)=a-1+b-1+(a-1)(b-1)=ab-1=\varphi(ab)$，也保持乘法，综上可知 φ 为环同构，即证. ♣

17.证明 显然作为加法群均同构于 $\mathbb{Z}$，因此同构；作为环，若有同构 φ，则其关于加法是同构，进而 $\varphi(km_1)=km_2$，对任意 $k\in\mathbb{Z}$，则关于乘法 $\varphi(m_1^2)=m_1m_2\neq m_2^2=\varphi(m_1)\varphi(m_1)$，因此不保持乘法，故矛盾，也即作为环不同构. ♣

18.证明 首先注意到对任意 $1\leq x\leq p,1\leq y\leq q$，有 $qx+py$ 模 pq 互不同余，这是因为若 $qx+py\equiv qx'+py'(\mathrm{mod}\ pq)$，进而可知 $p|x-x',q|y-y'$ 这即 $x=x',y=y'$，从而存在 a,b 使得 $\overline{qa+pb}=1$，从而我们考虑映射

$$\varphi:\mathbb{Z}_p\oplus\mathbb{Z}_q\to\mathbb{Z}_{pq},\quad (s,t)\mapsto\overline{qas+pbt},$$

这里 $1\leq s\leq p,1\leq t\leq q$，注意到任意 $(s,t),(s',t')$，若 $\varphi(s,t)=\varphi(s',t')$，则 $qas+pbt\equiv qas'+pbt'(\mathrm{mod}\ pq)$，进而可知 $p|a(s-s'),q|b(t-t')$，又 $(a,p)=(b,q)=1$，这即 $s=s',t=t'$，又 $|\mathbb{Z}_p\oplus\mathbb{Z}_q|=|\mathbb{Z}_{pq}|$，从而 φ 是双射，显然保持加法，又 $\varphi(s,t)\varphi(u,v)=\overline{(qas+pbt)(qau+pbv)}=\overline{q^2a^2su+p^2b^2tv}=\overline{qa(1-pb)su+pb(1-qa)tv}=\overline{qasu+pbtv}=\varphi(su,tv)$，进而保持乘法，综上我们可知 φ 是 $\mathbb{Z}_p\oplus\mathbb{Z}_q\to\mathbb{Z}_{pq}$ 的同构，即证.

若 p,q 不互素，则命题不一定正确，如考虑 $p=q=2$，则 $\mathbb{Z}_2\oplus\mathbb{Z}_2$ 的加法群同构于 K_4，显然不同构于 $\mathbb{Z}_4$，进一步也不为环同构. ♣

19.证明 (1) 考虑 $\{R\times R^*,+\}$，则封闭性，结合律与交换性是直接的，且由任意 $(a,b)\in R\times R^*$，有 $(a,b)+(0,1)=(a,b)=(0,1)+(a,b)$，从而关于加法构成交换幺半群.

再考虑 $\{R\times R^*,\cdot\}$，则封闭性，结合律与交换性是直接的，且由任意 $(a,b)\in R\times R^*$，有 $(a,b)(1,1)=(a,b)=(1,1)(a,b)$，从而关于乘法构成交换幺半群.

(2) 注意到 $ab=ba$，从而 $(a,b)\sim(a,b)$，故满足反身性，对称性由交换性是显然的，若

$(a,b)\sim(c,d)$ 且 $(c,d)\sim(e,f)$ 则 $ad=bc$ 且 $cf=de$ 则 $adcf=bcde$，由无零因子与交换性可知 $af=be$，进而 $(a,b)\sim(e,f)$ 即满足传递性，从而 $\sim$ 为等价关系.

又若 $(a,b)\sim(a',b')$ 且 $(c,d)\sim(c',d')$，则 $ab'=a'b$ 且 $cd'=c'd$，进而 $ab'cd'=a'bc'd$ 故 $(ac,bd)\sim(a'c',b'd')$，故关于乘法为同余关系，$(a,b)+(c,d)=(ad+bc,bd)$ 且 $(a',b')+(c',d')=(a'd'+b'c',b'd')$，则注意到 $(ad+bc)b'd'=adb'd'+bcb'd'a'bdd'+bb'c'd=(a'd'+b'c')bd$，进而 $(a,b)+(c,d)\sim(a',b')+(c',d')$，故关于加法也是同余关系.

(3) 在 (1) 中我们已证关于加法，乘法构成交换幺半群，对于加法，任意 $\frac{a}{b}\in F$，则 $\frac{a}{b}+\frac{-a}{b}=\frac{0}{b^2}$，又 $(0,b^2)\sim(0,1)$，则 $\frac{a}{b}+\frac{-a}{b}=\frac{0}{1}$ 故有逆元，从而可知关于加法构成群.

对于乘法，任意 $\frac{a}{b}$，如果 $a\in R^*$，那么显然其有逆元 $\frac{b}{a}$，若 $a=0$，那么 $\frac{0}{b}$ 均代表 F 中的零元，从而可知 F^* 构成了 Abel 群，综上可知 F 为域.

(4) 我们先证明 φ 是同态，任意 $a,b\in R$，$\varphi(a)+\varphi(b)=\frac{a}{1}+\frac{b}{1}=\frac{a+b}{1}=\varphi(a+b)$，故保持加法. 进一步，$\varphi(a)\varphi(b)=\frac{a}{1}\frac{b}{1}=\varphi(ab)$，故保持乘法，即为环同态. 若 $\varphi(a)=\frac{a}{1}=\frac{b}{1}=\varphi(b)$，即有 $\frac{a-b}{1}=\frac{0}{1}$，进而 $(a-b)\cdot 1=0\cdot 1$ 即 $a=b$，从而为单同态.

又任意 $\frac{a}{b}\in F$，则 $b\neq 0$，故显然能找到 $\frac{a}{1}$ 与 $\frac{b}{1}$，使得 $\frac{a}{b}=\frac{a}{1}\frac{1}{b}=\frac{a}{1}\left(\frac{b}{1}\right)^{-1}$，综上即证 F 是 R 的一个分式域.

(5) 注意到 K 是包含 R 的域，从而任意 $b\in R^*$，$ab^{-1}\in K$，那么我们按照 (3) 之定义取 $F_2=\{ab^{-1}|a\in R,b\in R^*\}/\sim$，一方面 $R\subseteq F_2\subseteq K$，另一方面由 (4) 可知 F_2 为域，且显然为 R 的分式域，即证分式域是包含 R 的最小域. ♣

20.证明 我们回忆，对于理想 I，$\sqrt{I}=\{a\in R|\exists n\in\mathbb{N},a^n\in I\}$，从而 $\sqrt{I+J}=\{a\in R|\exists n\in\mathbb{N},a^n\in I+J\subseteq\sqrt{I}+\sqrt{J}\}\subseteq\sqrt{\sqrt{I}+\sqrt{J}}$，另一方面，任意 $a\in\sqrt{\sqrt{I}+\sqrt{J}}$，即存在整数 n,s,t 与环中元素 i,j 使得 $a^n=i+j$，且 $i^s\in I$，$j^t\in J$，进而存在 $m=n(s+t)$ 使得 $a^m=(i+j)^{s+t}\in I+J$，则 $a\in\sqrt{I+J}$，综上即证 $\sqrt{I+J}=\sqrt{\sqrt{I}+\sqrt{J}}$. ♣

21.(挖补定理)

证明 我们考虑集合 $S'=R'\cup(S-R)$，若设 $\varphi:R\to R'$ 为同构，则可进一步定义 $\phi:S\to S'$，其中 $x\mapsto\phi(x)=\begin{cases}x, & 若x\in S-R\\ \varphi(x), & 若x\in R\end{cases}$，下面需要依次验证：$S'$ 可定义环结构，ϕ 是环同构，以及 R' 是 S' 的子环.

我们定义 $(S',\oplus,\otimes)$ 如下，对任意 $\bar{x},\bar{y}\in S'$，其中 $+,\cdot$ 均为 S 中加法与乘法，

$$\bar{x}\oplus\bar{y}=\begin{cases}\bar{x}+\bar{y}, & 若\bar{x},\bar{y}\in S-R\\ \varphi(x)+\varphi(y), & 若\bar{x}=\varphi(x),\bar{y}=\varphi(y)\in R'\\ \bar{x}+y, & 若\bar{x}\in S-R,\bar{y}=\varphi(y)\in R'\\ x+\bar{y}, & 若\bar{y}\in S-R,\bar{x}=\varphi(x)\in R'\end{cases},$$

同理也可定义乘法

$$\bar{x}\otimes\bar{y}=\begin{cases}\bar{x}\cdot\bar{y}, & 若\bar{x},\bar{y}\in S-R\\ \varphi(x)\cdot\varphi(y), & 若\bar{x}=\varphi(x),\bar{y}=\varphi(y)\in R'\\ \bar{x}\cdot y, & 若\bar{x}\in S-R,\bar{y}=\varphi(y)\in R'\\ x\cdot\bar{y}, & 若\bar{y}\in S-R,\bar{x}=\varphi(x)\in R'\end{cases}.$$

容易验证上述运算是良定义的，唯一值得说明的是 $\bar{x}+y\in S-R\subseteq S'$ 与 $\bar{x}\cdot y\in S-R\subseteq S'$，进而利用在 S 上构成的加法群与乘法半群，不难得到 $(S',\oplus,\otimes)$ 也是环.

下面验证 ϕ 是环同构，由其定义可知 ϕ 是自然的双射，按照定义分四类情况讨论也不难证明 $\phi(x+y)=\phi(x)\oplus\phi(y)$ 与 $\phi(xy)=\phi(x)\otimes\phi(y)$，进而保持加法与乘法，从而为环同构.

利用 R 关于运算的封闭性不难自然得到 R' 在 S' 中运算的封闭性，从而 R' 是 S' 的子环也是可以直接从定义验证的，细节略去. ♣

注：感觉这个定理只是玩了一下文字游戏，关键在于保证运算之合理定义，S' 长的其实很奇怪，本质上就是直接嫁接了剩余的部分.

2.4.3 幺环上的中国剩余定理

我们先给出幺环上中国剩余定理的一个简单版本：

定理 2.4.5: 习题 22

设 R 为幺环，I_1,I_2 为 R 的理想，且 $R=I_1+I_2$，试证明对任何 $a_1,a_2\in R$，必存在 $a\in R$ 使得 $a-a_1\in I_1$，$a-a_2\in I_2$.

证明 由 $R=I_1+I_2$，从而存在 $r_1,s_1\in I_1$，$r_2,s_2\in I_2$ 使得 $a_1=r_1+r_2$，$a_2=s_1+s_2$，从而考虑 $a=r_2+s_1$，从而 $a-a_1=r_1-s_1\in I_1$，$a-a_2=r_2-s_2\in I_2$，即证. ♣

为了推广到一般，并且与整数环上的版本形成呼应，我们需要推广一下同余与互素的概念：

定义 2.4.2: 同余与互素

设 R 为幺环，I,J 为理想，我们称 I,J **互素**，如果 $I+J=R$，我们称 R 中元素 x,y **模理想 I 同余**，如果 $x-y\in I$，并记为 $x\equiv y(\mathrm{mod}\ I)$.

注：这个定义放在整数环里是非常自然的，如考虑互素的正整数 m,n，那么其所对应的理想 $m\mathbb{Z}$ 与 $n\mathbb{Z}$ 在 Bezout 定理保证下，满足上述定义之条件，这也诱导出下面这个结果，

定理 2.4.6: 理想互素的等价定义

设 R 为幺环，I,J 为理想，则 I,J 互素的充要条件为存在 $a\in I,b\in J$ 使得 $a+b=1$.

证明 一方面是显然的，另一方面，若存在 a,b 使得 $a+b=1$，则任意 $r\in R$，$r=ar+br$ 且由吸收律，$ar\in I,br\in J$，即证 $R=I_1+I_2$. ♣

下面我们就可以给出中国剩余定理的一般表述：

定理 2.4.7: 幺环上的中国剩余定理——方程组版本

设 R 为幺环，且 $I_1,I_2,\cdots,I_n$ 为两两互素的理想，则任意 $r_1,r_2,\cdots,r_n\in R$，同余方程组

$$\begin{cases} x\equiv r_1 \pmod{I_1},\\ x\equiv r_2 \pmod{I_2},\\ \quad\vdots\\ x\equiv r_n \pmod{I_n}, \end{cases}$$

有解，且在模 $I_1\cap I_2\cap\cdots\cap I_n$ 的意义下解唯一.

证明 这个定理证明的核心在于：设理想 I,J,K，且 I 与 J,K 均互素，则 I 与 JK 互素. 注意到存在 $a,b\in I$，$c\in J$，$d\in K$ 使得 $a+c=b+d=1$，从而 $1=(a+c)(b+d)=(ab+ad+cb)+cd$，则存在 $ab+ad+cb\in I$，$cd\in JK$ 使得和为 1，故 I 与 JK 互素，由此不难归纳得到一般情形.

下设 $J_i=\prod\limits_{j\neq i}I_j$ 为 R 中理想，且有上文可知 I_i 与 J_i 互素，故存在 $a_i\in I_i$，$b_i\in J_i$ 使得 $a_i+b_i=1$，从而 $r_ib_i-r_i=a_ir_i\in I_i$，故 $r_ib_i\equiv r_i(\mathrm{mod}\ I_i)$，且任意 $j\neq i$，由 $b_i\in J_i$，故 $r_ib_i\in I_j$，进而模 I_j 余 0，综上有 $x=\sum\limits_{i=1}^{n}r_ib_i$ 为同余方程的一个解.

再设另有解 x_0，则 $x\equiv x_0(\mathrm{mod}\ I_i)$，$1\leq i\leq n$，从而 $x\equiv x_0(\mathrm{mod}\ I_1\cap I_2\cap\cdots\cap I_n)$，综上我们完成了中国剩余定理 (CRT) 之证明. ♣

下面是一种更简洁的版本，本质上没有区别

定理 2.4.8: 幺环上的中国剩余定理——同构版本

设 R 为幺环，且 $I_1,I_2,\cdots,I_n$ 为两两互素的理想，则

$$R\Big/\bigcap_{i=1}^{n}I_i\cong\bigoplus_{i=1}^{n}R/I_i.$$

证明 考虑 $\sigma:R\to R/I_1\oplus\cdots\oplus R/I_n$，$x\mapsto(x+I_1,\cdots,x+I_n)$，则显然 $\mathrm{Ker}\sigma=I_1\cap\cdots I_n$，而由定理 2.4.7 之中国剩余定理，任意 $(\overline{r_1},\overline{r_2},\cdots,\overline{r_n})\in R/I_1\oplus\cdots\oplus R/I_n$，存在 $x\in R$ 使得 $\sigma(x)=(\overline{r_1},\overline{r_2},\cdots,\overline{r_n})$，故 σ 为满同态，因此由环的同态基本定理即证. ♣

2.5 整环上的因子分解

2.5.1 Notes

我们从本节开始将研究环上的“分解”，“除法”，从而零因子是个很大的干扰，故无特殊说明，本节我们只考虑整环，即无零因子的交换幺环.

定义 2.5.1: 整除与因子

设 R 为一个整环，$a,b\in R$，若存在 $c\in R$ 使得 $a=bc$，称 a 能被 b **整除**，这时也称 b 为 a 的因子.

借助多项式环上，一个多项式乘上任意常数倍，并不本质上对多项式之间的整除关系产生影响，因为这个常数是 $\mathbb{P}[x]$ 中的可逆元 (即单位)，由此可把这种想法推广到一般的整环上:

定义 2.5.2: 相伴

设 R 为整环，$a,b\in R$，若存在 R 中的单位 (乘法可逆元)u，使得 $a=ub$，则称 a 与 b **相伴**，记为 $a\sim b$.

定义 2.5.3: 平凡因子与真因子

设 $a\in R^*$，则任何单位和 a 的相伴元都是 a 的因子，称为 a 的**平凡因子**，若 $b|a$，但 $a\nmid b$，则称 b 为 a 的**真因子**.

例 2.5.1. 设 $\mathbb{Z}[\sqrt{5}]=\{a+b\sqrt{5}|a,b\in\mathbb{Z}\}$，则 2 在 $\mathbb{Z}[\sqrt{5}]$ 只有平凡因子.

证明 这个例子的技巧在于，先证明 $\mathbb{Z}[\sqrt{5}]$ 的单位群为 $\{a+b\sqrt{5}||a^2-5b^2|=1\}$，这个的证明主要是构造 $N(a+b\sqrt{5})=|a^2-5b^2|$，进而对 $2=ab$，则 $4=N(a)N(b)$，利用数论性质，可知 $N(\cdot)\neq 2$，从而必有一个为 1，进而为单位. ♣

定义 2.5.4: 不可约元素与可约元素

设 R 为整环，$a\in R^*-U$，若 a 不存在非平凡因子 (即不存在真因子)，则称 a 为**不可约元素**，反之，则称 a 为**可约元素**.

定义 2.5.5: 素元素

R 为整环，$P\in R^*-U$，如果对任何 $a,b\in R$，$p|ab$ 蕴含 $p|a$ 或者 $p|b$，则称 p 为**素元素**.

紧接着上面两个定义，我们立即会关心的一个问题是

定理 2.5.1: 素元素一定是不可约元素

在任何整环中，素元素一定是不可约元素.

证明 设 $p \in R^* - U$ 为素元素，设 a 为 p 的一个因子，则存在 $b \in R^*$，使得 $p = ab$，若 $p|a$，则 $p \sim a$；若 $p|b$，则存在 $c \in R^*$ 使得 $b = pc$，进而 $p = ab = pac$，由无零因子的消去律可知 $ac = 1$，进而 a 为单位，进而 p 的任何因子为其相伴元或为单位，进而为不可约元素. ♣

例 2.5.2 (不可约元素不一定是素元素)**.** 考虑 $\mathbb{Z}[\sqrt{-5}]$，则 2 是不可约元素，但不是素元素.

证明 2 的不可约性已证，而又 $2|(1+\sqrt{5})(1-\sqrt{5})$，且 $2 \nmid 1+\sqrt{5}$，$2 \nmid 1-\sqrt{5}$，这是因为若 $2|1+\sqrt{5}$，则有 $c+d\sqrt{5}$ 使得 $2c+2d\sqrt{5} = 1+\sqrt{5}$，矛盾! ♣

下面我们考虑整环上的一些特殊条件

定义 2.5.6: 有限分解条件、因子链条件、素条件与公因子条件

设 R 为整环，则

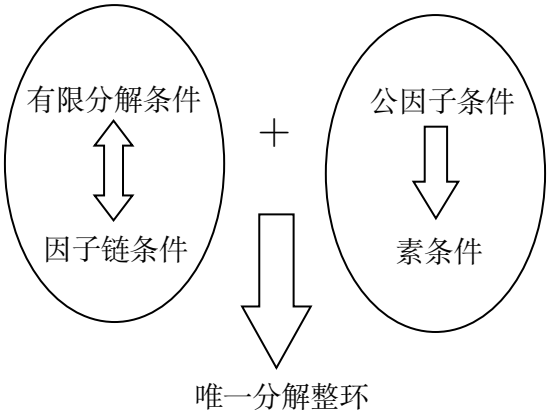
1. 若 R 中任何 $R^* - U$ 的元素在任何方式下都在有限次分解后不能再分解，则称 R 满足**有限分解条件**.
2. 若 R 中的一个元素序列 $a_1, a_2, \cdots$ 满足对任何 $l \geq 1$，a_{l+1} 为 a_l 的真因子，则称其为**真因子链**，如果 R 中任何真因子链都是有限的，则称 R 满足**因子链条件**.
3. 若 R 中每个不可约元素都是素元素，则称 R 满足**素条件**.
4. 对 R 中 n 个元素 $a_1, a_2, \cdots, a_n$，若 c 均能整除它们，称为其的一个**公因子**，若它们的一个公因子 d 满足能被其任何一个公因子整除，则称为其的一个**最大公因子**，若 R 的任何两个元素都存在最大公因子，则称 R 满足**公因子条件**.

上面这些条件，是为了铺垫得到一个重要的特殊环：

定义 2.5.7: 唯一分解整环 (UFD：Uniquely Factorial Domain)

设整环 R 满足有限分解条件，且满足分解的唯一性，则称 R 为**唯一分解整环**.

本节的剩下内容，是完成下面这个图表的证明：



定理 2.5.2

整环 R 满足有限分解条件当且仅当其满足因子链条件.

证明 一方面，若 R 满足有限分解条件，则对真因子链 $a_1, a_2, \cdots$，若其为无限，则任意 $a_l = a_{l+1}b_{l+1}$，则由于若 b_{l+1} 不为 a_l 真因子，则 $a_l \sim b_{l+1}$，进而 a_{l+1} 为单位，从而不为真因子矛盾，故 a_1 可以无限分解下去，即为 $a_1 = a_2b_2 = a_3b_3b_2 = \cdots$，矛盾.

另一方面是平凡且直接的，我们这里略去证明. ♣

例 2.5.3. 存在非唯一分解整环，如考虑 $\mathbb{Z}[\sqrt{5}]$，则 $9 = 3 \times 3 = (2+\sqrt{5})(2-\sqrt{5})$.

定理 2.5.3

整环 R 满足公因子条件，则其满足素条件.

证明 我们要证明即对任意满足公因子条件的整环，其不可约元素都是素元素，分为 5 步依次证明，核心在于**逐步给出最大公因子的刻画**.

(i) R 中任何两个元素的最大公因子在相伴意义下是唯一的. 这是因为设 d_1, d_2 为 a, b 的最大公因子，即任意 $c|a, b$，$c|d_1$ 且 $c|d_2$，从而 $d_1|d_2$，且 $d_1|d_2$，进而 $d_1 \sim d_2$，从而可记为 (a, b).

(ii) R 中任意有限个元素的最大公因子存在，且在相伴意义下唯一，这在上一条的基础上，利用归纳法不难得到，这里略去证明，且 $(a, (b, c)) \sim ((a, b), c)$.

(iii) 对任何 $a, b, c \in R$，$c(a, b) \sim (ca, cb)$. 不妨设 $(a, b) = d_1 \neq 0$，$(ca, cb) = d_2 \neq 0$，则 $cd_1|ca, cb$，进而 $cd_1|d_2$，设 $d_2 = ucd_1$，$ca = u'd_2$，则 $ca = u'ucd_1$，由消去律 $a = u'ud_1$，则 $ud_1|a$ 同理 $ud_1|b$，则 $ud_1|d_1$，进而 u 为单位，从而 $d_2 \sim cd_1$.

(iv) 对任何 $a, b, c \in R$，若 $(a, b) \sim 1$，$(a, c) \sim 1$，则 $(a, bc) \sim 1$. 注意到 $a \sim (a, ac)$，从而 $(a, bc) \sim ((a, ac), bc) \sim (a, (ac, bc)) \sim (a, c) \sim 1$.

(v) 若 p 为 R 中的不可约元素，且 $p|ab$，若不满足素条件，即 $p \nmid a, b$，则 $(p, a) \sim 1$，$(p, b) \sim 1$，进而 $(p, ab) \sim 1$，矛盾！从而即证. ♣

定理 2.5.4: 唯一分解整环的等价刻画

设 R 为整环，则下面三个条件等价：

1. R 为唯一分解整环；
2. R 满足因子链条件和素条件；
3. R 满足因子链条件和公因子条件.

2.5.2 Exercises From Z.Fh

1.证明 我们熟知 $\mathbb{Z}[\sqrt{-1}]$ 的单位群为 $\{1,-1,\sqrt{-1},-\sqrt{-1}\}$，从而 $a+b\sqrt{-1}$ 的相伴元为 $a+b\sqrt{-1},-a-b\sqrt{-1},-b+a\sqrt{-1},b-a\sqrt{-1}$. ♣

2.证明 设 $7=(a+b\sqrt{-1})(c+d\sqrt{-1})=(ac-bd)+(ad+bc)\sqrt{-1}$，则 $ac-bd=7$ 且 $ad+bc=0$，则 $(a^2+b^2)(c^2+d^2)=49$，又 $a^2+b^2=c^2+d^2=7$ 无解，且 $a^2+b^2=1,c^2+d^2=49$ 有解但这表明因子中必有一个单位，故综上 7 为不可约元素. 同理对 23，我们有 $(a^2+b^2)(c^2+d^2)=23^2$，也可做类似讨论知 23 不可约.

又不难注意到 $5=(1+2\sqrt{-1})(1-2\sqrt{-1})$，从而 5 是可约的. ♣

3.证明 设 $m,n\in\mathbb{Z}$，在整数环中最大公因子为 d，在 $\mathbb{Z}[\sqrt{-1}]$ 中最大公因子为 $a+b\sqrt{-1}$，从而不难发现 $d|a+b\sqrt{-1}$，设 $a+b\sqrt{-1}=d(p+q\sqrt{-1})$，则 $d(p+q\sqrt{-1})|m,n$，则 $d(p+q\sqrt{-1})|d$，进而 $p+q\sqrt{-1}|1$ 即为单位，故 $d\sim a+b\sqrt{-1}$，从而在相伴意义下，最大公因子是相同的. ♣

4.证明 关于加法构成群是显然的，交换性与无零因子是自然的，有幺元 1，从而构成整环.

先考虑 R 中的单位，即可逆元全体，若 $\dfrac{m}{2^n}$ 为单位，即 $\dfrac{2^n}{m}\in R$，从而 m 为 2 的幂次或其相反数，即 $U(R)=\{\pm 2^n|n\in\mathbb{Z}\}$.

再考虑其中不可约元素，我们断言其为 $\{\pm 2^n p|n\in\mathbb{Z},p\geq 3\text{为素数}\}$，一方面其不可约是显然的，另一方面若 $2^n m$ 不在其中，则 m 为合数，可分解为 $m=m_1m_2$，进而可分解为 $2^nm_1\cdot m_2$，综上即为所求.

最后考虑素元素，一方面任意 $2^np|(2^sa)(s^t)b$，则 $p|ab$，进而 $p|a$ 或 $p|b$，故 $2^np|2^sa$ 或 $2^np|2^tb$，可知其均为素元素，另一方面素元素均为不可约元素，而上述说明了 R 中不可约元素为素元素，因此全体素元素也为 $\{\pm 2^np|n\in\mathbb{Z},p\geq 3\text{为素数}\}$. ♣

5.证明 注意到在 $\mathbb{Z}_2$ 中，$(x^2+x+1)(x+1)=x^3+2x^2+2x+1=x^3+1$，从而 x^2+x+1 是 x^3+1 的因子，在 $\mathbb{Z}_3[x]$ 中，若设 $x^2+x+1|x^3+1$，则存在 $x+b$ 使得 $(x+b)(x^2+x+1)=x^3+(b+1)x^2+(b+1)x+b=x^3+1$，则 $b+1\equiv 0(\text{mod }3)$，$b\equiv 1(\text{mod }3)$ 无解，从而可知 x^2+x+1 不是 x^3+1 的因子. ♣

6.证明 设 $\sqrt{-3}|(a+b\sqrt{-3})(c+d\sqrt{-3})$，则存在 $u+v\sqrt{-3}$ 使得 $-3v+u\sqrt{-3}=(ac-3bd)+(ad+bc)\sqrt{-3}$，从而 $3|ac-3bd$，则 $3|ac$，不妨设 $3|a$，则 $\sqrt{-3}|a+b\sqrt{-3}$，故 $\sqrt{-3}$ 为素元素.

设 $4+\sqrt{-3}|(a+b\sqrt{-3})(c+d\sqrt{-3})$, 从而有 $4+\sqrt{-3}|(a+b\sqrt{-3})(c+d\sqrt{-3})-(4b+b\sqrt{-3})(c+d\sqrt{-3})-(a-4b)(4d+d\sqrt{-3})$, 这表明 $4+\sqrt{-3}|(a-4b)(c-4d)$, 进而 $19|(a-4b)^2(c-4d)^2$, 故不妨设 $19|a-4b$, 即 $4+\sqrt{-3}|a-4b$, 即有 $4+\sqrt{-3}|a+4\sqrt{-3}$, 这表明 $4+\sqrt{-3}$ 为素元素. ♣

7.证明 若 $3|1+2\sqrt{-5}$, 则 $9=N(3)|N(1+2\sqrt{-5})=21$, 显然矛盾, 故 $3\nmid 1+2\sqrt{-5}$, 又若 $3=ab$, 故 $N(a)N(b)=9$, 而 $N(c+d\sqrt{-5})=a^2+5b^2$ 不可能为 3, 从而 a,b 中有一个为单位, 又若 $N(a)=9$, 则 $a=\pm 3$ 或 $\pm 2\pm 1\sqrt{-5}$, 故可知 3 不可约. 又 $3|21=(1+2\sqrt{-5})(1-2\sqrt{-5})$, 且 $3\nmid 1\pm 2\sqrt{-5}$, 故可知 3 不为素元素, 进而 $\mathbb{Z}[\sqrt{-5}]$ 不为 UFD. ♣

8.证明 (1) 设 $a+b\sqrt{-5}=(c+d\sqrt{-5})(e+f\sqrt{-5})$, 从而有 $9=a^2+5b^2=(c^2+5d^2)(e^2+5f^2)$, 即 $c^2+5d^2=e^2+5f^2=3$ 或 $c^2+5d^2=1, e^2+5f^2=9$, 从而可知一定有 $c+d\sqrt{-5}=\pm 1$ 为单位, 进而可知 $a+b\sqrt{-5}$ 不可约.

(2) 反证法, 若 α 与 β 有最大公因子 d, 则 $3|\alpha,\beta$, 则 $3|d$, 设 $d=3(a+b\sqrt{-5})$, 则存在 $c+d\sqrt{-5}$ 使得 $3(a+b\sqrt{-5})(c+d\sqrt{-5})=9$, 进而 $(a^2+5b^2)(c^2+5d^2)=9$, 则可知 $a+b\sqrt{-5}=\pm 1,\pm 3$ 或 $\pm 2\pm\sqrt{-5}$, 显然 $9\nmid 6$, 且若为 $\pm 2\pm\sqrt{-5}$, 则 $2\pm\sqrt{-5}|3$, 均不可能, 这表明 $a+b\sqrt{-5}=\pm 1$, 则最大公因子为 3, 又 $9=(2+\sqrt{-5})(2-\sqrt{-5})$, $6=3\cdot(2+\sqrt{-5})$, 从而有公因子 $2+\sqrt{-5}$, 即 $2+\sqrt{-5}|3$, 矛盾! 综上可知不存在最大公因子. ♣

9.证明 反证法, 若不满足因子链条件, 从而存在无限长的真因子链 $a_1,a_2,\cdots,a_n,\cdots$, 且 a_{i+1} 均为 a_i 的真因子, 故 $N(a_{i+1})$ 为 $N(a_i)$ 的真因子, 这表明正整数列 $N(a_1),N(a_2),\cdots,N(a_n),\cdots$ 严格递减, 矛盾! ♣

10.证明 (1) 关于加法构成 Abel 群是自然的, 而对任意 $\dfrac{a+b\sqrt{-3}}{2}$ 与 $\dfrac{c+d\sqrt{-3}}{2}$, 有

$$\frac{(a+b\sqrt{-3})(c+d\sqrt{-3})}{4}=\frac{(ac-3bd)+(ad+bc)\sqrt{-3}}{4},$$

且 $ac-3bd+ad+bc=(a+b)(c+d)-4bd$ 为 4 的倍数, 从而即证关于乘法的封闭性, 而结合律与交换性是平凡的, 又显然有幺元 1. 若有 $ac-3bd=0$ 且 $ad+bc=0$, 则 $ac\cdot ad=3bd\cdot(-bc)$ 即 $(a^2+3b^2)cd=0$, 若 $a^2+3b^2=0$, 则 $a=b=0$; 若 $cd=0$, 简单讨论可知仍有 $a=b=0$ 或 $c=d=0$, 这即意味着 R 无零因子, 综上即证 R 为整环.

(2) 设 $u\in R$ 为单位, 设 $u=\dfrac{a+b\sqrt{-3}}{2}$, 由于其可逆, 从而设逆元 $u^{-1}=\dfrac{c+d\sqrt{-3}}{2}$, 则 $ac-3bd=4$, $ad+bc=0$, 若 $b=0$, 则 $ac=4$, $ad=0$, 故 $d=0$, 而 a,c 均为偶数, 从而 $a=c=\pm 2$, 即 $u=\pm 1$; 若 $b\neq 0$, 则可知 $d\neq 0$, 进而 a,b,c,d 均不为 0, 从而我们有

$$16=(ac-3bd)^2+3(ad+bc)^2=a^2c^2+9b^2d^2+3a^2d^2+3b^2c^2\geq 16,$$

故可知 $a^2=b^2=c^2=d^2=1$, 因此不难验证 $u=\dfrac{\pm 1\pm\sqrt{-3}}{2}$, 即证.

(3) 显然, 因为 $\dfrac{1+\sqrt{-3}}{2}$ 是单位, 且 $1+\sqrt{-3}=2\cdot\dfrac{1+\sqrt{-3}}{2}$. ♣

11.解 不存在最大公因子, 注意到 $4=(1+\sqrt{-3})(1-\sqrt{-3})=2\cdot 2$, 从而两者有公因子 $1+\sqrt{-3}$ 与 2, 则若它们有最大公因子 d, 则 $2|d$ 且 $1+\sqrt{-3}|d$, 而易见 2 与 $1+\sqrt{-3}$ 均不可约, 则不难发现 $2(1+\sqrt{-3})|d$, 从而 $d\sim 2(1+\sqrt{-3})$, 即 $2(1+\sqrt{-3})|4$, 显然矛盾, 即证. ♠

12.解 考虑 $\mathbb{Z}$ 为唯一分解整环，但其子环如 $4\mathbb{Z}$ 甚至不为整环，为一个反例. ♠

13.证明 (1) 由 $m_1 \sim m$，从而存在单位 u 使得 $m_1 = um$，则 $a|m_1$ 且 $b|m_1$，故 m_1 是 a, b 的公倍式. 而对任意公倍式 n，$m|n$，故设 $n = md = u^{-1}dm_1$，从而 $m_1|n$，综上表明 m_1 也为 a, b 的最小公倍式.

(2) 任意 $m, n \in R^*$，由 R 为 UFD，从而存在 $a = (m, n)$，设 $m = ac$，$n = ad$，下面证明 $nc = md$ 是 m, n 的最小公倍式. 一方面 $n|nc$，$m|md = nc$，从而 nc 为公倍式；另一方面，设 p 为 m, n 的公倍式，则 $m|p$ 且 $n|p$，则 $ac|p$ 且 $ad|p$，而 $(ac, ad) \sim a$，则 $acd|p$，综上可知 $nc = acd$ 为最小公倍式，即证存在性.

(3) 设 $a = (a, b) \cdot g$，$b = (a, b) \cdot h$，则由 (1)、(2) 可知 $[a, b] \sim ah = bg$，从而 $[a, b](a, b) \sim ah \cdot (a, b) = ab$.

由 R 为唯一分解整环，从而不难证明对 $x, y \in R^*$ 有不可约因子分解：

$$x = \varepsilon_1 p_1^{l_1} \cdots p_k^{l_k}, \quad y = \varepsilon_1 p_1^{r_1} \cdots p_k^{r_k}, \quad l_i, r_i \in \mathbb{Z},$$

则 $(x, y) \sim \prod_{i=1}^{k} p_i^{\min\{l_i, r_i\}}$，$[x, y] \sim \prod_{i=1}^{k} p_i^{\max\{l_i, r_i\}}$，其中 $p_i (1 \leq i \leq k)$ 均为不可约元素.

现设 $a \sim p_1^{a_1} \cdots p_k^{a_k}$，$b \sim p_1^{b_1} \cdots p_k^{b_k}$，$p_1^{c_1} \cdots p_k^{c_k}$，则不难计算得

$$[a, (b, c)] = \prod_{i=1}^{k} p_i^{\max\{a_i, \min\{b_i, c_i\}\}} = \prod_{i=1}^{k} p_i^{\min\{\max\{a_i, b_i\}, \max\{a_i, c_i\}\}} = ([a, b], [a, c]),$$

其中用到了 $\max\{a_i, \min\{b_i, c_i\}\} = \min\{\max\{a_i, b_i\}, \max\{a_i, c_i\}\}$，综上即证. ♣

14.证明 若 $d \sim (a_1, a_2)$，设 $e = (b_1, b_2)$，则 $ed|a_1, a_2$，进而 $ed|d$，从而 e 为单位，即 b_1, b_2 互素；若 e 为单位，则一方面 d 为 a_1, a_2 公因子，另一方面，任意 $f|a_1, a_2$，则 $f|d(b_1, b_2) = ed$，而 e 为单位故 $f|d$，这即表明 d 为最大公因子，即证. ♣

15.证明 从多项式的次数考虑，本题是显然的. ♣

16.证明 由 R 为 UFD，从而在相伴的意义下，任意 $a \in R^*$ 可以唯一分解成若干不可约元素乘积，也即 $a = p_1 p_2 \cdots p_r$，从而我们断言 a 的任一因子一定形如 $up_{i_1} \cdots p_{i_k}$，其中 $1 \leq i_1, \cdots, i_k \leq r$ 互不相等. 这个断言是自然的，因为若不成立，即存在因子 d 有不可约元素 q 不在 $p_1, \cdots, p_k$ 中，矛盾，因此设 U 为 R 的单位群，则有

$$\#\{a\text{的因子}\} \leq |U| \cdot 2^r < \infty,$$

即证其因子个数有限，进而我们完成了证明. ♣

17.证明 课本 2.9 节有更一般的版本，若 R 为 UFD，则 $R[x]$ 为 UFD，证明见教材即可. 不过也可由高等代数中的结果，本原多项式可以唯一分解成不可约的本原多项式的乘积，而任一多项式与其对应的本原多项式仅相差一个单位 (一个正整数). ♣

2.6 素理想与极大理想

2.6.1 Notes

定义 2.6.1: 素理想

设 I 为环 R 的理想，$I \neq R$，若由 $ab \in I$ 蕴含着 $a \in I$ 或 $b \in I$，则称 I 为 R 的**素理想**.

素理想这个概念的产生源自对整环 (无零因子) 的渴望，而我们自然希望把一个一般的环模掉理想后，就没有零因子了，即 $ab+I=(a+I)(b+I)=0+I$ 蕴含着 $a+I=0+I$ 或 $b+I=0+I$，即 $a \in I$ 或 $b \in I$，这就是定义所表示的.

并且我们也不难看到：*判断一个理想是否是素理想的充要条件为看 R/I 是否为整环.*

命题 2.6.1

对任意正整数 m，求 $\mathbb{Z}_m$ 的所有素理想和极大理想.

解 **Case I.** 若 m 为素数，从而 $\mathbb{Z}_p$ 之子环仅有 $\{0\}$ 与其自己，从而容易看见 $\{0\}$ 为域 $\mathbb{Z}_p$ 的全体素理想和极大理想 (这里极大理想是显然的，因为理想拢共就俩).

Case II. 若 m 为合数，注意到 $\mathbb{Z}_m=\mathbb{Z}/m\mathbb{Z}$ 为商环，从而我们由环的同态基本定理，对交换幺环 R，I 为其理想，则对任意包含 I 的理想 J，成立 $(R/I)/(J/I) \cong R/J$，进而结合定理 2.6.1 与定理 2.6.5 可知，以及 R/I 的理想均形如 J/I 可知*R/I 的素理想和极大理想与 R 中包含 I 的素理想和极大理想一一对应* (这里是用到了若 J 为素/极大理想，则同构保持 R/J 为整环/域).

从而考虑 $\mathbb{Z}$ 中包含 $m\mathbb{Z}$ 的理想，这即 $n\mathbb{Z}$，且 $n|m$，又 $n\mathbb{Z}$ 为 $\mathbb{Z}$ 的素理想/极大理想，从而 $n=p$ 为素数，故可知设 m 的全体素因子为 $p_1,\cdots,p_k$，从而 $\mathbb{Z}_m$ 的全体素理想和极大理想为 $p_i\mathbb{Z}/m\mathbb{Z}=p_i\mathbb{Z}_m$.(这里简单讨论可知 $\{0\}$ 不为 $\mathbb{Z}_m$ 理想).

综上我们可知，$\mathbb{Z}_m$ 的素理想和极大理想为 $\begin{cases}\{0\}, & m\text{为素数}\\ p\mathbb{Z}_m, & m\text{为合数},p|m\end{cases}$. ♠

注：本题最有价值的想法是*R/I 的素理想和极大理想与 R 中包含 I 的素理想和极大理想一一对应*，这极大的简化了问题，相当漂亮的思想，并且这个观察的一个直接推论就是，$\mathbb{Z}_m$ 的理想一共有 $d(m)$ 个，这里 $d(m)$ 表示 m 的不同因子个数，特别的

$$d(m)=\prod_{i=1}^{k}(\alpha_i+1), \quad \text{若} m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}.$$

本命题的讨论来源于知乎回答.

定理 2.6.1

设 R 是交换幺环，I 为环 R 的理想，$I \neq R$，则 I 是 R 的素理想当且仅当 R/I 为整环，进一步可知 R 为整环的充要条件为 $\{0\}$ 是 R 的素理想.

利用环的同态基本定理，我们可以得到

定理 2.6.2

设 f 是交换幺环 R_1 到 R_2 的满同态，I 是 R_1 中包含 $K=\mathrm{Ker}f$ 的一个素理想，则 $f(I)$ 是 R_2 的素理想.

证明 注意到 I 为包含 K 的素理想等价于 R_1/I 为整环，而由同态基本定理可知 $R_1/I\cong R_2/f(I)$，故 $R_2/f(I)$ 为整环，等价于 $f(I)$ 为素理想，即证. ♣

如果我们对交换幺环 R 的两个非空子集 A,B，定义

$$AB=\left\{\sum_{i=1}^{n}a_ib_i\middle|a_i\in A,b_i\in B\right\},$$

则不难发现 A,B 都是 R 的子环 (理想)，那么 AB 也是 R 的子环 (理想). 由此我们可以给出素理想的第二定义 (重要性质)：

定理 2.6.3

设 I 是交换幺环 R 的理想，$I\neq R$，则 I 是 R 的素理想当且仅当对任何理想 A,B，由 $AB\subseteq I$ 可推出 $A\subseteq I$ 或 $B\subseteq I$.

为了进一步希望得到域，我们引入极大理想的概念

定义 2.6.2: 极大理想

设 I 是交换幺环 R 的真理想，且包含 I 的 R 中理想只有 I 和 R，则称 I 为**极大理想**.

例 2.6.1. 整数环 $\mathbb{Z}$ 的所有极大理想为 $p\mathbb{Z}$，其中 p 为素数即全体素理想.

命题 2.6.2

上一例中表明整数环的非零理想是极大理想当且仅当其是素理想，但这对一般的整环并不成立，但值得注意的是极大理想一定为素理想.

解 我们给出本节习题 2 作为反例：$\langle x\rangle$ 为 $\mathbb{Z}[x]$ 的素理想但不为极大理想.

显然 $\langle x\rangle=\{p(x)\in\mathbb{Z}[x]|p(0)=0,\text{i.e.},x|p(x)\}$，从而其为理想是显然的，任意 $f(x)g(x)\in\langle x\rangle$，则 $f(0)g(0)=0$，从而必有 $f(0)=0$ 或 $g(0)=0$，这蕴含着 $f(x)\in\langle x\rangle$ 或 $g(x)\in\langle x\rangle$，即证 $\langle x\rangle$ 为素理想. 又考虑 $\langle x,2\rangle=\{p(x)\in\mathbb{Z}[x]|p(0)\text{为偶数}\}$，显然其为包含 $\langle x\rangle$ 的理想，进而 $\langle x\rangle$ 不为极大理想，综上我们完成了证明. ♠

定理 2.6.4

设 R 是交换幺环，则 R 是域的充要条件为 $\{0\}$ 是 R 的极大理想.

证明 一方面，若 R 是域，设 I 为 R 的非零理想，则存在非零元 $a \in I$，进而 $a^{-1} \in I$，则 $1 = a \cdot a^{-1} \in I$，故任意 $b \in R$，有 $b = b \cdot 1 \in I$，故 $I = F$，这即表明 $\{0\}$ 为域 R 的极大理想. 这也表明域没有非平凡理想.

另一方面，若 $\{0\}$ 是 R 的极大理想，从而任取 $a \in R^*$，考虑生成理想 $\langle a \rangle = \{ra | r \in R\}$，显然 $\{0\} \subseteq \langle a \rangle$，结合 $\{0\}$ 为极大理想，故 $\langle a \rangle = \{ra | r \in R\} = R$，故存在 $r \in R$ 使得 $ra = e$，故 a 可逆，故 R^* 中每个元素均可逆，因此 R 为域. ♣

定理 2.6.5: 定义极大理想的目的

设 R 为交换幺环，M 为 R 的理想，则 M 是 R 的极大理想当且仅当 R/M 是域.

证明 一方面，若 R/M 是域，则可知对 R 中任意包含 M 的理想 A，可知 A/M 是 R/M 的理想，又后者为域，故可知 $A/M = \{0 + M\}$ 或 R/M，进而 $A = M$ 或 R，从而 M 为极大理想.

另一方面，若 M 是极大理想，从而任意 $a + M \neq 0 + M$，考虑生成理想

$$I = \langle M \cup \{a\} \rangle = \left\{ \sum_{i=1}^{n} r_i m_i + ra \middle| r_i, r \in R, m_i \in M \right\},$$

则由 M 极大，故 $I = R$，也即存在 $\sum_{i=1}^{n} r_i m_i + ra = e$，也即 $ar + M = e + M$，故 $a + M$ 有逆元 $r + M$，这表明商环 R/M 中任意非零元素均可逆，故为域. ♣

证明 (另证)M 为极大理想，当且仅当 R 中不存在包含 M 的非 M 真理想，而根据 R 中包含 I 的理想一一对应于 R/I 的理想可知 R/M 的理想只有 $0 = M/M$ 和 R/M，即只有平凡理想，从而 R/M 为域. ♣

我们已经知道极大理想一定是素理想，因此若极大理想存在那么素理想也一定存在，下面的问题就是什么样的环总存在极大理想? 首先需要排除的情形是并非所有的环均有极大理想，比如零环 (这里指相乘全定义为 0 的环)，如考虑 $\{\mathbb{Q}, +, *\}$，这里任意 $a * b = 0$，其关于加法没有极大子群 (Why?)，进而没有极大理想.

但我们下面将说明，任意幺环都存在极大理想:

定理 2.6.6: 极大理想的存在性

任意幺环 R，每一个真理想都包含在一个极大理想中.

证明 证明是构造性的，因此我们这里承认 *Zorn's Lemma*. 设 I 为 R 的非零真理想，设 $\mathcal{S}$ 为 R 中所有包含 I 的真理想构成的集合，从而 $\mathcal{S}$ 在包含关系下构成一个偏序集，进而设 $\mathcal{C}$ 为 $\mathcal{S}$ 的任意一个链，定义 J 为 $\mathcal{C}$ 中理想之并，i.e. $J = \bigcup_{A \in \mathcal{C}} A$.

下面证明 J 为一个理想，一方面 J 非空，因为 $\mathcal{C}$ 非空 (包含理想 0)，另一方面 J 关于乘法显然吸收，关于加法封闭且构成群，注意到 $A, B \in \mathcal{C}$ 为链，从而 $A \subseteq B$ 或反之，但无论如何任意 $a \in A, b \in B$，均有 $a - b \in J$，故 J 为理想.

显然真理想不会包含幺元 1(不然任意 $r \in R$，$r = r \cdot 1 \in I$)，因此 $\mathcal{C}$ 中理想均不包含 1，进而 J 不包含 1 从而为真理想，从而 $J \in \mathcal{S}$，进而可知其为 $\mathcal{C}$ 的上界，因此由 Zorn's Lemma，$\mathcal{S}$ 又最大元，进而即为包含 I 的极大理想. ♣

下面是一些关于 *Zorn's Lemma* 的解释：

首先是偏序集，本质上这是一个集合在其上定义了序关系 (但是注意，这并不代表任意两个元素间可以比较)，全序集则弥补了这一点即任两个间可比较，那么偏序集的一个链，就是指这里面全序的一部分 (也即链中元素可以两两比较)，进一步定义的上界和最大元都是自然推广的，不再赘述.Zorn's Lemma 则是声称对于一个偏序集，若其每一个链均有上界，那么这个偏序集有最大元.(更详细内容可参考集合论相关资料)

2.6.2 Exercises From Z.Fh

1.解 (a) 注意到 $\mathbb{R} \times \mathbb{R}/(\mathbb{R}, 0) \cong \mathbb{R} \times \mathbb{R}/(0, \mathbb{R}) \cong \mathbb{R}$ 为域，从而 $(\mathbb{R}, 0)$ 与 $(0, \mathbb{R})$ 均为极大理想. 另一方面，对任意 $\mathbb{R} \times \mathbb{R}$ 的极大理想 I，若存在 $(a, b) \in I$ 且 $ab \neq 0$，则 $(1, 0) = (a, b) \cdot \left(\frac{1}{a}, 0\right) \in I$，这即表明 $(\mathbb{R}, 0) \subseteq I$，而前者为极大理想，从而 $I = \mathbb{R} \times \mathbb{R}$，综上我们证明了 $\mathbb{R} \times \mathbb{R}$ 的极大理想为 $(\mathbb{R}, 0)$ 和 $(0, \mathbb{R})$.

(b) 我们给出 (b)、(c)、(d) 的一个统一结果，设 $p(x) \in \mathbb{R}[x]$，那么设其全体不可约因式为 $p_1(x), \cdots, p_m(x)$，那么下证：$\mathbb{R}[x]/\langle p(x)\rangle$ 的全体极大理想为 $\langle p_k(x)\rangle / \langle p(x)\rangle$，其中 $1 \leq k \leq m$.

注意到，$\mathbb{R}[x]$ 是 ED，自然为 PID，结合类似于命题 2.6.1 之讨论，我们可得 $\mathbb{R}[x]/\langle p(x)\rangle$ 的极大理想与 $\mathbb{R}[x]$ 中包含 $\langle p(x)\rangle$ 的极大理想一一对应，设 I 为极大理想且 $\langle p(x)\rangle \subseteq I$，一方面 I 为主理想，从而存在 $q(x)$ 使得 $I = \langle q(x)\rangle$，这意味着 $q(x) | p(x)$，另一方面 $\langle q(x)\rangle$ 为极大理想，从而 $q(x)$ 是 $\mathbb{R}[x]$ 中的不可约多项式，即证.

因此 $\mathbb{R}[x]/\left\langle x^2\right\rangle$ 的全体极大理想为 $\langle x\rangle / \left\langle x^2\right\rangle \cong \mathbb{R}$.

(c)$\mathbb{R}[x]/\left\langle x^2 - 3x + 2\right\rangle$ 的全体极大理想为 $\langle x - 1\rangle / \left\langle x^2 - 3x + 2\right\rangle$ 与 $\langle x - 2\rangle / \left\langle x^2 - 3x + 2\right\rangle$.

(d) 由于 $x^2 + x + 1$ 在 $\mathbb{R}[x]$ 中不可约，故可知其不存在极大理想. ♠

2.证明 除了命题 2.6.2 之证明，还可以注意到 $\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}$ 为整环不是域来证明. ♣

3.证明 本题蕴含在命题 2.6.1 之证明中. ♣

4.解 本题是命题 2.6.1 之特例，$\mathbb{Z}_{36}$ 的全体素理想和极大理想为 $2\mathbb{Z}_{36}$ 和 $3\mathbb{Z}_{36}$. ♠

5.证明 注意到 $\langle 4\rangle = \{4n | n \in \mathbb{Z}\}$，从而任意 $\langle 4\rangle \subseteq I$，$I$ 为理想，若 $I \neq \langle 4\rangle$，则存在 $4n + 2 \in I$，故 $2 \in I$，进而 $I = R$，从而 $\langle 4\rangle$ 为极大理想. 另一方面，$R/\langle 4\rangle \cong \mathbb{Z}_2$ 为域 (?) ♣

6.证明 注意到 $\mathbb{Z}_2[x]$ 与 $\mathbb{Z}_3[x]$ 是 ED，进而为 PID，从而类似于第 1 题，我们可知是否为域取决于 $\langle p(x)\rangle$ 是否是极大理想，进而取决于 $p(x)$ 是否为不可约多项式. 在 $\mathbb{Z}_2[x]$ 中，$x^3 + x + 1 = 1$ 当 $x = 0, 1$ 时，从而不可约，在 $\mathbb{Z}_3[x]$ 中，显然 $x^3 + x + 1 = (x + 2)(x^2 + x + 2)$ 可约，因此 $\mathbb{Z}_2[x]/\left\langle x^3 + x + 1\right\rangle$ 是域，$\mathbb{Z}_3[x]/\left\langle x^3 + x + 1\right\rangle$ 不是域. ♣

7.证明 设 N 为 R 理想，且 $M \subseteq N$，若 $N \neq M$，则存在单位 $u \in N$，故任意 $r \in R$，$r =$

$(ru^{-1})u \in N$，故 $N = R$，从而 M 为极大理想，又设 P 为 R 中极大理想，则 $P \subseteq M$ 或 P 包含单位，分别蕴含着 $P = M$ 和 $P = R$，综上 M 为 R 中唯一的极大理想. ♣

8.证明 任意 $p \in P$，$r \in R$，取 $a \in A - P$，则考虑 $pra = p(ra) \in P$，且 $ra \in A$，结合 P 为 A 的素理想，且 $a \notin P$，故 $pr \in P$，同理 $rp \in P$，只需考虑 arp 即可，综上 P 是 R 的理想，即证. ♣

9.证明 (1) 由 R/N 为除环，从而 $\{0+N\}$ 是 R/N 的极大理想，从而任意 I 为 R 中包含 N 的理想，则 I/N 是 R/N 中包含 $\{0+N\}$ 的理想，从而 $I/N = \{0+N\}$ 或 R/N，这表明 $I = N$ 或 R，从而 N 为极大理想.

(2) 反证法，若 $a \notin N$，则由 R/N 为除环，故存在 $b \notin N$，使得 $(a+N)(b+N) = e+N$，进而 $a+N = (a+N)(e+N) = (a^2+N)(b+N) = 0+N$，这表明 $a \in N$，矛盾！从而 $a \in N$. ♣

10.证明 A 是 $\mathbb{Z}[x]$ 的理想与 $\langle x \rangle \subseteq A$ 是显然的，其中后者是由于 $\langle x \rangle$ 中元素 $f(x)$ 满足 $f(0) = 0$，显然 $m|f(0)$. 若 A 为素理想，从而任意 $m|f(0)g(0)$ 则蕴含着 $m|f(0)$ 或 $m|g(0)$，这等价于 m 为素数，从而当且仅当 m 为素数时 A 为素理想. ♣

11.证明 设 M 为 R 的极大理想，假设其不为素理想，则存在 $a, b \in R - M$ 使得 $ab \in M$，则考虑理想 $M + (a)$ 和 $M + (b)$，则由 M 为极大理想，则 $M + (a) = M + (b) = R$，因此任取 $t \in R$，存在 $s \in R$ 使得 $t = s^2$，则存在 $m_1, m_2 \in M$，$a_1 \in (a)$，$b_1 \in (b)$，使得 $t = m_1 + a_1 = m_2 + b_1$，则 $s = t^2 = (m_1 + a_1)(m_2 + b_1) = m_1m_2 + a_1m_2 + m_1b_1 + a_1b_1$，由 M 为理想，且 $ab \in M$ 从而 $m_1m_2, a_1m_2, m_1b_1, a_1b_1 \in M$，因此 $t \in M$，故 $R \subseteq M$，故 $M = R$ 矛盾！ ♣

12.证明 (大显题) 事实上 P 为素理想当且仅当任意 $ab \in P$ 蕴含 $a \in P$ 或 $b \in P$ 当且仅当若 $a \in Q$，$b \in Q$，则 $ab \in Q$，即证. ♣

13.证明 注意到在 UFD 的 R 中，p 为不可约元素 $\Leftrightarrow$ p 为素元素 $\Leftrightarrow$ 任意 $a, b \in R$，$p|ab$ 蕴含 $p|a$ 或 $p|b$ $\Leftrightarrow$ 任意 $a, b \in R$，$ab = pr \in \langle p \rangle$ 蕴含着 $a \in \langle p \rangle$ 或 $b \in \langle p \rangle$ $\Leftrightarrow$ 主理想 $\langle p \rangle$ 为素理想，即证. ♣

14.证明 注意到 $\mathbb{Z}[x]/\langle x, n \rangle \cong \mathbb{Z}_n$ 为域当且仅当 n 为素数，即证. ♣

15.证明 注意到 $\mathbb{P}[x]/\langle x \rangle \cong \mathbb{P}$ 为数域，进而为域，从而 $\langle x \rangle$ 为极大理想. ♣

2.7 主理想整环与欧几里得整环

2.7.1 Notes

定义 2.7.1: 主理想整环 (PID)：Principal Ideal Domain

如果一个交换幺环的每个理想都是主理想，则称其为**主理想环**，若其还为整环，则称为**主理想整环**.

例 2.7.1. $\mathbb{Z}[x]$ 不为主理想整环，因为不难证明理想 $\langle 3, x\rangle$ 不为主理想.

命题 2.7.1: 思考题

求素数 p 与 $u(x) \in \mathbb{Z}[x]$ 且其次数大于 0 满足的条件，使得 $\langle p, u(x)\rangle$ 是主理想.

解 易见当且仅当 $p|u(x)$ 时，其为主理想 $\langle p\rangle$，证明是平凡的. ♠

引理 2.7.2. 设 $I_i, i = 1, 2, \cdots$ 为 R 中的一个升理想序列，即满足任意 j，有 $I_j \subset I_{j+1}$，则 $I = \cup_i I_i$ 是 R 的理想.

定理 2.7.1

主理想整环是唯一分解整环

证明 我们只需证明主理想整环满足因子链条件和素条件.

(1) 先证明主理想整环满足因子链条件，即考虑 R 的一个序列 $a_1, a_2, \cdots, a_n, \cdots$，其中 a_{k+1} 是 a_k 的真因子，则进而考虑 a_k 生成的主理想 $\langle a_k\rangle$，从而不难看见 $I_k \subset I_{k+1}$，故由引理 $I = \cup_k I_k$ 为理想，进而为主理想，从而存在 $d \in R$ 使得 $\langle d\rangle = I$，从而由 $d \in I$，故存在 m 使得 $d \in I_m = \langle a_m\rangle$. 我们断言 a_m 是序列中的最后一个元素，若不然存在 a_m 的真因子 a_{m+1}，则由 $a_{m+1} \in \langle d\rangle$，则 $a_m|d|a_{m+1}$，矛盾！故可知 R 满足因子链条件.

(2) 再证明主理想整环满足素条件，这部分证明的核心在于**不可约元素生成的主理想为极大理想**，那么利用模掉极大理想的商环是域就不难证明. 我们先证明前面一个断言，设 p 是不可约元素，且 I 为 R 的理想，$\langle p\rangle \subseteq I$，则由 R 为主理想整环，故存在 r 使得 $I = \langle r\rangle$，则 $r|p$，而 p 不可约，则 $r = p$ 或为单位，这表明 $I = R$ 或 $\langle p\rangle$，故 $\langle p\rangle$ 是极大理想.

现设 $p|ab$，则在商环 $R/\langle p\rangle$ 中有 $(a + \langle p\rangle)(b + \langle p\rangle) = ab + \langle p\rangle = 0 + \langle p\rangle$，又 $R/\langle p\rangle$ 为域，从而不妨 $a + \langle p\rangle = 0 + \langle p\rangle$，进而 $p|a$，即证 p 为素元素，故满足素条件. ♣

定理 2.7.2: 主理想整环的 Bezout 定理

设 R 为主理想整环，$a, b \in R$，且 d 为 a, b 的一个最大公因子，则存在 $u, v \in R$ 使得 $d = ua + vb$.

证明 由 R 为主理想整环，从而存在 d_1 使得 $\langle d_1\rangle = \langle a, b\rangle$，故有 $d_1|a, b$，从而 $d_1|d$，又 $d_1 \in \langle a, b\rangle$，从而存在 u_1, v_1 使得 $d_1 = u_1 a + v_1 b$，故可知 $d|a, b$ 进而 $d|d_1$，故 $d \sim d_1$，进而存在单位 ε 使得 $d = u_1\varepsilon a + v_1\varepsilon b = ua + vb$，即证. ♣

命题 2.7.2: 思考题

由前面的例子可知 $\mathbb{Z}[x]$ 不为主理想整环，从而举出一个不满足 Bezout 等式的例子.

解 很显然考虑 $f(x) = x$, $g(x) = 3$, 则 $(f, g) = 1$, 若存在 $u(x), v(x) \in \mathbb{Z}[x]$, 则 $3u(x)+xv(x) = 1$, 令 $x = 0$，则 $3u(0) = 1$，这与 $u(0) \in \mathbb{Z}$ 矛盾！即为一个反例. ♠

定义 2.7.2: 欧几里得环 (ED)：Euclidean Domain

设 R 为整环，如果存在从 R^* 到 $\mathbb{N}$(包含 0) 的一个映射 δ，使得对任何 $a, b \in R$，$b \neq 0$，存在 $q, r \in R$ 使得 $a = qb + r$，其中 $r = 0$ 或 $\delta(r) < \delta(b)$，则称 (R, δ) 为**欧几里得环**.

例 2.7.3. *对任意数域 $\mathbb{P}$，$\mathbb{P}[x]$ 为 ED，其中 $\delta(f(x)) = \deg(f(x))$.*

定理 2.7.3

欧几里得环为主理想整环，进而为唯一分解整环.

证明 设 I 为欧几里得环 R 的理想，若 I 为非平凡理想，则非负整数集合 $\{\delta(x)|x \in I\}$ 有最小值，设为 $\delta(a)$，则对任意 $b \in I$，作带余除法，存在 $q, r \in R$ 使得 $b = qa + r$，则 $r = b - qa \in I$，故 $\delta(r) \geq \delta(a)$，而 $r = 0$ 或 $\delta(r) < \delta(a)$，从而 $r = 0$，故可知 $b = qa$，进而 $I = \langle a\rangle$，这即表明 I 为主理想整环. 综上我们完成了证明. ♣

对于这几节涉及到的环，有如下包含关系 (真包含)

$$\text{域} \subset \text{欧几里得环} \subset \text{主理想整环} \subset \text{唯一分解整环} \subset \text{整环}$$

定理 2.7.4: Gauss 整数环是 ED

Gauss 整数环 $\mathbb{Z}[\sqrt{-1}]$ 是欧几里得环.

证明 对于 $\beta = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$，定义 $\delta(\beta) = a^2 + b^2$，从而任意 $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$，则 $\alpha\beta^{-1} = u + v\sqrt{-1} \in \mathbb{Q}[\sqrt{-1}]$, 从而存在 $c, d \in \mathbb{Z}$, 使得 $|c-u| \leq \frac{1}{2}$, $|d-v| \leq \frac{1}{2}$, 设 $\beta = c+d\sqrt{-1}$, 则取 $r = \alpha - q\beta$，则一方面 $\alpha = q\beta + r$，另一方面

$$\delta(r) = \delta(\beta)\delta(q - u - v\sqrt{-1}) \leq \frac{1}{2}\delta(\beta),$$

这即表明 δ 的选取使得 $\mathbb{Z}[\sqrt{-1}]$ 构成了欧几里得环. ♣

2.7.2 Exercises From Z.Fh

1.证明 $\langle a\rangle=\langle b\rangle$ 等价于 a,b 互相整除，在整环 R 中等价于 $a\sim b$. ♣

2.证明 由 c,d 互素，从而由 Bezout 定理，存在 $d'\in R$ 使得 $dd'+cc'=1$，故 $(d+\langle c\rangle)(d'+\langle c\rangle)=1+\langle c\rangle$，其中显然 1 和 c 互素，从而 $d'+\langle c\rangle$ 为其逆元，即证 S 构成群. ♣

3.证明 反证法，若 $a=bc$，则 $\langle a\rangle\subset\langle c\rangle\neq R$，矛盾. ♣

4.证明 (1) 注意到 R/I 的全体理想形如 J/I，其中 J 为 R 中包含 I 的理想，则由 R 为 PID，故存在 $a\in R$ 使得 $J=\langle a\rangle$，故 $J/I=\langle a+I\rangle$ 因此也为主理想，故 R/I 为主理想环.

但 R/I 不一定为 PID，因为它不一定为整环，如考虑 $\mathbb{Z}/4\mathbb{Z}$，不为整环，更不为 PID.

(2)R/I 中理想全体为 $\{J/I|I\subseteq J\text{为理想}\}$，则由 I,J 均为主理想，从而设 $I=\langle r\rangle$，$J=\langle a\rangle$，则 $a|r$，故 R/I 中理想与 r 的因子一一对应，又 r 的因子有限，因此只有有限个理想. ♣

5.证明 注意到 $1=x^5+x^3+1-x^3\cdot(x^2+1)$，则 $1\in\left\langle x^2+1,x^5+x^3+1\right\rangle$，故可知 $f(x)=1$. ♣

6.证明 考虑理想 $\langle x,y\rangle$ 即可. ♣

7.证明 验证其是整环是繁琐且平凡的，这里略去，我们定义 $\delta\left(a+b\cdot\dfrac{1+\sqrt{-3}}{2}\right)=a^2+ab+b^2$，因此任意 α,β，由模长的积性，只需证明存在 $t=x+y\sqrt{-3}$ 使得 $0\leq N\left(\dfrac{\alpha}{\beta}-t\right)<1$，因此等价于选取合适的 x,y 有 $\dfrac{(a-cx)^2+3(b-cy)^2}{c^2}\in[0,1)$，考虑 a,b 对 c 的带余除法，设 $a=cx+r$，$b=cy+r'$，其中 $|r|,|r'|\leq c/2$，进而我们有其模长 ≤ 1，若取到 1，则 $\dfrac{\alpha}{\beta}=x+y\sqrt{-3}+\dfrac{1+\sqrt{-3}}{2}\in R$，因此其模长实际为 0，综上所述，我们证明了这个环为欧几里得环. ♣

8. 过程完全仿照上一题即可.

9.证明 注意到 $1+\sqrt{-1}=\sqrt{-1}\cdot 2+(1-\sqrt{-1})$，$1+\sqrt{-1}=1\cdot 2+(-1+\sqrt{-1})$，且 $\delta(1-\sqrt{-1})=\delta(-1+\sqrt{-1})=2<\delta(2)$，故为一个例子. ♣

10.证明 考虑 $\delta(0)=0$，对任意 $a\in F^*$，$\delta(a)=1$，则任意 $a,b\in F^*$，$a=ab^{-1}b+0$，则 $0=\delta(0)<\delta(b)=1$，故可知域 F 为欧几里得环，即证. ♣

11.证明 我们证明 $\mathbb{Z}[\sqrt{-6}]$ 不为 PID，考虑生成理想 $I=\left\langle 2,2+\sqrt{-6}\right\rangle$，反证法，若 $\mathbb{Z}[\sqrt{-6}]$ 为 PID，则存在 $a+b\sqrt{-6}$ 使得 $\left\langle 2,2+\sqrt{-6}\right\rangle=\left\langle a+b\sqrt{-6}\right\rangle$，因此我们设 $2=\alpha(a+b\sqrt{-6})$，$2+\sqrt{-6}=\beta(a+b\sqrt{-6})$，因此 $N(\alpha)(a^2+6b^2)=4$，$N(\beta)(a^2+6b^2)=10$，因此 $a^2+6b^2=1,2$，显然不会为 2，故 $a+b\sqrt{-6}=\pm1$，进而 $I=R$，从而存在 γ,δ 使得 $2\gamma+(2+\sqrt{-6})\delta=1$，同时乘上 $2-\sqrt{-6}$，则有 $2-\sqrt{-6}=10\delta+2(2-\sqrt{-6})\gamma$，这表明 $2|2-\sqrt{-6}$，矛盾! ♣

12.证明 一方面，若 $a\in U$，由 $\delta(a)=\delta(a)\delta(1)$，则 $\delta(1)=1$，进一步 $\delta(a)\delta(a^{-1})=\delta(1)=1$，故 $\delta(a)=1=\delta(1)$.

另一方面，若 $\delta(a)=1$，则在 ED 中存在 a' 使得 $1=a'a+r$，且 $\delta(r)<\delta(a)=1$，故 $\delta(r)=0$ 即 $r=0$，因此 $a'a=1$，故 $a\in U$. ♣

13.证明 本题有误，题干应修改为 $\delta(ab)\geq\delta(a)\delta(b)$.

(1) 由 $\delta(a)\geq\delta(1)\delta(a)$ 故可知 $\delta(1)=1$，从而 $1=\delta(1)\geq\delta(u)\delta(u^{-1})$，故对任意单位 u 有

$\delta(u)=1$，从而设 $a\sim b$，则存在单位 u 使得 $a=ub$，故 $\delta(a)\geq\delta(u)\delta(b)\geq\delta(y^{-1})\delta(a)=\delta(a)$，从而可知 $\delta(a)=\delta(b)$，即证.

(2) 反证法，由 $\delta(ab)\geq\delta(a)\delta(b)\geq\delta(a)$，若 $\delta(ab)=\delta(a)$，则有 $\delta(b)\leq 1$，即 $\delta(b)=1$，而 $b\neq 0$，从而 $\delta(b)=1$，进而仿照 12 题不难得到 b 为单位，矛盾，即证. ♣

2.7.3 PID 不一定是 ED 的反例

本节我们将要证明的结果是整环 $R=\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-19})\right]$ 是主理想整环但不是欧几里得环，为了行文方便，记 $\theta=\frac{1}{2}(1+\sqrt{-19})$.

定理 2.7.5: R 不是 ED

整环 $R=\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-19})\right]$ 不是欧几里得环.

我们回忆如何证明一个整环不是 ED，一般有以下几种方法；

- 证明其不为 UFD(一般找到一个元素的两种分解方式，这在处理二次数域的代数整数环时尤其强大，比如在 $\mathbb{Z}[\sqrt{-6}]$ 中 $10=2\times 5=(2+\sqrt{-6})(2-\sqrt{-6})$)；
- 证明其不为 PID(一般思路是找到两个元素的生成理想，根据整除关系确定其对应的主理想，再通过 Bezout 等式寻找矛盾，如 $\mathbb{Z}[x]$ 是 UFD 但不是 PID，考虑生成理想 $\langle 2,x\rangle$，不难得到想要的矛盾)；
- 证明其没有 univeral side divisor(下面给出定义).

定义 2.7.3: univeral side divisor

设 $\widetilde{R}=U\cup\{0\}$ 即全体单位与零元，我们称 $u\in R-\widetilde{R}$(非单位的非零元) 为 **univeral side divisor**，如果任意 $x\in R$，存在 $z\in\widetilde{R}$ 使得 $u\mid x-z$. 等价地，每个 $x\in R$ 可以写成 $x=qu+z$，其中 u 不为单位不为 0，z 为单位或为 0.

下面我们将看到，具有 univeral side divisor 弱于 ED 的条件：

定理 2.7.6: ED 的一个性质

R 为不为域的整环，若 R 是 ED，则 R 中有 univeral side divisor.

证明 注意要求不为域是因为对域 F，$\widetilde{F}$ 可能为空集.

设 u 是 $R-\widetilde{R}$ 中模长最小的，下证其为 univeral side divisor，任意 $x\in R$，x 对 u 作带余除法 $x=qu+r$，则 $N(r)<N(u)$，因此 $r\in\widetilde{R}$，即证. ♣

下面我们就使用这条必要性质去证明 $\mathbb{Z}[\theta]$ 不为 ED：

证明 我们熟知二次数域的代数整环 $\mathbb{Z}[\theta]$ 中单位均只有 ±1(这是因为考虑模长 $N(a+b\omega)=(a+b\omega)(a+b\overline{\omega})$), 如 $N(a+b\theta)=a^2+ab+b^2\cdot5$, 因此不难观察到对 $a,b\in\mathbb{Z}$, $b\neq0$ 时, $N(a+b\theta)=a^2+ab+5b^2=(a+b/2)^2+19/4\cdot b^2\geq5$.

借助上面的事实, 我们要证明 R 中不存在 univeral side divisor, 事实上这里即要选取合适的 x, 讨论 $x,x\pm1$ 的因子. 先取 $x=2$, 则若有 u 为 usd, 则 $u|2-0$ 或 2 ± 1, 因为 u 非零非单位, 且 $u|2$ 或 3, 则 $N(u)|4,9$, 由上一段的观察, 可知 $u\in\{\pm2,\pm3\}$, 下一步再取 $x=\theta$, 易见 ±2 或 ±3 均不可能成为 $\theta-0$ 或 $\theta\pm1$ 的因子, 即是一个矛盾, 综上即证. ♣

下面我们考虑证明本节的第二部分:

定理 2.7.7: R 是 PID

整环 $R=\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-19})\right]$ 是主理想整环.

为了进一步刻画主理想整环和欧几里得环之间的区别, 我们引入 Dedekind-Hasse 模长

定义 2.7.4: Dedekind-Hasse Norm

我们定义 N 为一个 **Dedekind-Hasse Norm**, 如果任意 $r\in R$, $N(r)\in\mathbb{N}^*$, 且对任意 $a,b\in R$, 有以下两者之一一定成立:

- $b|a$ 等价地说 $a\in\langle b\rangle$ 或者 $\langle a,b\rangle=\langle b\rangle$;
- 存在 $s,t\in R$, $0<N(sa-tb)<N(b)$.

注: 不难看见, 欧几里得环中的模长是 Dedekind-Hasse 模长的特例, 注意到在 ED 中我们考虑 $a=tb+r$, 则 $r=0$(也即 $b|a$) 或者 $0<N(r)=N(a-tb)<N(b)$ 成立, 也即 ED 是 Dedekind-Hasse 模长 s 恒取 1 的特殊情形.

命题 2.7.3: PID 的重要刻画

整环 R 是 PID 当且仅当 R 有 Dedekind-Hasse 模长.

证明 一方面, 若整环 R 有 Dedekind-Hasse 模长, 则任意非零理想 I, 存在 $b\in I^*$ 使得 $N(b)$ 最小, 因此任意 $a\in I$, 由 $\langle a,b\rangle\subseteq I$, 故任意 $s,t\in R$, $N(sa-tb)\geq N(b)$, 从而 $a\in\langle b\rangle$, 进而 $I=\langle b\rangle$ 故为主理想, 即证 R 为 PID.

另一方面, 设 R 为 PID, 我们下面构造其 Dedekind-Hasse 模长, 令 $N(0)=0$, 任意单位 u, $N(u)=1$, 注意到 R 为 UFD, 因此其可分解为不可约元素乘积, 设 $a=p_1p_2\cdots p_n$, 则 $N(a)=2^n$, 显然 $N(ab)=N(a)N(b)$, 下证这为 Dedekind-Hasse 模长, 任意 $a,b\in R$, 若 $a\notin\langle b\rangle$, 从而设 $\langle a,b\rangle=\langle r\rangle$, 则 $r|b$, 但 $b\nmid r$(若不然 $b|a$, 则 $a\in\langle b\rangle$ 矛盾), 从而 $b=xr$, 且 x 不为单位, 则 $N(b)=N(x)N(r)>N(r)$, 故存在 $s,t\in R$, $sa-tb=r$ 满足要求, 即证. ♣

下面我们就证明在这个基础上，$\mathbb{Z}[\theta]$ 为 PID：

证明 我们下证 $N(a+b\theta)=a^2+ab+5b^2$ 是 R 上的 Dedekind-Hasse 模长，为此我们只需证，对任意 $\alpha,\beta\in R$ 且 $\alpha/\beta\notin R$ 则存在 $s,t\in R$ 使得 $0<N(s\alpha-t\beta)<N(\beta)$，而由 N 的积性，可知这等价于证明

$$0<N\left(\frac{\alpha}{\beta}s-t\right)<1,\quad \exists s,t\in R.\quad (*)$$

设 $\dfrac{\alpha}{\beta}=\dfrac{a+b\sqrt{-19}}{c}\in\mathbb{Q}[\sqrt{-19}]$，且 $\gcd(a,b,c)=1$，从而为了找到符合的 s,t，我们用待定系数法，设 $s=x+y\sqrt{-19}$，$t=z+w\sqrt{-19}$，因此我们有

$$\begin{aligned}\frac{\alpha}{\beta}s-t&=\frac{(a+b\sqrt{-19})(x+y\sqrt{-19})}{c}-(z+w\sqrt{-19})\\&=\frac{(ax-19by-cz)+\sqrt{-19}(bx+ay-cw)}{c},\end{aligned}$$

故我们有可以选取 x,y,w 使得 $bx+ay-cw=1$(Bezout 定理保证)，这取定之后，$ax-19by$ 也随之确定，因此考虑带余除法，$ax-19by=cz+r$，这里 r 最好的估计能有 $|r|\le c/2$，因此代入模长即有

$$N\left(\frac{\alpha}{\beta}s-t\right)=\frac{(ax-19by-cz)^2+19(bx+ay-cw)^2}{c^2}\le\frac{1}{4}+\frac{19}{c^2},$$

因此可知在这种取法下，对 $c\ge 5$ 时，$(*)$ 成立.

Case I. 若 $c=2$，则 a,b 具有不同的奇偶性，进一步容易看到，选取 $s=1$，$t=\dfrac{(a-1)+b\sqrt{-19}}{2}$ 即满足 $(*)$；

Case II. 若 $c=3$，则注意到 a^2+19b^2 不被 3 整除，因此设 $a^2+19b^2=3q+r$，则 $r=1,2$，取 $s=a-b\sqrt{-19}$，$t=q$，则我们有模长为 $r/3$ 不超过 1，也符合 $(*)$；

Case III. 若 $c=4$，则依然考虑 a^2+19b^2，则易见若 a,b 奇偶性不同，则 $a^2+19b^2=4q+r$，$r=1,3$，因此选取 $s=a-b\sqrt{-19}$，$t=q$ 即可；若 a,b 均为奇数，则注意到 $a^2+19b^2\equiv 4(\mathrm{mod}\,8)$，则考虑 $s=\dfrac{a-b\sqrt{-19}}{2}$ 即可. ♣

2.7.4 素元、不可约元、素理想、极大理想

我们这里对以上概念做进一步的区分，并证明一个 Striking result. 以下讨论限制在整环：

简单回忆一下，素元是指 $p|ab$ 蕴含 $p|a$ 或 $p|b$，不可约元是指 $p=ab$ 蕴含 a,b 中至少有一者为单位，由定义不难得到**素元一定是不可约元**，这是一条最广泛的结论，没有对整环加以任何限制，下一步在 UFD 中，其满足的素条件是指上一结论的逆命题，因此在 UFD、PID 乃至 ED 中，**素元和不可约元是一回事**.

整环已经没有多少讨论价值了，下面说的环至少是 UFD，我们关心素元 (不可约元) 生成的理想，这是主理想 (显然)，我们紧接着不难说明**素元生成的主理想在 UFD 中一定是素理想**，因为若 $ab\in(p)$，则 $a\in(p)$ 或 $b\in(p)$，这直接翻译过来就是：$p|ab$ 则 $p|a$ 或 $p|b$，因此上面的断言

是成立的. 但是反过来在 UFD 中则不对了，因为素理想甚至不可能是主理想. 所以下面我们的目光落在 PID 身上，在它上我们有I **为素理想当且仅当它是由一个素元 (不可约元) 生成的主理想**.

因为在 PID 中，每个理想都有非常好的表现形式，故以下结果不是那么让人惊讶:

定理 2.7.8: PID 的重要性质

PID 中每个素理想均为极大理想，反之亦然.

证明 一个之前漏提的一个普适事实是，对任意交换幺环，**极大理想均为素理想** (这看起来很容易和素元一定是不可约元弄混)，因此另一方面是普遍成立的.

我们来看前一方面，对任意素理想 (a)，注意这里 a 一定为素元，因此任意 $(a) \subseteq (b)$，则 $b|a$，因此 $b = a$ 或为单位，这即表明任何一个比 (a) 大的理想只能是 (a) 或者 R，即证. ♣

但当我们把目光放在 UFD 和 PID 间的联系时，我们就会得到一个十分令人惊讶的结论 (至少我第一次看感到惊讶)，PID 中素理想为极大理想这一看似普通的条件，却蕴含着极大能量:

定理 2.7.9: 令人震惊的结果

UFD 是 PID 当且仅当 UFD 的每个素理想是极大理想.

证明 其中一方面是上一定理所直接蕴含的：PID 有两条性质，UFD+ 素理想是极大理想，下面专心攻克另一方面：UFD+ **素理想是极大理想则是** PID.

We first prove that for two prime elements p and q, either they are associates, or there exists $a, b \in R$ such that $ap + bq = 1$. Indeed, if p and q are not associates, the ideals (p) and (q) cannot have containment relations (otherwise, say $(p) \subseteq (q)$, we must have $q|p$; which would immediately forces p and q to be associates). Now as nonzero prime ideals (such as (p) and (q)) are maximal, the ideal (p, q) must be the unit ideal, i.e. there exists $a, b \in R$ such that $ap+bq = 1$.

Next, we show that if, in the factorization of two elements $c, d \in R$, no prime factors of c are associates of prime factors of d, then there exists $a, b \in R$ such that $ac + bd = 1$. By induction, it suffices to prove that: if $(p_1, q) = (p_2, q) = (1)$, then $(p_1p_2, q) = (1)$. Indeed, write $\lambda_1 p_1 + \mu_1 q = 1$ and $\lambda_2 p_2 + \mu_2 q = 1$ for $\lambda_1, \lambda_2, \mu_1, \mu_2 \in R$, then

$$\lambda_1\lambda_2 p_1 p_2 = (1-\mu_1 q)(1-\mu_2 q) = 1-(\mu_1 + \mu_2 - \mu_1\mu_2 q)q$$

This implies that $(p_1p_2, q) = (1)$.

We finally prove that R is a PID. Let I be a nonzero ideal. Pick an element $x \in I$ with minimal number of prime factors. We show that $I = (x)$. If $y \in I - (x)$, then write $d = \gcd(x, y)$ and $x = dx_d$ and $y = dy_d$ with $x_d, y_d \in R$, andx_d, y_d have distinct prime factors. By the discussion above, there exist $a, b \in R$ such that $ax_d + by_d = 1$. This implies that $d \in I$, contradicting with the minimality of prime factors of $x \in I$. Thus I is a principal ideal. ♣

2.8 环上的多项式

2.8.1 Notes

环上多项式第一种定义——R 上序列

我们为了消解对一般多项式 $a_0 + a_1x + \cdots + a_nx^n$ 中文字 x 的关注，而把多项式看成是许多环 R 作直积的结构，在直积上定义对应运算，进而得到一个新的环，因此出于这种目的，我们以无穷序列的结构去定义：

定义 2.8.1: R 上的一元多项式

设 R 是一般的环，我们定义 R 的**一元多项式**是 R 上无穷序列

$$f = (a_n)_{n\in\mathbb{N}} = (a_0, a_1, a_2, \cdots), \quad \forall n \in \mathbb{N}, a_n \in R,$$

且满足 $\#\{n|a_n \neq 0\} < \infty$，也即不为 0 的项只有有限多个.

一个值得说明的注是，这里对不为 0 的项只有有限个的限制条件，对比一般多项式我们容易理解这种约定，而如果没有这个限制，我们称为 R 上的一个**形式幂级数**，在习题 8 中讨论了它的性质.

定义 2.8.2: R 上的一元多项式环

我们设 R 上全体一元多项式构成的集合为 S，我们下面在 S 上定义元素，使之成为环，任意 $f = (a_n)_{n\in\mathbb{N}}$，$g = (b_n)_{n\in\mathbb{N}}$，定义

$$\begin{aligned} f + g &= (c_n)_{n\in\mathbb{N}}, \quad \forall n \in \mathbb{N}, \quad c_n := a_n + b_n, \\ f \cdot g &= (d_n)_{n\in\mathbb{N}}, \quad \forall n \in \mathbb{N}, \quad d_n := \sum_{i=0}^{n} a_i b_{n-i} \end{aligned} .$$

不难验证 $(S, +, \cdot)$ 是一个良定义的环，且零元为 $(0, 0, \cdots)$.

有时为了方便，我们也引入文字 x，用 $R[x]$ 来等价代换 S，在后文中总是不对这两种记号作区分，而是自由的在计算论证中使用方便的那个记号，但切记这里 x 无任何实际意义，仅提示着我们运算规则.

下面是一些自然的观察与命题，揭示了 R 与 S 间的关系

定理 2.8.1: R 与其多项式环间的关系

1. R 为交换幺环当且仅当 S 为交换幺环；
2. R 无零因子当且仅当 S 无零因子，进而 R 为整环当且仅当 S 为整环.

在下一节中，我们将知道 R 为 UFD 则 S 为 UFD，但其余情形，有：

命题 2.8.1: 思考题

若 R 为 PID，$R[x]$ 是否一定为 PID? 若 R 为 ED，$R[x]$ 是否一定为 ED?

证明 两个命题的一个统一反例是 $R=\mathbb{Z}$，易见 $\mathbb{Z}$ 为 ED，但 $\mathbb{Z}[x]$ 不为 PID. ♣

在把 R 视为 S 的自然子环情形下，我们有这样一个有趣结论：

命题 2.8.2: 思考题

证明：若 R 为整环，则整环 S 的所有单位就是 R 的所有单位.

证明 这里即要证任意 $(a_n)_{n\in\mathbb{N}}(b_n)_{n\in\mathbb{N}}=(1,0,0,\cdots)$，则 $(a_n)_{n\in\mathbb{N}}=u$，$(b_n)_{n\in\mathbb{N}}=u^{-1}$. 设 $(a_n)_{n\in\mathbb{N}}$ 的次数为 m，$(b_n)_{n\in\mathbb{N}}$ 次数为 n，因此若 $m+n\geq 1$，则由 $a_mb_n=0$ 可知 $a_m=0$ 或 $b_n=0$，这与次数最高矛盾. ♣

既然 R 都可以视为 $R[x]$ 中的一部分，那么我们原来很不想用的文字 x，自然也可以在其中扮演一个顶有趣的角色，可以约定 $x=(0,1,0,\cdots)$，则在整环中，我们有

命题 2.8.3: 整环中 x 的性质

任给整环 R，设 U 为其单位群，则有

- 单项式 x 是 $R[x]$ 中的一个不可约元素且是素元素；
- $R[x]/(x)\cong R$；
- 设存在 $a\in R^*-U$(即 a 非零且不可逆)，则理想 (a,x) 不为主理想；
- 结合上两条，我们有 $R[x]$ 为 PID 则 R 为域.

证明 我们象征性地以若干评注代表证明，第一条需要注意的是只有在 UFD(满足素条件) 下不可约元素才始终是素元素，一般整环下只有素元素是不可约的，因此我们只需证明 x 不可约即可，借助多项式的度不难给出一个直接的证明.

第三条在 $R=\mathbb{Z}$ 时我们已经是熟知的，反证法，若 $(a,x)=(f)$，则 $f|a$，$f|x$，因此 $\deg f=0$，而 x 不可约，故 $f\in U$，从而 $(a,x)=R[x]$，因此存在 g,h 使得 $ag+xh=1$，故 ag 的常数项为 1，因此 $ag_0=1$，这与 a 非零非单位矛盾，即证.

对第四条，$R[x]$ 为 PID 时，x 为不可约元，进而为素元，进而 (x) 为素理想，进而为极大理想，进而 $R[x]/(x)$ 为域，进而 $R\cong R[x]/(x)$ 为域. ♣

对于更进一步整环上的多项式环性质，我们先收起好奇心，留到下一节讨论，我们先回到枯燥的一般环上，看看还有什么理论可以发展 (推广)，但这个环也不一般，下面如果不特殊说

明，研究的环均为**交换幺环** (回忆：此时多项式环也是交换幺环！).

另外，当我们讨论一个交换幺环包含另一个交换幺环为子环的时候，我们总是假设两个环的幺元相同，这是顶重要的，因为：

命题 2.8.4: 思考题

存在 $R \subseteq R_1$ 为均为交换幺环，但幺元不同.

解 我们考虑 $R_1 = \mathbb{Z} \times \mathbb{Z}$，$R = \mathbb{Z} \times \{0\}$，前者幺元为 $(1,1)$，后者为 $(1,0)$. ♠

我们下面讨论的出发点是：设 $R \subseteq R_1$，则考虑 R 上的每一个多项式 f，我们将任意 $a \in R_1$ 代入 f 得到 $f(a) \in R_1$，因此 $f \in R[x]$ 可以看作是 R_1 到 R_1 的映射，换句话说，我们要从**多项式函数**的视角去理解多项式环.

命题 2.8.5: 思考题

高等代数中我们学过，数域上的两个多项式如果看成多项式函数相同，则两个多项式一定相等. 举例说明，上面的结论对一般环上的多项式不成立.

解 一个顶重要的注是：多项式函数相同意味着映射相同意味着定义域与陪域之间的对应相同，而多项式相等是指多项式的对应系数相等，与文字 x 无关 (不妨从无穷序列角度理解).

在有了上面这个认知之后，例子便是容易的了，考虑 $\mathbb{Z}_2$ 上的多项式，且取值也在 $\mathbb{Z}_2$ 上，则考虑多项式 $x + x^2$ 和 0，显然作为多项式，对应系数不同，一定不同，但是作为 $\mathbb{Z}_2$ 上的多项式函数，其之恒为 $0(\bar{1} + \bar{1} = \bar{0})$，故作用效果是一样的，，因此作为函数是一样的. ♠

为了进一步明确多项式与多项函数，我们方便地引入以下记号：

定义 2.8.3: 环 R 的自映射环

设 R 为交换幺环，并记所有从 R 到自身的映射的集合为

$$\mathcal{F}(R) := \{\phi \in R \times R | \phi\text{为一个映射}\}.$$

并且我们定义 $\mathcal{F}(R)$ 上的和与乘，$\phi + \psi : R \to R$，$a \mapsto (\phi + \psi)(a) := \phi(a) + \psi(a)$，以及乘积为 $\phi\psi : R \to R$，$a \mapsto (\phi\psi)(a) = \phi(a)\psi(a)$. 不难验证 $\mathcal{F}(R)$ 是交换幺环，其中幺元为 $e : R \to R$，$a \mapsto e(a) = 1$，我们称为 R 的**自映射环**.

注：本质上，$\mathcal{F}(R)$ 是全体定义于 R 取值于 R 的函数，因此乘法定义成元素相乘而不是映射复合就不难理解了，且这也需要与自同态构成的集合作区分 (它关于加法和乘法封闭吗？).

多项式函数

下面我们明确一下什么是多项式函数：

定义 2.8.4: 多项式函数

任取 $a_0,\cdots,a_n\in R$，我们定义如下映射 $R\to R$，$u\mapsto a_0+a_1u+a_2u^2+\cdots+a_nu^n$，对于这样的映射 (函数) 成为 R 上的一个**多项式函数**，进一步任给多项式

$$f=\sum_{n\geq 0}a_nx^n\in R[x],$$

我们可以构造一个多项式函数 $f:R\to R$，$u\mapsto f(u):=\sum_{n\geq 0}a_nu^n$，因此可以看见这样定义的 f 是取值于 R 结果为 R 的函数 (自映射)，也即 $f\in\mathcal{F}(R)$.

注：在这个观点下，我们可以将任一个 $R[x]$ 中的元素 f，几乎不加任何补充的，理解为 $\mathcal{F}(R)$(自映射环，定义域和值域相同的函数) 中元素，更准确的，记为 $\Phi_R:R[x]\to\mathcal{F}(R)$，本质上就是把原本的文字赋予了意义，这个意义取自 R.

命题 2.8.6: 一个熟练定义的练习

映射 $\Phi_R:R[x]\to\mathcal{F}(R)$ 是一个环同态.

证明 加法是内蕴的，为了保持乘法运算，我们即要希望 $\Phi_R(fg)=\Phi_R(f)\cdot\Phi_R(g)$，(这里类似于验证函子与自然变换)，要证明相等，这里等号两边都是映射，因此我们要随便选一个 $a\in R$，代入摊摊手一看，确实成立. ♣

更一般地，我们可以保持系数所在的环 R 不变，但是作用的定义域和陪域在更大的一个环里，比如 $R\subseteq R_1$，这里 R 为与 R_1 具有相同幺元的交换幺环子环，则可以自然定义 $\Phi_{R_1}:R[x]\to\mathcal{F}(R_1)$，值得注意的是尽管我们熟悉数域时 $R[x]$ 中元素不同，不管定义域 R_1 啥样，$\mathcal{F}(R_1)$ 中对应函数也不同，但是这对一般环不成立 (见命题 2.8.5 的讨论).

但是令人惊奇的，我们如果适当扩大定义域 R_1，则命题反而可能成立：

定理 2.8.2: Φ_{R_1} 为单同态

设 R 为交换幺环，则存在交换幺环 $R_1\supset R$，有 Φ_{R_1} 为单同态，也即任何 $R[x]$ 中两个不同的多项式作为 R_1 上的函数也不同.

解 我们自然会去考虑 $R_1=R[x]$，从而 $\Phi_{R_1}:R[x]\to\mathcal{F}(R_1)$ 满足任意 $f=a_0+\cdots+a_nx^n\in R[x]$，对 $g\in R_1$，$\Phi_{R_1}(f)(g)=a_0+\cdots+a_ng^n$，因此对 $R[x]$ 中 $f_1\neq f_2$，我们下证 $\Phi_{R_1}(f_1)\neq\Phi_{R_1(f_2)}$，也即要证存在 g 使得 $\Phi_{R_1}(f_1)(g)\neq\Phi_{R_1(f_2)}(g)$，也即 $f_1(g)\neq f_2(g)$，故取 $g=x\in R[x]$ 即可. ♠

下面我们从多项式函数过渡到借助大环为定义域引入**环的扩张**：

定义 2.8.5: 赋值映射、代数元、超越元

给定 $u \in R_1 \supset R$，考虑 $R[x]$ 上的赋值映射 $\varphi_u : R[x] \to R_1$，$f \mapsto f(u)$，进一步我们称 $u \in R_1$ 为 R 上的

- **代数元**，如果存在 $f \in R[x] - \{0\} = (R[x])^*$，使得 $\varphi_u(f) = f(u) = 0$；
- **超越元**，如果任意 $f \in R[x] - \{0\} = (R[x])^*$，均有 $\varphi_u(f) = f(u) \neq 0$.

超越元和代数元有许多平凡的等价刻画，这里不再摘录，这里只选取其一说明：

定理 2.8.3: 超越元与 R 生成的子环与 R 多项式环同构

任取 $u \in R_1$，$\varphi_u : R[x] \to R_1$ 为赋值映射，则 u 为代数元当且仅当 $\mathrm{Ker}\varphi_u \neq 0$，$U$ 为超越元当且仅当 $\mathrm{Ker}\varphi_u = 0$，进一步可知后者表明 u 为超越元当且仅当 φ_u 为从 $R[x]$ 到 $\mathrm{Im}\varphi_u(R[x]) = R[u]$ 的环同构.

环上多项式第二种定义——利用生成元的扩张

现在我们从代数元和生成元的角度去定义多项式环：

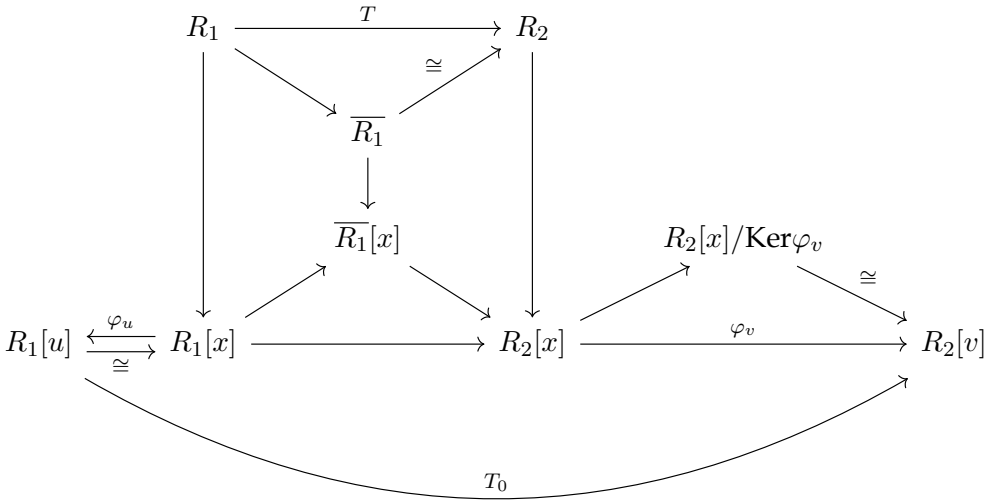
定义 2.8.6: 多项式环

R 为交换幺环，R_1 为包含 R 为子环的交换幺环 (幺元相同)，称 R_1 为 R 上的多项式环，若存在 $u \in R_1$ 为 R 上的超越元，且 $R_1 = R[u]$，称 u 为 R_1 在 R 上的**生成元**.

命题 2.8.7: 思考题

R_1 为 R 上的多项式环，生成元是否唯一？

解 不一定，如考虑 $\mathbb{Z}[\sqrt{-1}]$ 为 $\mathbb{Z}$ 上的多项式环，但 $\sqrt{-1}$ 和 $-\sqrt{-1}$ 均为生成元. ♠



2.9 整环上的多项式

我们本节开始考虑整环上的多项式，为了区分，这里统一用 $D[x]$ 表示.

2.10 2021 伯苓班抽象代数 I 期末考试

Problem 1. (20 分) 判断下列命题是否正确, 如果正确请给出证明，不正确请举出反例.

1. 如果二元关系 R 满足对称性和传递性，那么它一定满足反身性;
2. 群 G 中所有有限阶元素组成的集合 H 构成 G 的正规子群;
3. 如果 A 是环 R 的素理想，P 是 A 的素理想，那么 P 是 R 的素理想;
4. 对任意无限整环 R，都存在 $u, v \in R, u, v \neq 0$，使得 $\{ku + lv | k, l \in \mathbb{Z}\}$ 是无限集.

解 1. 错误，考虑 $\mathbb{R}$ 上的二元关系 $a\mathrm{R}b$ 等价于 $ab > 0$，不难看见满足传递性和对称性，但 $0 \not\mathrm{R} 0$;

2. 错误，考虑群 $\langle a, b | a^2 = b^2 = 1 \rangle = \{1, a, b, ab, ba, aba, bab, \cdots\}$，因此容易看见有限阶元构成的集合为 $\{1, a, b\}$ 显然不构成群，更不可能为正规子群;

3. 错误，考虑 $R = \mathbb{Q}[x]$ 为 PID，则显然 $A = \langle x^2 + 1 \rangle$ 为素理想，$P = \langle (x^2 + 1)(x + 1) \rangle$ 为 A 的素理想，但明显 P 不是 R 的素理想，因为 $(x^2 + 1)(x + 1)$ 可约，不是素元 (不可约元);

4. 错误，考虑整环 $\mathbb{Z}_2[x]$，则任意 $u = x^n + a_{n-1}x^{n-1} + \cdots a_0$，$v = x^m + b_{m-1}x^{m-1} + \cdots b_0$，$\{ku + lv | k, l \in \mathbb{Z}\}$ 至多有 $2^{\max\{m,n\}}$ 个元素 (每项系数前只能取 0 或 1). ♠

Problem 2. (20 分) 幺环 R 中，证明：任意 $a, b \in R, e-ab$ 可逆当且仅当 $e-ba$ 可逆.

证明 不妨假设 $e - ab$ 可逆，则记 $r = e + b(e - ab)^{-1}a$，下证其为 $e - ba$ 的逆元，注意到 $(e - ba)r = e - ba + b(e - ab)^{-1}a - bab(e - ab)^{-1}a$，利用 $ab(e - ab)^{-1} = e - (e - ab)^{-1}$，不难得到 $(e - ab)r = e$，同理不难证明 $r(e - ba) = e$，进而即证. ♣

Problem 3. (20 分) 设群 G 满足 $|G| = 120$，$H < G$，$|H| = 24$. 证明：如果存在 $g \in G-H$，使得 $gHg^{-1} = H$，那么 $H \lhd G$.

证明 注意到 $H < N_G(H) < G$，从而可知 $24 = |H| | |N_G(H)|$，且 $|N_G(H)| | |G| = 120$，因此 $|N_G(H)| = 24$ 或 120，也即 $N_G(H) = H$ 或 G，而存在 $g \notin H$ 使得 $g \in N_G(H)$，因此 $N_G(H) = H$ 进而 H 为正规子群，即证. ♣

Problem 4. (15 分) 证明如果无零因子环 R 满足 $|R|$ 是偶数，那么环 R 的特征为 2.

证明 我们熟知由于无零因子环 $|R|<\infty$，因此每个非零元素关于加法具有相同的阶，且为素数 p，因此 R 可划分为若干 p 阶加法循环群 (去掉零元) 的不交并，也即

$$R=\{0\}\bigcup\{a_1,\cdots,(p-1)a_1\}\bigcup\cdots\bigcup\{a_k,\cdots,(p-1)a_k\},$$

因此我们有 $|R|=1+k(p-1)$，又注意到 $|R|$ 是偶数，因此 $k(p-1)$ 为奇数，故 $p-1$ 为奇数，这表明 $p=2$，故环 R 的特征为 2. ♣

Problem 5. (15 分) 设 G_1 是 $\{\mathbb{Q};+\}$ 的真子群，证明：存在 G_2，其为 $\{\mathbb{Q};+\}$ 的真子群且 $G_1\subseteq G_2, G_1\neq G_2$.

解 任取 $x\in\mathbb{Q}-G_1$，从而考虑 $G_2=\langle G_1,x\rangle$ 为 G_2 和 x 共同生成的群，则一方面显然 $G_1\subseteq G_2, G_1\neq G_2$，另一方面，任取 $y\in G_1$，设 $\dfrac{y}{x}=\dfrac{p}{q}$，这里 $p,q\in\mathbb{Z}$，我们断言 $\dfrac{x}{p}\notin G_2$，反证法，若不然，则存在 $g\in G_1$，$n\in\mathbb{Z}$ 使得 $\dfrac{x}{p}=g+nx$，故 $x=pg+npx=pg+nqy\in G_1$，矛盾!

综上，$G_2=\langle G_1,x\rangle$ 为一个符合题意的构造. ♠

Problem 6. (10 分) 交换环 R 无非零幂零元. 证明：对于 $u,v\in R$，如果存在 $a,b\in\mathbb{N},(a,b)=1$ 使得 $u^a=v^a,u^b=v^b$ 则 $u=v$.

证明 由 $(a,b)=1$，不妨设存在 $m,n\in\mathbb{N}$ 使得 $am-bn=1$，因此 $u\cdot u^{bn}=u^{am}=v^{am}=v^{1+bn}=v\cdot u^{bn}$，因此 $(u-v)\cdot u^{bn}=0$，进而 $[(u-v)u]^{bn}=0$，而 R 中无非零幂零元，故 $(u-v)u=0$，同理 $(u-v)v=0$，因此 $(u-v)^2=0$，进而 $u=v$，即证. ♣

吐槽：极其厌恶考试的时候考这种不涉及本质知识，纯粹是初等奇技淫巧的无趣题 (当然竞赛除外)，只能体现谁更能灵光一现，这与厚积薄发的数学学习思想相违背，只能体现命题人为了刁难而刁难的低水准.

3 模论

3.1 模的基本概念

3.1.1 Notes

定义 3.1.1: 模的定义

设 R 是一个环 (不必要求交换幺环)，我们称一个 Abel 群 M 是一个**左 R 模**，如果存在 $\phi : R \times M \to M$，$(r, m) \mapsto rm$ 使得对任何 $r, s \in R$，$m, n \in M$，有

- 满足“系数加法”分配律：$(r+s)m = rm + sm$；
- 满足“向量加法”分配律：$r(m+n) = rm + rn$；
- 满足系数乘法结合律：$(rs)m = r(sm)$；
- 若 R 为幺环，则对幺元 1，$1m = m$.

注：事实上模 M 就是环 R 上的线性空间，我们只是试图将域上线性空间上的结果照搬到模上，如线性变换 (对应的矩阵理论)，包括线性空间的运算 (直和，商空间).

定义 3.1.2: 子模

我们称 N 是 M 的子模，如果满足

- N 是加法群 M 的子群；
- 任意 $a \in R$，$x \in N$，有 $ax \in N$.

例 3.1.1. 关于模的一个简单例子便是环 R 自己，以及不难根据子模上乘法的封闭性，可知 R 作为 $R-$ 模的所有子模为其全体左理想. 容易看到，当 R 交换时，R 作为自己的左模或右模均是一致的，一个自然的问题是是否有左模，右模不同的例子？

考虑 $R = \mathbb{R}^{2\times 2}$，则考虑

$$M := \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$$

显然是 R 作为左 $R-$ 模的子模，但不是作为右 $R-$ 模的子模，这表明左右模不同.

例 3.1.2. 任何一个 *Abel* 群均可看成一个 $\mathbb{Z}$ 模，反之亦然. 若存在 $m \in \mathbb{Z}$ 使得任意 $x \in M$ 有 $mx = 0$，则 M 可看成一个 $\mathbb{Z}_m$ 模，这事实上由一个更一般的结果保证：若 I 为 R 双边理想，且 I 零化 M(即 $I \subseteq \mathrm{Ann}(M)$)，则可将 R 模 M 看作 R/I 模.

定义 3.1.3: R 代数

设 R 为交换幺环，我们称一个幺环 A 是R **代数**，如果存在环同态 $f : R \to A$，使得 $f(1_R) = 1_A$，并且 $f(R)$ 作为 A 的子环包含在 A 的中心中.

注: A 作为 R 代数, 容易看到 A 可自然视为 R 双模, 事实上只需定义 $r\cdot a = a\cdot r = f(r)a = af(r)$, 因此如果我们想回忆 R 代数的定义，一个合适的方式是幺环，进一步有 R 到 A 的同态，且同态像总与 A 中元素可交换.

定义 3.1.4: R 代数同态

设 A, B 为两个 R 代数同态，一个 R 代数同态是一个环同态，保持幺元，以及保持 R 系数的乘法，即 $\varphi(r \cdot a) = r \cdot \varphi(b)$.

例 3.1.3. 每个交换幺环 R 都可以看作一个自然的 $\mathbb{Z}$ 代数，事实上只需要 $f(n) = n1_A$ 即可.

模的生成与运算

例 3.1.4 (有限生成模的子模)**.** 对于有限生成模的子模，我们直觉会想这也一定是有限生成的，但这可不一定对哩! 聪明的读者很快会意识到: 考虑任一个交换幺环 R, 则其作为自己的 R 模，当然是有限生成的, 因为有生成元为幺元! 那么其子模均是其理想对应的 R 模, 这可不见得是有限生成的, 一个乍一看比较奇怪的例子是考虑域 F 上的无穷元多项式环 $R = F[x_1, x_2, \cdots, x_n, \cdots]$, 它的一个子模 (理想)$(x_1, x_2, \cdots)$ 肯定不是有限生成的.

但是对 R 模的 R 做一定限制，事情便豁然开朗，那便是若 R 为 *PID*，则其上有限生成模的子模一定是有限生成的，这个事情看起来比较离奇，但核心在于 *PID* 与 *Bezout* 等式间密不可分的联系，以及 *Bezout* 等式这一项重要结果在后续论证中的作用，未来我们事实上能得到一些关于 *PID* 上有限生成模有价值的结构定理呢!

定义 3.1.5: 模的直和

设 M_i，$1 \le i \le s$ 为 M 的子模，满足 $M = M_1 + M_2 + \cdots + M_s$，则下面四个条件等价:

- $M = M_1 \oplus M_2 \oplus \cdots \oplus M_s$;
- 将 $m \in M$ 表示成 $m_1 + \cdots + m_s$，其中 $m_i \in M_i$ 的方式唯一;
- 若 $m_1 + \cdots + m_s = 0$，且 $m_i \in M_i$，则 $m_i = 0$，任意 i;
- 对任何 i，我们有 $M_i \cap \left(\bigcap_{j \neq i} M_j \right) = \{0\}$.

注：一个经典易混淆的问题是直积与直和，粗略来讲，直积是写成括号里分量形式，直和则是写成一个加法式子，心理上和技术上我们都已确信在有限情形下，两者是完全一样的，但是在无限情形，对于直和中的加法式子，无限项加法很难良好定义 (注意这是代数不是分析！)，因此此时无限项直和里总约定只有有限项不为 0(直积的子结构)，但括号一直延伸下去总没什么太大问题，因此直积不必有有限项不为 0 的要求.

商模和模同态

定义 3.1.6: 模同态

设 R 为环，M,N 为 R 模，若 $\varphi: M\to N$ 为**模同态**，如果

- $\varphi(x+y)=\varphi(x)+\varphi(y)$，任意 $x,y\in M$；
- $\varphi(rx)=r\varphi(x)$，任意 $r\in R$，$x\in M$.

我们把从 M 到 N 的模同态收集起来，构成的集合记为 $\mathrm{Hom}_R(M,N)$.

例 3.1.5. 设 R 为环，I 为 R 的双边理想，且 M,N 为被 I 零化的 R 模，即 $I\subseteq \mathrm{Ann}(M),\mathrm{Ann}(N)$，则任意 M 到 N 的 R 模同态可自然看成 R/I 模同态，因为两个模可以看成 R/I 模.

定理 3.1.1: Hom 的函子性质

若 R 为交换环，给定 R 模 M，则 $\mathrm{Hom}_R(\cdot,M)$ 是从 $\mathsf{R}_{\mathsf{Mod}}$ 到 $\mathsf{R}_{\mathsf{Mod}}$ 范畴的反变函子.

证明 为了证明 $\mathrm{Hom}_R(\cdot,M)$ 是函子，我们需要验证两件事情：

1. 作用在对象上，对任意 $A\in \mathsf{R}_{\mathsf{Mod}}$，我们需要证明 $\mathrm{Hom}_R(A,M)$ 为一个 R 模，加法是自然的，其中乘法可以定义为任意 $m\in M$，$(r\varphi)(m):=\varphi(rm)$，这里需要 R 的交换性以保证系数乘法的结合律
$$r(s\varphi)(m)=\varphi(srm)=\varphi(rsm)=(rs)\varphi(m),$$
由此不难知道有 $\mathrm{Hom}_R(A,M)\in \mathsf{R}_{\mathsf{Mod}}$，故可知在对象上符合定义.

2. 作用在态射上，设任意 $f: A\to B$，这里 A,B 均为 R 模，函子作用下这个态射 (R 模同态) 我们记为 f_*，则任意 $g\in \mathrm{Hom}_R(B,M)$，可以定义 $f_*g=g\circ f\in \mathrm{Hom}_R(A,M)$，由此可见 $f_*: \mathrm{Hom}_R(B,M)\to \mathrm{Hom}_R(A,M)$，即为一个反变函子.

综上我们证明了 $\mathrm{Hom}_R(\cdot,M)$ 是从 $\mathsf{R}_{\mathsf{Mod}}$ 到 $\mathsf{R}_{\mathsf{Mod}}$ 范畴的反变函子. ♣

定理 3.1.2

若 R 为交换环，则 $(\mathrm{End}_R(M),+,\circ)$ 是一个 R 代数.

类似于群同构与环同构基本定理，我们有：

定理 3.1.3: 环同构定理

1. (模第一同构定理)

   设 M, N 为 R 模，$f : M \to N$ 为 R 模同态，则有 $M/\mathrm{Ker}f \cong f(M)$；

2. (模第二同构定理)

   设 A, B 为 R 模 M 的子模，则 $(A+B)/B \cong A/(A \cap B)$；

3. (模第三同构定理)

   设 M 为 R 模，A, B 为 M 的子模，且 $A \subseteq B$，则 $(M/A)/(B/A) \cong M/B$.

4. (模第四同构定理)

   设 N 为 M 的子模，则 M 中包含 N 的子模 A 与商模 M/N 的子模 A/N 形成一个一一对应.

未来将会用到的一个重要结论是：

命题 3.1.1: 直和的同构

设 M 为 R 模，$M_1, \cdots, M_s$ 为 M 的子模，且 $M = M_1 \oplus \cdots \oplus M_s$，又 N 是 M 的子模，且 $N = N_1 \oplus \cdots \oplus N_s$，其中 $N_i \subseteq M_i$，$i = 1, 2, \cdots, s$，则有

$$M/N \cong M_1/N_1 \oplus M_2/N_2 \oplus \cdots \oplus M_s/N_s.$$

3.1.2 Some Meaningful Exercises

Problem 1. 本题我们关心在 Abel 群上定义 $\mathbb{Q}$ 模结构的问题：设 $(G, +, 0)$ 为 Abel 群

1. 若 G 中存在有限阶非零元素，也即存在 $g \in G$，$n \in \mathbb{Z}$ 使得 $ng = 0$，证明：G 上没有 $\mathbb{Q}$ 模结构，特别地，若 G 有限则没有 $\mathbb{Q}$ 模结构；

2. 证明：若 G 上存在 $\mathbb{Q}$ 模结构，则该模结构唯一.

证明 回忆一个模结构本质上是指定了一个 $R \times M \to M$ 的一个映射，对第一问而言，若有模结构 φ，则有 $g = \varphi(1, g) = \varphi(1/n, ng) = 0$，矛盾！对第二问，若有两个不同的模结构 φ, ψ，即有 $h = \varphi(p/q, g) - \psi(p/q, g) \neq 0$，但是注意到 $qh = pg - pg = 0$，即 h 为 G 中有限阶元素，由第一问可知矛盾，综上我们完成了证明. ♣

3.2 自由模与环上的线性代数

3.2.1 Notes

首先祭出 Dummit 上的图，这张图足以说明我们想干的事情了：

Terminology for R any Ring	**Terminology for R a Field**
M is an R-module	M is a vector space over R
m is an element of M	m is a vector in M
α is a ring element	α is a scalar
N is a submodule of M	N is a subspace of M
M/N is a quotient module	M/N is a quotient space
M is a free module of rank n	M is a vector space of dimension n
M is a finitely generated module	M is a finite dimensional vector space
M is a nonzero cyclic module	M is a 1-dimensional vector space
$\varphi : M \to N$ is an R-module homomorphism	$\varphi : M \to N$ is a linear transformation
M and N are isomorphic as R-modules	M and N are isomorphic vector spaces
the subset A of M generates M	the subset A of M spans M
$M = RA$	each element of M is a linear combination of elements of A i.e., $M = \text{Span}(A)$

定义 3.2.1: 自由模

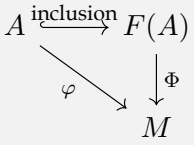
$R-$ 模 F 称为是 F 子集 A 的**自由模**，如果任意 $x \in F^*$，存在**唯一**的 R 中非零元素 $r_1, r_2, \cdots, r_n$ 以及**唯一**的 A 中元素 $a_1, a_2, \cdots, a_n$ 使得 $x = r_1a_1 + \cdots + r_na_n$，进而我们称 A 为 F 的一组基.

注：一个直觉的错误是，自由模似乎就是若干子模的直和？但是注意，自由模的要求可比直和高的多哩！对 N 的两个子模 $N_1 \oplus N_2$，我们只是说对 n 可被唯一表示成 $n_1 + n_2$，但自由模对系数还作了唯一性的要求 (后面将看到，系数唯一本质上要求了线性无关).

一个有价值的例子是 $\mathbb{Z}$ 模 $N_1 = N_2 = \mathbb{Z}_2$，毫无疑问直和是合理的，但是注意对 $(1,0) \in N_1$，$3(1,0) \in N_1$，换言之 $(1,1) = a(1,0) + b(0,1)$，这里 a, b 可以取任意奇数！简单来讲，原因在于 $2(1,0) = (0,0)$，线性相关！

定理 3.2.1: 自由模的泛性质

对任意集合 A，存在一个 A 上的自由 R 模 $F(A)$ 满足如下**泛性质**：对任意 R 模 M，一旦确定从集合 A 到集合 M 的映射 φ，则存在**唯一**的 R 模同态 $\Phi : F(A) \to M$ 使得对任意 $a \in A$，$\Phi(a) = \varphi(a)$，也即有下图交换：



当 $A=\{a_1,a_2,\cdots,a_n\}$ 为有限集时，则 $F(A)=Ra_1\oplus Ra_2\oplus\cdots\oplus Ra_n\cong R^n$.

注：等等，上一个注不是说 $F(A)$ 这种自由模不是直和么，这咋又写成直和了？注意，这里的直和分量 Ra_1 与之前不同，可以理解成 “a_1 不是有限阶元” 了，即 $ra_i=0$ 当且仅当 $r=0$，需要小心这其中的区别.

按上述定义给出的自由模十分的自然好用，但是你开课本选择从泛性质角度反过来定义自由模，是如下表述的：

定义 3.2.2: 从泛性质出发定义的自由模

设 R 为一个幺环，M 为一个 R 模. 我们称 M 为一个**秩为 n 的自由模**，若 M 中存在 n 个元素 $u_1,\cdots,u_n$，使得对任意 R 模 N，以及 N 中任意的 n 个元素 $v_1,\cdots,v_n$，有唯一的模同态：$\varphi:M\to N$，满足对任意 $1\leq j\leq n$，使得 $\varphi(u_j)=v_j$. 我们进一步称 $\{u_1,\cdots,u_n\}$ 为 M 的一组基.

在这个定义的基础上，我们有：

定理 3.2.2: 自由模的基的刻画

设 M 为幺环 R 上的模，$u_1,u_2,\cdots,u_m\in M$，则 M 为自由模，且 $u_1,u_2,\cdots,u_m$ 为一组基的充分必要条件为

1. $u_1,\cdots,u_m$ 是 M 的一组是生成元，也即 $M=Ru_1+Ru_2+\cdots+Ru_m$，也即任取 $u\in M$，存在 $r^i\in R$ 使得 $u=r^iu_i$；
2. $u_1,\cdots,u_m$ 是 R 线性无关的.

证明 核心是利用泛性质，先考虑必要性，为证是生成元，即证 $N=Ru_1+\cdots+Ru_m=M$，从而考虑 $M\to N$ 的模同态与 $M\to M$ 内射模同态，从而两者复合为单位映射即证. 为证线性无关，则考虑到 R^m 的映射，注意到 R^m 也为自由模，从而再次利用泛性质，可以证明 $M\cong R^m$，即可证明. 充分性是自然的，我们不做证明 (嘻嘻). ♣

证明中最核心的一句话是：

推论 3.2.1: 幺环上的自由模

设 R 为幺环，M 为一个 R 模，则 M 为一个秩为 m 的 R 模当且仅当 M 与 R^m 同构.

注：我们这里无法得到自由模的秩是唯一的，事实上对幺环并不唯一，交换幺环才唯一.

环上的矩阵

命题 3.2.1: 交换幺环上的可逆矩阵

设 R 为交换幺环，则 $A\in R^{n\times n}$ 可逆当且仅当$\det(A)$ 是 R 中单位，且若 $AB=\boldsymbol{I}_n$，则必有 $B=A^{-1}$，因此 $BA=\boldsymbol{I}_n$，事实上 $B=(\det A)^{-1}A^*$.

我们依旧希望研究矩阵的标准型，一般交换幺环性质太差，不屑于研究 (这里点名一个 shit 里找糖的学科)，下面考虑的环都是 PID，为了区分，用 D 代替：

定义 3.2.3: PID 上的矩阵等价

任取矩阵 $A,B\in D^{n\times m}$，我们称 A 与 B **等价**，若存在可逆矩阵 $P\in R^{m\times m}$，$Q\in R^{n\times n}$ 满足有 $B=QAP$.

我们利用 PID 上具有 Bezout 等式的特性，对 $d=(a,b)$，且 $a=da'$，$b=db'$，且 $pa'+qb'=1$，因此我们注意到

$$\begin{pmatrix}a & b\end{pmatrix}\begin{pmatrix}p & -b'\\ q & a'\end{pmatrix}=\begin{pmatrix}d & 0\end{pmatrix},$$

故总能使得下面这一标准型成立 (注意利用 $pa'+qb'=1$ 可知矩阵可逆)：

定理 3.2.3: 主理想整环上的相抵标准型

设 D 为 PID，则 D 上任一 $m\times n$ 矩阵 A 等价于对角矩阵 $\operatorname{diag}\{d_1,\cdots,d_r,0,\cdots,0\}$，且 $d_i\mid d_{i+1}$，称该对角阵为 A 的**标准型**，r 为 A 的**秩**.

定义 3.2.4: 等价变换的不变量

称 $d_1,\cdots,d_r$ 为**不变因子**，$\Delta_i=d_1\cdots d_i$ 为**行列式因子**，它们均为不变量.

我们以一个具体的算例表明求相抵标准型的算法：

例 3.2.1. 我们下求 $\operatorname{diag}\{4,6,9\}$ 在 $\mathbb{Z}$ 上的标准型，事实上容易求出 $\Delta_1=1,\Delta_2=\gcd(24,54,36)=6$，$\Delta_3=216$，因此不变因子为 $d_1=1$，$d_2=6$，$d_3=36$，那么如何求可逆矩阵 P,Q 呢？首先注意，左乘是行变换，右乘是列变换

$$\begin{pmatrix}4&&\\&6&\\&&9\end{pmatrix}\xrightarrow{r_3+r_1}\begin{pmatrix}4&&9\\&6&\\&&9\end{pmatrix}\xrightarrow{\text{对第一行 }4,9\text{ 右乘}}\begin{pmatrix}1&&0\\&6&\\9&&36\end{pmatrix}\xrightarrow{-9r_1+r_3}\begin{pmatrix}1&&\\&6&\\&&36\end{pmatrix},$$

注意这里左乘 $P=\begin{pmatrix}1&&\\&1&\\-9&&1\end{pmatrix}\begin{pmatrix}1&&1\\&1&\\&&1\end{pmatrix}=\begin{pmatrix}1&&1\\&1&\\-9&&-8\end{pmatrix}$，右乘 $Q=\begin{pmatrix}-2&&-9\\&1&\\1&&4\end{pmatrix}$.

3.2.2 Some Meaningful Exercises

Problem 1. 整环上的自由模一定是无扭模

证明 任取 $a\in R$ 为整环，$m\in M$，若 $am=0$，不妨设有基 e_i，且 $m=b^ie_i$，则有 $(ab^i)e_i=0$，故可知任意 i，$ab^i=0$，由 R 为整环，从而若 $a\neq 0$，则 $b^i=0$，即 $m=0$，故 $a=0$ 或 $m=0$ 至少有一者成立，即证. ♣

Problem 2. 设 R 为交换幺环，而且任何有限生成的 R 模都是自由模，证明 R 为域.

证明 本题具有一定的技巧性，为证明 R 为域，一个自然的观察就是，那 R 一定没有非平凡理想，从而我们先证明这件事，注意到 R/I 可自然视为由 $\overline{1}$ 有限生成的 R 模，从而为自由模，设有基 $\overline{a_1},\cdots,\overline{a_s}$，则注意到若 $I\neq(0)$ 或 R，则存在 $a\in R-I$ 使得 $a\overline{a_i}=\overline{aa_i}=\overline{0}$，因此这与基矛盾，从而我们确实得到了 R 没有非平凡理想.

进一步我们考虑主理想 (a) 也可以自然视为有限生成 R 模，从而为自由模，事实上由上一段我们知道 $a\neq 0$，$(a)=R$，又有交换幺环的性质，存在 $b\in R$，使得 $ab=ba=1$，即证 a 可逆，故可知 R 为域. ♣

3.3 PID 上的有限生成模

3.3.1 Notes

这一节我们研究主理想整环 D 上的有限生成模 M 的结构，也即研究 $M = Du_1 + \cdots + Du_n$，生成元为 $u_1, \cdots, u_n$，一个基本的观察是，考虑秩为 n 的自由模 D^n 到 M 的模同态：$\varphi(e_i) = u_i$，进一步做线性扩充，那么由模同构基本定理 $M \cong D^n/\ker\varphi$，从而研究有限生成模，本质上就是研究自由模的子模和商模，那么一个自然而然的问题是，子模还是自由模吗？甚至，还是有限生成模吗？(回顾第一节我们构造了一个有限生成模的子模并不有限生成的例子).

但生活总是充满希望：

定理 3.3.1: PID 上有限生成模的重要性质

主理想整环上的自由模的子模必为自由模，且子模的秩不超过本身的秩.

证明 我们考虑对 M 的秩用数学归纳法，假设对不超过 $m-1$ 的自由模已经成立，现在考虑 D^m 的子模 K，不妨 D^m 有基 $\{e_1, \cdots, e_m\}$，若 $K \subseteq De_2 \oplus \cdots \oplus De_m$，则由归纳原理，$K$ 为 D^{m-1} 的子模，必为自由模，且秩不超过 $m-1 < m$.

现在若 K 不完全在 $De_2 \oplus \cdots \oplus De_m$ 中，从而存在 $a^i e_i \in K$，且 $a^1 \neq 0$，自然地，我们想把 K 拆分成两个子模的直和，一个完全在 $M_1 = De_2 \oplus \cdots \oplus De_m$ 中，尽管我们自然希望另一个完全在 De_1 中，但用猪脚趾想想都知道不可能，但我们可以把 K 和 De_1 中相关的全取出来.

我们考虑 D(才发现 PID 还没用上呢) 的一个集合 $I = \{b^1 \in D | \text{存在} b^i \in D, b^i e_i \in K\}$，换句话说，就是把 K 这个子空间里所有第一项坐标挑出来，不难发现 I 构成理想，从而为主理想 (d)，因此 K 中元素 $k = a^i e_i$ 总能写成 $b^1 de_1 + a^i e_i$，进而取 $v = de_1$，考虑 $K_2 = Dv$，则易证 $K = K_1 \oplus K_2$，这里 $K_2 = K \cap M_1$，从而用归纳原理即证. ♣

命题 3.3.1: 思考题

域上自由模的真子模的秩严格小于自由模的秩，但对一般 PID 不一定正确.

解 考虑 $\mathbb{Z}$ 模 $\mathbb{Z}$ 和 $2\mathbb{Z}$，它们秩都为 1. ♠

在有了这一强大结论的基础上，我们自然会意识到，自由模 D^n 子模 K 也为自由模，从而前者有基 $u_1, \cdots, u_n$，后者有基 $v_1, \cdots, v_k$，利用命题 3.1.1 的直和的同构，我们很快意识到，若选取的 v_i 足够好，好到恰有 $Dv_i \subseteq Du_i$，那么商模的结构就十分清晰了！因此从这个角度出发，我们自然希望下面这个定理：

定理 3.3.2: 自由模的子模的基

设 K 是 PID 上自由模 D^n 的子模，则存在 D^n 的一组基 $u_1,\cdots,u_n$ 和 K 的一组基 $v_1,\cdots,v_k$，使得$v_i=d_iu_i,\ 1\leq i\leq k$，且 $d_i\neq 0$，$d_i|d_{i+1}$，这里 $1\leq i\leq k-1$.

证明 任取 K 的一组基 $\mathcal{C}$ 和 $M=D^n$ 一组基 $\mathcal{B}$, 考虑嵌入模同态 i, 从而在这组基下的矩阵为 $A\in D^{n\times k}$, 故由 PID 上的矩阵理论可知, 存在可逆矩阵 P,Q 使得 $PAQ=\mathrm{diag}\{d_1,\cdots,d_r,0,\cdots,0\}$, 从而考虑基 $\mathcal{V}=Q\mathcal{B}$，$\mathcal{U}=P^{-1}\mathcal{C}$，即可知满足定理条件，即证. ♣

从而利用上述定理，我们可以得到商模 D^n/K 从能表达成

$$\left(\bigoplus_{i=1}^{k}Du_i/D(d_iu_i)\right)\oplus\left(\bigoplus_{j=k+1}^{n}Du_j\right),$$

这里前半部分的直和分量不再是自由模，但仍然是循环模，可以理解成 $D(u_i+D(d_iu_i))$，设 $y_i=u_i+D(d_iu_i)$，则某种程度上y_i 是“阶为 d_i” 的元，这表明对于一般的有限生成模，它不一定自由，会有很多可以被零化的部分，我们下面就回到对有限生成模的研究：

定义 3.3.1: 模的零化

设 M 为交换幺环R 上的模，设 $x\in M$，称 $\mathrm{ann}(x)=\{a\in R|ax=0\}$ 这一理想为 M 的**零化子** (验证它是理想是直接的). 进一步任取 $x\in M^*$,

- 1. 若 $\mathrm{ann}(x)=\{0\}$，即 R 中没有元素零化它，则称其为**自由元**；
  2. 若 $\mathrm{ann}(x)\neq\{0\}$，即 R 中有元素零化它，则称其为**扭元**
- 1. 若 M 中没有扭元，我们称 M 为一个**无扭模**；
  2. 若 M 中全是扭元，我们称 M 为一个**扭模**；

注：一个需要阐明的事情是自由模和无扭模尽管看起来是类似的，因为不零化这一性质为我们提供了这一直觉，但事实上

- 自由模不一定是无扭模：考虑 $\mathbb{Z}_4$ 作为 $\mathbb{Z}_4$ 模为自由模 (任何一个环 R 作为自己的模总是秩为 1 的自由模)，但明显有扭元 $\overline{2}$；
- 无扭模不一定是自由模：考虑 $\mathbb{Z}$ 模 $\mathbb{Q}$，显然其为无扭模，但不是自由模，因为它不是有限生成的，取不在生成元分母出现的素数即可阐明这一点.

容易看到在 D^n/K 直和分解中，$Du_i/D(d_iu_i)$ 生成元是 $y_i=u_i+(d_iu_i)$ 是阶为 d_i 的扭元，从而为扭模，且 $\mathrm{ann}(y_i)=(d_i)$，但 Du_j 均为无扭模，因此借助这个观察，我们可以得到：

定理 3.3.3: 有限生成模的结构定理

设 M 为有限生成 D 模，则存在 $w_1,\cdots,w_n\in M$，使得 $M=Dw_1\oplus\cdots\oplus Dw_n$，并满足 $\mathrm{ann}(w_1)\supseteq\mathrm{ann}(w_2)\supseteq\cdots\supseteq\mathrm{ann}(w_n)$.

证明 这个定理的证明思想已经蕴含在前面的分析之中了，这里正向书写，首先利用有限生成的条件，存在 $u_1,\cdots,u_n\in M$，使得 $M=Du_1+\cdots+Du_n$，因此我们可以得到 M 到 D^n 的模同态 $\varphi:u_i\mapsto e_i$，从而由模同态基本定理，$M\cong D^n/K$，这里 $K=\ker\varphi$，从而利用之前的商模的结构定理，可知存在 D^n 的一组基 $e_1,\cdots,e_n$ 和 K 的一组基 $v_1,\cdots,v_k$，使得$v_i=d_ie_i,\ 1\le i\le k$，且 $d_i\neq 0$，$d_i|d_{i+1}$，这里 $1\le i\le k-1$，进一步

$$M\cong D^n/K=\left(\bigoplus_{i=1}^{k}D(e_i+(d_ie_i))\right)\oplus\left(\bigoplus_{j=k+1}^{n}De_j\right),$$

且容易看见 $\mathrm{ann}(e_i+(d_ie_i))=(d_i)$，$\mathrm{ann}(e_j)=\{0\}$，从而基本上已经找到符合要求的了，现在只需要找到这些生成元的原像即可，显见 e_j 的原像是 u_j，故取$w_j=u_j$，再取 w_i 为 $e_i+(d_ie_i)$ 的同构像即可，这即e_i 的同态像，从而可知能够选取一组 $w_1,\cdots,w_n$ 使得定理成立. ♣

推论 3.3.1: 无扭模与自由模的关系

有限生成的无扭模是自由模.

证明 利用有限生成模结构定理，可知 $M=Du_1\oplus\cdots\oplus Du_s$，且 u_i 均不被零化，构成一组基. ♣

命题 3.3.2: 思考题

上述推论对一般交换幺环并不成立.

解 考虑一个 $\mathbb{Z}[x]$ 模，$(2,x)$，则其为无扭模，不存在 $f(x)\in\mathbb{Z}[x]$ 零化这一有限生成模的元素，故为有限生成无扭模，但是不为自由模，若为自由模，则在交换幺环上，秩唯一且不超过 2，若秩为 1 且基为 $g(x)$，则 $g(x)|2,x$，表明 $g=1$，矛盾，若秩为 2，注意到 2 和 x 是 $\mathbb{Z}[x]$ 系数线性相关的，从而也矛盾，因此我们举出了一个合适的反例. ♠

像所有高等代数获得标准型的思想一样，我们渴望知道，我们这种分解是否唯一？对于一个有限生成模 M，n 是否唯一？w_i 和 $\mathrm{ann}(w_i)$ 是否唯一？我们当然期望：

定理 3.3.4: 有限生成模的结构唯一

设 M 为有限生成 D 模，其有两种分解：

$$M=Du_1\oplus\cdots\oplus Du_s=Dv_1\oplus\cdots\oplus Dv_t,$$

则 $s=t$，且 $\mathrm{ann}(u_i)=\mathrm{ann}(v_i)$.

它的证明当然是肉眼可见的复杂，但这不妨碍我们心里先接受它，在这个唯一性的基础上，我们可以很轻松给出下面这些定义：

定义 3.3.2: 有限生成模的秩、不变因子、扭部

有限生成 D 模 $M = M^{\mathsf{T}} \oplus M^{\mathsf{F}}$，前者为扭模，后者为自由模，若记 $\mathrm{Tor}(M) = \{u \in M^* | \exists a \in D, am = 0\}$ 为 M 的**扭部**，则 $\mathrm{Tor}(M) = M^{\mathsf{T}}$，称自由模 M^{F} 的秩为 M 的**秩**，则不难看见 $M^{\mathsf{F}} \cong M/\mathrm{Tor}(M)$，对 $M^{\mathsf{T}} = Du_1 \oplus \cdots \oplus Du_k$，且 $\mathrm{ann}(u_i) = (d_i)$，称 d_i 为**不变因子**，在上一定理保证下不难有这些均不依赖于分解形式.

注：事实上我们有 M 的秩 $r(M) = r(M^{\mathsf{F}}) = r(D^n) - r(K) = n - r(K)$.

我们先跳过有限生成模结构唯一性的证明，先给出若干应用：

有限生成 Abel 群的分类

视有限生成 Abel 群 G 为自然的 $\mathbb{Z}$ 模，则我们可以得到

定理 3.3.5: 有限生成 Abel 群的结构

存在 G 中元素 $u_1, \cdots, u_s$，满足

$$G = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_s,$$

且 $\mathrm{ann}(u_1) \supseteq \cdots \supseteq \mathrm{ann}(u_s)$.

进一步我们考虑模同构 $\mathbb{Z}u_i \cong \mathbb{Z}/(d_i) = \mathbb{Z}_{d_i}$，因此我们有

命题 3.3.3: 有限生成 Abel 群结构

设 G 为一个有限生成的既有扭元又有自由元的交换群，则存在 $r \in \mathbb{N}^*$，以及 $d_1, \cdots, d_k \in \mathbb{N} \setminus \{0, 1\}$，满足

$$G \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r\text{个}} \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_k},$$

且对任意 $1 \leq i \leq k-1$，$d_i \mid d_{i+1}$，若利用 $\mathbb{Z}_{mn} = \mathbb{Z}_m \oplus \mathbb{Z}_n$，其中 $(m, n) = 1$，则

$$G \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r\text{个}} \oplus \mathbb{Z}_{p_1^{s1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{st}},$$

这里 $p_1 \leq \cdots \leq p_t$ 为素数，注意这里 p_i 可以相等，就是把 d_i 进行素因数分解.

注：利用上述结构定理，我们可知对 $n = p_1^{m_1} \cdots p_s^{m_s}$ 阶 Abel 群，我们可知其结构依赖于 $p_i^{m_i}$ 分拆成若干个 $p_i^{m_{i,k}}$ 乘积，$m_{i,k}$ 关于 k 递增，且 $\sum m_{i,k} = m_i$，则记这种拆分数为 $\rho(m_i)$，则一共有 $\prod \rho(m_i)$ 种 Abel 群的结构.

例 3.3.1. 我们考虑 24 阶 *Abel* 群的可能结构，则利用 $24 = 2^3 \cdot 3^1$，则共有 $\rho(1)\rho(3) = 3$，可能的情形是 $\mathbb{Z}_3 \otimes \mathbb{Z}_8$，$\mathbb{Z}_3 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_4$，$\mathbb{Z}_3 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$.

线性变换的标准型

3.3.2 Some Meaningful Exercises

3.4 模的张量积

3.4.1 Notes

3.4.2 Some Meaningful Exercises

3.5 正合序列——射影模、内射模与平坦模

3.5.1 Notes

3.5.2 Some Meaningful Exercises

4 域论

4.1 域的基本概念

4.1.1 Notes

定义 4.1.1: 域

若 F 是一个含有非零元的整环 (回忆：无零因子交换幺环)，且 F 的每个非零元都可逆 (回忆：$F^* = U$)，则称 F 为**域**.

命题 4.1.1: 域的基本性质

一个交换幺环F 是域当且仅当 F 只有平凡理想.

定义 4.1.2: 域同态

我们称映射 φ 为域 F 到域 E 的一个**域同态**，若满足以下条件：

1. 任取 $a, b \in F$，有 $\varphi(a+b) = \varphi(a) + \varphi(b)$；
2. 任取 $a, b \in F$，有 $\varphi(ab) = \varphi(a)\varphi(b)$；
3. $\varphi(1_F) = 1_E$.

一个与群同态、环同态不同的是，我们有

命题 4.1.2

任何域同态都是单射.

证明 只需要注意到 $\ker f$ 为域 E 的理想. ♣

定义 4.1.3: 子域与扩张

设 $E \in \mathsf{Field}$，如果 E 的一个子集 F 在 E 的运算下也构成域，称 F 为 E 的**子域**，也称 E 为 F 的**扩张**，记为 E/F.

注：判断一个子集为子域只需判断其为子环，且 $F \cap E^* \neq \varnothing$.

命题 4.1.3: 一个基本的代数性质

若 $\{F_\lambda\}_{\lambda\in\Lambda}$ 为域 E 的一些子域，则 $\bigcap\limits_{\lambda\in\Lambda} F_\lambda$ 也为子域.

在这一结论的基础上，我们便可以考虑一般集合的生成子域：

定义 4.1.4: 生成子域

我们称所有包含集合 S 的 E 的子域的交 (仍为子域) 为**由 S 生成的子域**：

$$C(S)=\bigcap\{F|S\subseteq F\subseteq E,F\text{为}E\text{的子域}\}.$$

注：集合生成的子域也可以借助生成子环的分式域得到，两种定义等价.

定义 4.1.5: 素域

既然任意子域相交均为域，那么 E 的全体子域相交也为域，且不难验证这是所有子域中最小的一个，换言之该最小子域无任何非平凡子域，我们称不包含任何非平凡子域的域为**素域**.

注：不难得到任何域都包含唯一的一个子域为素域.

定理 4.1.1: 素域的结构

任何一个素域一定同构于 $\mathbb{Q}$ 或某个 $\mathbb{F}_p$，进一步

1. 若 E 特征为 p，则其素域同构于 $\mathbb{F}_p$；
2. 若 E 特征为 0，则其素域同构于 $\mathbb{Q}$.

证明 我们注意到，域 E 的素域实际上为 $C(1)$，即1 生成的子域，从而自然的，考虑 $\mathbb{Z}$ 到 E 的环同态：$\varphi:1\mapsto 1_E$，则若 E 特征为 p，则 $\ker f=p\mathbb{Z}$，从而 1 生成的环同构于 $\mathbb{Z}/p\mathbb{Z}$，则 $C(1)$ 同构于 $\mathbb{Z}_p$ 的分式域，也即 $\mathbb{F}_p$.

若 E 特征为 0，则 1 生成的环同构于 $\mathbb{Z}$，从而 $C(1)$ 同构于 $\mathbb{Z}$ 的分式域，也即为 $\mathbb{Q}$. ♣

命题 4.1.4: 素域不同扩张间的同态

设 E,F 均为素域 Π 的扩张，且 $\varphi:E\to F$ 为域同态，则 $\varphi_\Pi=\mathrm{id}_\Pi$. 换一种表述，域同态只能建立在同一素域扩张的域之间，也就是等价地要求两个域具有相同的特征.

证明 核心就一句话：素域间的同态一定是同构，因为素域的像仍为域. ♣

域的核心问题是研究域的扩张，一个最自然的看法是：

定理 4.1.2

若 E/F，则 E 可以看作是 F 上的线性空间.

证明 稍稍回顾一下线性空间定义：V 是域 F 上的线性空间，如果其是 F 模，由于 F 是 E 的子域，这些都不难保证. ♣

定义 4.1.6: 域扩张的次数

我们记 $[E:F]:=\dim_F E$ 表示 E/F 的扩张次数.

例 4.1.1. $\mathbb{R}$ 是 $\mathbb{Q}$ 上的无限扩张，因为不难注意到若为有限扩张，则 $\mathbb{R}$ 为有限个基的 $\mathbb{Q}$ 线性组合，这表明 $\mathbb{R}$ 可数，顶荒谬.

定理 4.1.3: 域扩张的一个经典计算公式

若 E/F，F/K 均为有限扩张，则 E/K 为有限扩张，且 $[E:K]=[E:F][F:K]$.

证明 证明的核心是，对 E/F 的基 α_i，F/K 的基 β_j，有 E/K 的基为 $\alpha_i\beta_j$. ♣

命题 4.1.5: 思考题 4.1.18

域扩张的次数与它们作为 Abel 群的指数之间有没有关系?

解 没有关系，比如考虑 $\mathbb{Q}(\sqrt{2})$ 与 $\mathbb{Q}$，作为域扩张的次数显然为 2，但是回忆一下作为加法子群，若 $(a+b\sqrt{2})\mathbb{Q}=(c+d\sqrt{2})\mathbb{Q}$，则有 $b=d$(相减为有理数)，从而 $(m\sqrt{2})\mathbb{Q}$ 均为不同的左陪集，因此作为 Abel 群，这个指数是无穷，因此两者之间不存在必然联系. ♠

4.1.2 Some Meaningful Exercises

Problem 1. 设 $\alpha\in\mathbb{C}$ 是一个 n 次不可约有理多项式 $p(x)$ 的根.

1. 证明：$\mathbb{Q}(\alpha):=\{f(\alpha)|f(x)\in\mathbb{Q}[x]\}$ 是一个域，且 $[\mathbb{Q}(\alpha):\mathbb{Q}]=n$;
2. 试求 $\mathrm{Hom}(\mathbb{Q}(\alpha),\mathbb{C})$.

证明 设 $p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{Q}[x]$，且 $p(\alpha)=0$.

(1) 任取 $f(\alpha)\in\mathbb{Q}(\alpha)$，由 $p(x)$ 不可约，因此 $p|f$ 或 $(p,f)=1$，若为前者则 $f(\alpha)=0$，若为后者，则存在 $k(x),\ell(x)$ 使得 $k(x)p(x)+\ell(x)f(x)=1$，代入 α，则有 $\ell(\alpha)f(\alpha)=1$，从而 $f(\alpha)\in F^*$ 则 $f(\alpha)$ 可逆，证明其为整环是自然的，略去.

由于 $1,\alpha,\cdots,\alpha^{n-1}$ 恰为一组基，从而可知扩张次数为 n.

(2) 任取 $\varphi \in \mathrm{Hom}(\mathbb{Q}(\alpha), \mathbb{C})$，则设 $\varphi(\alpha) = \beta$，则有 $p(\beta) = \varphi(p(\alpha)) = 0$，从而 β 为 p 的一个根，另一方面由 $\mathbb{Q}$ 为素域，因此 $\varphi|_{\mathbb{Q}} = \mathrm{id}$，因此 φ 完全由 $\varphi(\alpha)$ 确定，因此可知 $\mathrm{Hom}(\mathbb{Q}(\alpha), \mathbb{C}) = \{\varphi : \varphi(g(\alpha)) = g(\beta), p(\beta) = 0\}$. ♣

4.2 代数扩张

4.2.1 Notes

我们从现在开始，想要研究域扩张 E/F，直观来看，域扩张就是从 F 中添加了若干元素，比如 $\mathbb{Q}(\sqrt{-1})$，$\mathbb{Q}(\pi)$，这里 $\mathbb{Q}(\alpha)$ 表示环 $\mathbb{Q}[\alpha]$ 对应的分式域，我们在上一节已经看到，若 α 为某个 $\mathbb{Q}$ 上多项式的根，则 $\mathbb{Q}(\alpha)=\mathbb{Q}[\alpha]$，而显然对 π 这种超越元，那么

$$\mathbb{Q}[\pi]=\{a_0+\cdots+a_n\pi^n\}\subset\mathbb{Q}(\pi)=\left\{\frac{a_0+\cdots+a_n\pi^n}{b_0+\cdots+b_m\pi^m}\right\},$$

那么这便驱使我们去研究扩张的代数元和超越元，为此我们先澄清一些概念：

定义 4.2.1: 零化多项式

设 E/F 为域扩张，任取 $\alpha\in E$，有一个自然的赋值环同态：

$$\Phi_\alpha:F[x]\to E,\quad f(x)\mapsto f(\alpha),$$

则考虑 $\ker\Phi_\alpha$ 为 $F[x]$ 的一个理想，若 $f(x)\in\ker\Phi_\alpha$，则自然有 $f(\alpha)=0$，称其为 α 的**零化多项式**.

事实上，依赖于 F 是域的性质，我们有 $F[x]$ 是 PID(事实上为 ED)，当然这个命题反过来也对，考虑 $F[x]/(x)$ 就行. 这表明 $\ker\Phi_\alpha$ 为主理想，记为 (f_α).

定义 4.2.2: 代数元与超越元

设 E/F 为域扩张，则任取 $\alpha\in E$，$\ker\Phi_\alpha=(f_\alpha)$，则

1. 若 $f_\alpha\neq0$，则称 α 为 F 上的**代数元**，对应的称 f_α 为其在 F 上的**最小多项式** (所有零化多项式均为其倍式)，记作 $\mathrm{Irr}(\alpha,F)$；
2. 若 $f_\alpha=0$，则称 α 为 F 上的**超越元** (因为没有 F 上多项式零化它).

一个很简单却有力的推论是：

定理 4.2.1: 最小多项式的性质

设 E/F 为域扩张，$\alpha\in E$，则 $\mathrm{Irr}(\alpha,F)$ 为不可约多项式.

证明 真要说起来就一句话，若 $f_\alpha=gh$，则 $g(\alpha)h(\alpha)=0$，两者均为域 E 中元素，因此必有一个为 α 零化多项式，这么想来必然有 g 或 h 是 f_α 的倍式，便结束了证明. ♣

命题 4.2.1: 一个构做扩域的办法

利用 f_α 在 F 上不可约，故 (f_α) 为 $F[x]$ 的极大理想，进而 $F[x]/(f_\alpha)$ 为一个包含 F 的域.

注意，我们时常会把目光过度聚焦在 F 上，想着怎么扩出去，而忽视了大条件 E 的限制，所以为了澄清这一点，需要注意 F 上代数元总是有的 (F 自己！)，但超越元不一定有 (针对 E/F)：

定理 4.2.2: 有限扩张一定是代数扩张

若 E/F 为有限扩张，落在实地的，$[E:F]<\infty$，则每一个 $\alpha\in E$，均为 F 上代数元.

证明 和点拓一样，倒腾一下定义，想来论证是代数元无非就是要找一个多项式 $f(x)=a_0+\cdots+a_nx^n$，有 $f(\alpha)=0$(这个 0 是 E 中的 0)，大胆想一想，就是有一个 $1,\alpha,\cdots,\alpha^n$ 的 $F-$ 线性组合为 0，而扩张次数有限，那便一定存在这样的 n 它们线性相关哩！ ♣

定义 4.2.3: 代数扩张与超越扩张

设 E/F 为域扩张，若任意 E 中元素均为 F 上代数元，则称为**代数扩张**，反之只要有一个为超越元，则称为**超越扩张**.

例 4.2.1. *很显然 $F[x]/(p(x))$ 这里 $p(x)$ 是任意 F 上不可约多项式，均为 F 的代数扩张，事实上这是扩张次数为 $\deg p$ 的有限扩张，而 $\mathbb{R}/\mathbb{Q}$ 为超越扩张 (π 为超越数).*

一个值得关心的问题就是，在 E/F 中，E 中所有代数元全体构成的集合有什么结构么？为了回答这个问题，一个更自然但不平凡的问题是：代数元关于四则运算封闭吗？

很显然，任给一个 $\alpha\in E$ 为代数元，α 和 F 拼拼凑凑总归还是代数元，因为拼凑得到的是 $F(\alpha)=C(F\cup\{\alpha\})$，而 $F(\alpha)\cong F[x]/(f_\alpha(x))$ 为代数扩张，因此为了研究 α,β 这两个代数元的信息，无非就是往 F 里一次性丢两个元素，更本质地，先丢一个再丢一个应该完全一样，这样想来 $F(\alpha,\beta)=F(\alpha)(\beta)$，前者的扩张次数可以由 $[F(\alpha)(\beta):F(\alpha)]\cdot[F(\alpha):\alpha]$ 控制，后者有限自然导出丢两个代数元进去生成的域为有限扩张，进而为代数扩张.

注：$F(\alpha)=F[\alpha]\cong F[x]/(f_\alpha(x))$ 是基本且关键的，想看清楚只需把 α 和 $\overline{x}$ 等同起来.

为了推广到一般，我们给出如下信息：

定义 4.2.4: 集合生成的扩域

任给 E 的非空子集 S，我们称 $C(F\cup S)$ 为S **在** F **上生成的域**，并记作 $F(S)$.

注：容易看见 $E/F(S)/F$，所以 $F(S)$ 可以看成 F 的扩域，也可以看成是 E 的子域，从生成的角度来看，$F[S]$ 是 F 上的多元多项式环，则 $F(S)$ 是 $F[S]$ 的分式域.

定理 4.2.3: 扩域的基本性质

设 E 为域 F 的扩域，$S \subseteq E$，则

1. $F(S) = \bigcup_{S' \subseteq S} F(S')$，其中 S' 取遍 S 的所有有限子集；
2. 若 $S = S_1 \cup S_2$，则 $F(S) = F(S_1)(S_2) = F(S_2)(S_1)$，进一步有 $F(\alpha_1, \cdots, \alpha_n) = F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$.

证明 为了理清证明，首先回顾 $F(S)$ 的等价刻画，即是所有包含 $F \cup S$ 的子域的交，因此讨论 $F(A)$ 与 $F(B)$ 之间的包含关系，无非就是看 A 和 B 之间的关系，注意到 $S' \subseteq S$，从而右侧包含于左侧；另一方面

$$F \cup S \subseteq \bigcup_{\alpha \in S} F(\alpha) \subseteq \bigcup_{S' \subseteq S} F(S'),$$

利用 $F(S)$ 的最小性即可知另一方向的包含.

对于另一条，由 $F \cup S \subseteq F(S_1)S_2$，从而可知 $F(S) \subseteq F(S_1)(S_2)$，另一方面，显然 $F(S_1)(S_2) \subseteq F(S_1 \cup S_2) = F(S)$，从而可知正确，另一个则是直接的归纳即可. ♣

注：这条定理便严格的说清了我们的直觉：从 F 出发，逐渐丢进 E 中的元素，和丢的元素个数、先后均无关，得到的扩域均是一致的.

现在我们可以完满回答之前的问题了：代数元的组合是否依然是代数元，严谨写来，大抵是考虑下面这个定理形式：

定理 4.2.4: 丢进有限个代数元的扩域结构

设 E/F，$K = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$，这里 $\alpha_1, \cdots, \alpha_n \in E$，则下列条件等价：

1. $\alpha_1, \cdots, \alpha_n$ 是 F 上的代数元；
2. K 是 F 的有限扩张；
3. K 是 F 的代数扩张.

证明 1 推 2 是将我们之前二元版本的证明做一点改进，需要注意到的事实是 $K = F(\alpha_1)\cdots(\alpha_n)$，且 α_k 是 F 的代数元，自然明显不言而喻的，α_k 是 $F(\alpha_1)\cdots(\alpha_{k-1})$ 上的代数元，且扩张次数不超过在 F 上的，从而

$$[K : F] = \prod_{k=1}^{n} [F(\alpha_1)\cdots(\alpha_k) : F(\alpha_1)\cdots(\alpha_{k-1})] \leq \prod_{k=1}^{n} [F(\alpha_k) : F] < \infty,$$

也即 K 是 F 的有限扩张，2 推 3，3 推 1 更是明显的. ♣

注：注意这里 K 的特性，对一般的代数扩张其可不一定是有限扩张，如考虑 $\mathbb{Q}$ 的代数闭包.

定理 4.2.5: 代数扩张的传递性

若 E/K，K/F 都是代数扩张，则 E/F 也是代数扩张.

证明 为了证明此事，无非就是任取 $\alpha \in E$ 为 K 上代数元，想说明其为 F 上代数元，前者表明存在 $k_0, \cdots, k_n \in K$ 使得 $k_0 + \cdots + k_n\alpha^n = 0$，一个自然的想法是把 k_i 表达成 F 中元素的形式，但这无疑是行不通的，一个巧妙地处理是 $V = F(k_0, \cdots, k_n)$ 是 F 上的有限扩张，而 $[V(\alpha) : V] \leq n$，从而 $F(k_0, \cdots, k_n, \alpha)$ 为 F 上有限扩张，这表明 α 是代数元，即证. ♣

定义 4.2.5: 纯超越扩张，单 (代数) 扩张

设 E/F 为域扩张，如果 $E - F$ 均为 F 上超越元，则称其为**纯超越扩张**，如果存在 $\alpha \in E$ 使得 $E = F(\alpha)$，则称 E 为**单扩张**，若 α 为代数元，则称其为**单代数扩张**.

事实上，我们有

定理 4.2.6: 单扩张的结构

1. 域 F 的单代数扩张 $F(\alpha)$ 必同构于 $F[x]/(f_\alpha)$，其中 f_α 为最小多项式；
2. 域 F 的单超越扩张都同构于 $F(x)$，即 $F[x]$ 的分式域.

4.2.2 Some Meaningful Exercises

Problem 1. 设 E/F 为有限扩张，且对 E 中任意两个包含 F 的子域 K_1, K_2，必有 $K_1 \subseteq K_2$ 或 $K_2 \subseteq K_1$，证明：E/F 是单代数扩张.

证明 设 $E = F(\alpha_1, \cdots \alpha_n)$，则 $F(\alpha_1, \alpha_2)$ 为 $F(\alpha_1)$ 或 $F(\alpha_2)$ 为单扩张，归纳即可. ♣

Problem 2. 设 K 是 F 的有限扩张，证明：必存在中间域的升链

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = K,$$

其中 F_{i+1} 是 F_i 的单代数扩张，$i = 0, 1, \cdots, r-1$.

证明 对扩张次数 n 运用数学归纳法即可，挑出一个 $K - F$ 中元素构成中间域实现降阶. ♣

Problem 3. 设 F 特征为 $p > 0$，$c \in F$，若 K/F 为域扩张，且在 K 中 $x^p - x - c$ 可以分解为一次因式的乘积 (为其分裂域). 证明：$x^p - x - c$ 在 $F[x]$ 中不可约当且仅当其在 F 中无根.

证明 若其有根，显然可约，进而不可约蕴含无根，反过来，下假设 x^p-x-c 在 F 上可约，我们下证其一定有根. 反证法，若无根，且设 $x^p-x-c=f(x)g(x)$，这里 $f(x),g(x)\in F[x]$. 现在在域 K 上考虑问题，注意到若 $a\in K$ 为 x^p-x-c 的根，则 $a,a+1,\cdots,a+(p-1)$ 均为其根 ($(a+b)^p=a^p+b^p$，有限域的重要特性！)

因此在 K 上，我们有 $x^p-x-c=(x-a)\cdots(x-a-p+1)$，则有 $f(x)=(x-a-i_1)\cdots(x-a-i_s)\in F[x]$，从而考虑 x^{s-1} 系数为 $-(sa+i-1+\cdots+i_s)\in F$，进而 $sa\in F$，而 s 与 p 互素，从而存在 u,v 使得 $us+vp=1$，也即 $a=usa\in F$，这与 x^p-x-c 在 F 上无根矛盾！ ♣

Problem 4. (Steinitz 定理) 设 E 为 F 的有限扩张，证明 E 是 F 的单代数扩张当且仅当 E 与 F 之间只有有限个中间域.

4.3 分裂域

4.3.1 Notes

我们在这一节主要关心的问题是：给定一个域 F，以及这个域上的一个代数方程，也即 $f(x) \in F[x]$，$f(x) = 0$，我们能否找到一个域扩张 E，使得存在 $\alpha \in E$，有 $f(\alpha) = 0$(这里的 0 是 E 中的 0，因为在域运算中，子域的数总能自然看成大域中的，因此如果出现高阶的域，运算应当处在高阶域的视角下进行).

一个十分具有启发性的构造是 Kronecker 给出的，对于$f(x) = p(x)$ 在 F 上不可约时：

定理 4.3.1: Kronecker 构造

考虑 $E = F[x]/(p(x))$，由后者的不可约性可知其是域，由上一节可知这是 F 的有限扩张，但注意，这里 F 中的元素 a 在 E 中应表示成 $\overline{a} = a + (p(x))$，因此考虑 $F[x]$ 上的多项式方程 $p(t) = \overline{a}_n t^n + \cdots + \overline{a_0} = \overline{0}$ 在 E 上的解，取 $t = \overline{x} = x + (p(x))$，从而 $p(\overline{x}) = \overline{p(x)} = \overline{0}$.

对于一般的多项式 $f(x)$，则考虑其不可约分解也能的到类似的构造，事实上我们得到了：

定理 4.3.2: 扩张有根的存在性

给定域 F，以及 $F[x]$ 上多项式 $f(x)$，我们总能找到一个域扩张 E/F，使得存在 $\alpha \in E$，$f(\alpha) = 0_E$.

注：我们为什么一再强调 0_E，因为在 Kronecker 构造中，F 的扩域 E 看起来并不那么像“数域”，这干扰了我们的直观想象，如 $\mathbb{Q}$ 和 $\mathbb{Q}(\sqrt{2})$，在数域里，我们总知道代数方程在 $\mathbb{C}$ 中有根，我们便会去下意识的对一般的 $F[x]$ 上多项式找根α，再去扩张成 $F(\alpha)$，但事实上一般的 α 我们无法给出，这也导致了扩张的 E 会比较奇怪，这样一个与数域不同的障碍需要我们逐渐习惯.

我们不难利用下面这个引理将有一个根推广到一般：

命题 4.3.1: 有根则可在大域上分解出一次因式

给定域 F，以及 $F[x]$ 上多项式 $f(x)$，我们知道存在 E/F，使得存在 $\alpha \in E$，有 $f(\alpha) = 0$，则进一步，在$E[x]$上，存在 $f_1 \in E[x]$使得，$f(x) = (x - \alpha) f_1(x)$.

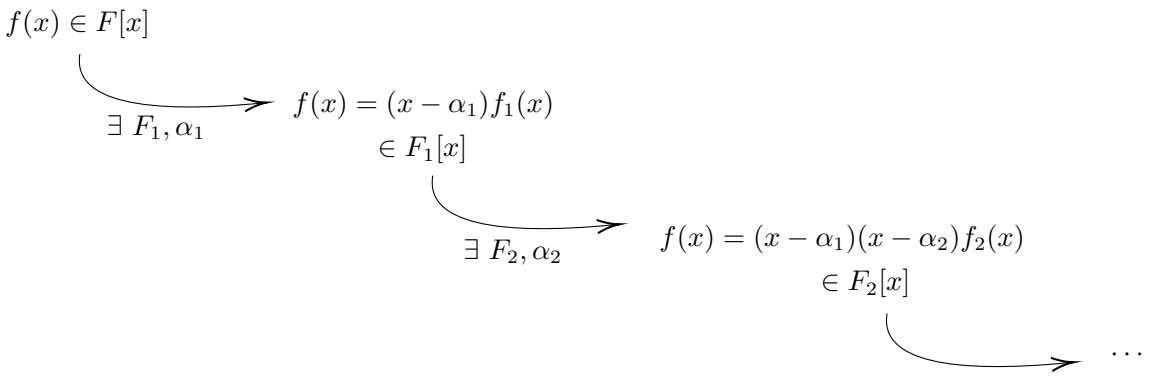
证明 考虑 $f(x) = f(x - \alpha + \alpha)$ 展开关于 $x - \alpha$ 整理即可. ♣

利用这个信息，我们事实上可以得到：

定理 4.3.3: 分裂域的存在性

给定域 F，以及 $F[x]$ 上多项式 $f(x)$，次数为 n，存在 E/F 为有限扩张，使得存在 $\alpha_1,\cdots,\alpha_n\in E$，有 $f(x)$ 视作 $E[x]$ 中多项式时，$f(x)=a(x-\alpha_1)\cdots(x-\alpha_n)$，$a\in E$.

证明 下面这张图生动展现了证明过程: ♣



在此基础上，我们可以给出分裂域的概念:

定义 4.3.1: 分裂域

给定域 F，以及 $F[x]$ 上的多项式 $f(x)$，次数为 n，我们称 $f(x)$ 在 F 上的一个扩张 E 上**分裂**，如果存在 $\alpha_1,\cdots,\alpha_n\in E$ 使得 $f(x)$ 能在 $E[x]$ 分解成 $f(x)=a(x-\alpha_1)\cdots(x-\alpha_n)$. 若进一步，在确定了 $\alpha_1,\cdots,\alpha_n$ 的基础上，E 不太大，恰好是 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，则称 E 为 $f(x)\in F[x]$ 的**分裂域**，换句话说，如果 E 是 $f(x)$ 分裂域，那么在 E 任何真子域 K 上，$f(x)$ 作为 $K[x]$ 上多项式无法分解成一次因式的乘积.

注: 利用之前的定理，我们可以确信 $f(x)$ 的分裂扩张 E 一定是存在的，但注意按这个流程 (指沿着 Krnonecker 构造逐步扩张) 得到的域不一定是分裂域! 因此我们只需要考虑其子域 $F(\alpha_1,\cdots,\alpha_n)$ 即可，这便给出了分裂域的存在性.注意分裂域使用的时候用 $F(\alpha_1,\cdots,\alpha_n)$ 最方便.

命题 4.3.2: 一个直接的推论

利用 Kronecker 构造，我们可以得到分裂域的一个简单估计 $[E:F]\leq n!$.

证明 由 E 为 $f(x)$ 的分裂域，从而存在 $\alpha_1,\cdots,\alpha_n\in E$，有 $f(x)=a(x-\alpha_1)\cdots(x-\alpha_n)$，则 $E=F(\alpha_1,\cdots,\alpha_n)$，因此设 $F_k=F(\alpha_1,\cdots,\alpha_k)$，则有 $[E:F]=\prod_{k=1}^{n}[F_k:F_{k-1}]$.

注意到 $f(x)$ 作为 $F_k[x]$ 上的多项式，可以分解成 $f(x)=(x-\alpha_1)\cdots(x-\alpha_k)f_k(x)$，从而 α_{k+1} 在 F_k 上的最小多项式次数不超过 f_k 次数 (因为 f_k 是 $F_k[x]$ 上 α_{k+1} 的一个零化多项式)，也即不超过 $n-k$，因此 $[F_k:F_{k-1}]\leq n-k+1$，故 $[E:F]\leq n!$，即证. ♣

例 4.3.1. 设 $f(x)=x^3-2\in\mathbb{Q}[x]$，则其在 $\mathbb{C}$ 上有根 $\sqrt[3]{2}$，$\sqrt[3]{2}\zeta_3$，$\sqrt[3]{2}\zeta_3^2$，从而 $\mathbb{C}$ 是 $f(x)$ 在 $\mathbb{Q}$ 上的一个分裂扩张，因此由定义，分裂域为 $\mathbb{C}$ 的子域 $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\zeta_3,\sqrt[3]{2}\zeta_3^2)=\mathbb{Q}(\sqrt[3]{2},\zeta_3)$，这里 ζ_3 为三次单位根，从而易见分裂域次数为 6，从而上一命题得到的不等式是紧的.

例 4.3.2. 考虑 $f(x)=x^p-1\in\mathbb{Q}[x]$，则其在 $\mathbb{C}$ 上有根 ζ_p^k，$0\leq k\leq p-1$，从而其有分裂域 $\mathbb{Q}(\zeta_p)$，其最小多项式为 $x^{p-1}+\cdots+1$，从而其扩张次数为 $p-1$，故表明上面的估计是有意义的，分裂域的扩张次数不会恒为 $n!$.

现在有了分裂域的存在性，我们自然关心，这样的分裂域是否唯一？数域上的版本给我们的直观是，在同构意义下唯一，如 $\mathbb{R}[x]$ 上 x^2+1 的分裂域为 $\mathbb{C}$ 或 $\mathbb{R}[x]/(x^2+1)$，其中 $a+b\mathrm{i}\mapsto\overline{a+bx}=a+bx+(x^2+1)$，下面我们就推广这一想法.

设 E,E' 是 $f(x)\in F[x]$ 的两个分裂域，且存在 $\alpha_1,\cdots,\alpha_n\in E$ 使得 $E=F(\alpha_1,\cdots,\alpha_n)$，我们现在想要构造两个域之间的域同构 σ，首先自然会要求 $\sigma|_F=\mathrm{id}_F$，进一步我们只需要确定σ 在 $\alpha_1,\cdots,\alpha_n$ 的像即可.

万事开头难，我们先解决 $n=1$ 的情形，关键在于，我们应该把 α_1 送到哪里？设 α_1 在 F 上的最小多项式为 $p(x)\in F[x]$，则 $p(x)|f(x)$，那么考虑 $p(x)$ 在 E' 中的任一根 α_1'，我们考虑 $\sigma:F(\alpha_1)\to F(\alpha_1')$，将 α_1 送到 α_1'，不难验证这是域同构!

现在从 $F_1=F(\alpha_1)$ 和 $F_1'=F(\alpha_1')$ 出发，σ 是这两者上的域同构，再考虑 α_2，送到那里去？类似地，考虑其在F_1上的最小多项式 $p_2(x)$，我们发现 $p_2(x)$ 不再是 F_1' 上的最小多项式 (因为系数压根都不在 F_1' 中)，但好在我们可以考虑 $p_2'(x)$，其系数是 $p_2(x)$ 的系数同构 σ 送到 F_1' 中的. 我们自然要问了，$p_2'(x)$ 是不是也不可约？因为是域同构，从而这是很显然的，因此任取 $p_2'(x)$ 的一个在 E' 中的根 α_2'，考虑 $\sigma:F(\alpha_1,\alpha_2)\to F(\alpha_1',\alpha_2')$，也不难验证这是域同构!

归纳下去，我们就得到了 E 和 E' 的一个域同构. 整理一下思路，核心是下面这条引理，从 0 到 1 的关键:

定理 4.3.4: 域同构的开拓

设 $\sigma:K\to K'$ 为域同构，且 $K(\alpha)/K$ 为单代数扩张，记 $p(x)=\mathrm{Irr}(\alpha,K)$，$p'(x)$ 为 $p(x)$ 各项系数通过 σ 对应送过去得到的. 若 E' 是 $p'(x)$ 在 F' 上的分裂扩张，则存在域同态 $\varphi:K(\alpha)\to E'$ 使得 $\varphi|_K=\sigma$，且这样域同态的个数 $\leq[K(\alpha):K]$，且等号成立当且仅当 $p(x)$ 在 E 中没有重根.

证明 域同态 φ 被 $\varphi(\alpha)$ 唯一确定，而 $\varphi(\alpha)$ 在 E' 中的最小多项式一定是 $p'(x)$，从而 $\varphi(\alpha)$ 至多 $\deg p'$ 种选择，由 $\deg p'=\deg p=[K(\alpha),K]$ 可知命题得证. ♣

总结起来，我们由下面这个定理结果:

定理 4.3.5: 分裂域的唯一性

设 $f(x)\in F[x]$，E 和 E' 是其两个分裂域，则存在域同构 $\sigma:E\to E'$，进一步这样的域同构个数不超过 $[E:F]$，且等号成立当且仅当 $f(x)$ 的任何不可约因式在 E 中没有重根.

证明 逐渐考虑 σ 限制在 $F_k=F(\alpha_1,\cdots,\alpha_k)$ 上，从 F_k 开拓到 F_{k+1} 至多有 $[F_{k+1}:F_k]$ 种选法. 因此不难证明原题结论. ♣

4.3.2 Some Meaningful Exercises

Problem 1. 设 F 为一个特征为素数 p 的域，$F(\alpha)$ 是 F 上的单超越扩张，证明：$x^p-\alpha$ 在 $F(\alpha)[x]$ 上不可约.

证明 关键是要记得，若 $f(x)\in D[x]$ 上不可约，则 $f(x)$ 在 $\mathrm{Frac}(D)[x]$ 上也不可约，这里 $\mathrm{Frac}(D)$ 表示 D 的分式域，故只需证 $x^p-\alpha$ 在 $F[\alpha][x]$ 上不可约，使用 Eisenstein 判别法即可. ♣

Problem 2. 求 $(x^2-2)(x^3-3)$ 在 $\mathbb{Q}$ 上的分裂域与其分裂域自同构的数目.

解 给定一个多项式 $f(x)\in F[x]$，如果 F 为数域，那么可以求出其在 $\mathbb{C}$ 上的根，从而将这些根添入 F 即可得到分裂域，如本题有根 $\pm\sqrt{2}$ 和 $\sqrt[3]{3}\zeta^k$，这里 ζ 为三次单位根，从而分裂域为 $\mathbb{Q}(\sqrt{2},\sqrt[3]{3}\zeta)=\mathbb{Q}(\sqrt{2},\sqrt[3]{3},\zeta)$，接下来对分裂域 $F(\alpha_1,\cdots,\alpha_n)$，我们一般都会像 $\mathbb{Q}(\sqrt{2},\sqrt[3]{3},\zeta)$ 这样整理成每个 α_i 的最小多项式都互不相同的情形，从而我们只需要确定每个 α_i 的次数即可，比如 x^2-2，x^3-3，x^2+x+1，从而自同构个数为 $2\times3\times2=12$. ♠

Problem 3. 设 p 为素数，求多项式 x^p-2 在 $\mathbb{Q}$ 上的分裂域 E，并求 $[E:\mathbb{Q}]$.

解 仿照上一题，首先在 $\mathbb{C}$ 上找到所有根 $\sqrt[p]{2}\zeta^k$，这里 ζ 为 p 次单位根，从而分裂域为

$$E=\mathbb{Q}(\sqrt[p]{2},\cdots,\sqrt[p]{2}\zeta^k,\cdots,\sqrt[p]{2}\zeta^{p-1})=\mathbb{Q}(\sqrt[p]{2},\zeta).$$

进一步注意到 $\sqrt[p]{2}$ 的次数为 p，ζ 次数为 $p-1$，且 $(p,p-1)=1$，因此 $[E:\mathbb{Q}]=p(p-1)$.(对于二重扩张 $F(\alpha,\beta)$，如果 α,β 的扩张次数互素，则二重扩张的次数恰为两次数乘积). ♠

Problem 4. 求多项式 x^4-x^2+1 在 $\mathbb{Z}_3$ 上的分裂域.

解 如果 F 不为数域，则无法直接在 $\mathbb{C}$ 上找到根填充进去，就得采用 Kronecker 构造，对 $f(x)$ 进行不可约分解，逐渐商掉不可约因式生成的极大理想，故我们本题先要对 x^4-x^2+1 在 $\mathbb{Z}_3$ 上不可约分解，这是具有技巧性的，注意到 $f(x)=(x^2+1)^2$，故分裂域为 $\mathbb{Z}_3[x]/(x^2+1)$. ♠

Problem 5. 设 F 为域，E 是次数为 n 的 $f(x)\in F[x]$ 的分裂域，证明：$[E:F]\mid n!$.

证明 我们对 n 用数学归纳法，$n=1$ 时显然成立，因为 $E=F$，假设命题对小于 n 均成立，则对次数为 n 时，设 α 是 $f(x)$ 的任一根，我们自然想到 $f(x)=(x-\alpha)f_1(x)$，这里 $f_1(x)\in F(\alpha)[x]$，从而 $[E:F]=[E:F(\alpha)][F(\alpha):F]$，由归纳假设可知 $[E:F(\alpha)]\mid(n-1)!$，因为 E 显然是 $f_1(x)\in F(\alpha)[x]$ 的分裂域，但是，$[F(\alpha):F]$ 我们只知道其不超过 n，但不一定整除 n 哇！从而我们只能回到原来的估计！但是如果 $f(x)$ 为 F 上的不可约多项式，则可知扩张次数为 n，从而完成归纳，这表明需要分类讨论.

若 $f(x)$ 在 F 上可约，存在 $f(x)=g(x)h(x)$，设 $g(x)$ 在 F 上分裂域为 G，$h(x)$ 视作 G 上多项式分裂域仍为 E，从而设两者次数为 n_1,n_2，则 $n_1+n_2=n$，且 $[G:E]\mid n_1!$，$[F:G]\mid n_2!$，故有 $[E:F]\mid n_1!n_2!\mid n!$，综上即证. ♣

4.4 域的正规扩张与可分扩张

4.4.1 Notes

当时，我们先学习各种群的基本知识，比如扩张、单群、可解群、导出列和降中心列等. 为什么要讲这些？不知道！学域论的时候，先讲各种扩张：有限扩张、代数扩张、超越扩张、正规扩张、可分扩张和不可分扩张等. 有什么用？不知道！更要命的是讲分裂域的时候自然要讨论分裂域的唯一性，构造了同构还不行，还要数一数同构的个数. 为什么要数个数？不知道！

————朱富海，《问题引导的代数学》

为了给 Galois 扩张做铺垫，我们先介绍可分扩张和正规扩张，尽管让人感到莫名其妙，但是不妨先耐住性子，数学总是循序渐进的：

正规扩张

定义 4.4.1: 正规扩张

设 E/F 为代数扩张，称其为**正规扩张**，若 E 中任何元在 F 上的极小多项式在 E 中分裂，或者说 $F[x]$ 中的任何不可约多项式 $p(x)$ 只要在 E 中有一个根，则 $p(x)$ 在 E 中分裂.

注：上面定义无非是在说任给一个 $F[x]$ 上多项式，在 E 上要么无根，要么分裂，如果无论有没有根，都分裂，那么 E 实际上是 F 的代数闭包，因此加上有根才分裂的性质表明正规扩张是一种介于分裂域和代数闭包的性质.

我们看看正规扩张有没有什么等价刻画，毕竟从定义出发，我们要想验证一个扩张是正规扩张，我们要么得验证每个 $F[x]$ 上每个不可约多项式，要么验证每个 F 中元素极小多项式，显然不现实，自然地，我们先考虑有限正规扩张：

定理 4.4.1: 有限正规扩张与多项式分裂域

设 E/F 为有限扩张，则 E/F 正规当且仅当存在 $f(x)\in F[x]\setminus F$，使得 E/F 是 $f(x)$ 的分裂域. 换言之，我们想要验证一个有限扩张是否正规，找到一个多项式使得其恰好为分裂域即可，这说明有限正规扩张和单个多项式分裂域是一回事！

证明 对于大前提的有限扩张，我们自然要假设 $E=F(\alpha_1,\cdots,\alpha_n)$，从而一方面，若为正规扩张，我们知道对每个 α_i，$p_i(x)=\mathrm{Irr}(\alpha_i,F)$ 都在 E 上分裂，现在我们想找到一个 $f(x)\in F[x]$ 使得 E 是 $f(x)$ 的分裂域，要紧的是保证 f 系数全在 F 中，因此自然会想到取 $f(x)=p_1(x)\cdots p_n(x)$，则显然在 E 中分裂，而 $f(x)$ 完全分解后根均在 α_i 中，因此不难看到 $E=F(\alpha_1,\cdots,\alpha_n)$ 是 $f(x)$ 分裂域，这是直接运用分裂域定义哦！

另一方面，我们知道 E 是 $f(x)$ 的分裂域，我们想要说明这是正规扩张，就要对任意 $\alpha \in E$，设其极小多项式为 $p(x) = \mathrm{Irr}(\alpha, F)$，说明其在 E 上分裂，换言之考虑 K 为 $p(x)f(x)$ 在 F 上的分裂域，我们想要说明对 $\beta \in K$，且 $p(\beta) = 0$，则 $\beta \in E$！一个经典的操作是考虑域同构 $\sigma : F(\alpha) \to F(\beta)$，$\sigma(\alpha) = \beta$，则我们只需要说明 $\sigma(\alpha) \in E$ 即可！我们将 σ 延拓为 K 上的 F 自同构，因此由 $E = F(\alpha_1, \cdots, \alpha_n)$，这里 α_i 为 $f(x)$ 的根集，则 σ 是根集上的一个置换，因此 $\sigma(E) = F(\sigma(\alpha_1), \cdots, \sigma(\alpha_n)) = E$，也就说明了 $\sigma(\alpha) \in E$！综上我们完成了证明. ♣

注：尽管上述证明存在一定的技巧性，但结论是相当自然好记的，拿出一个有限扩张，只要它是分裂域，不管三七二十一，就是正规扩张，由此可见正规扩张非常容易判断，分裂域就足够. 但另外也容易误解的是，似乎每个有限扩张都是正规扩张？那可不一定哩，因为有限扩张可不总能实现成分裂域，如 $\mathbb{Q}(\sqrt[3]{2})$.

当然也会遇到不是有限扩张的情形，但我们有类似的判别手段：

定理 4.4.2: 一般正规扩张的判别方法

E/F 是正规扩张当且仅当存在一族 $F[x] \setminus F$ 上的多项式 $\mathscr{F}$，使得 E 为 $\mathscr{F}$ 在 F 上的分裂域，换言之对无限扩张，就需要成为更多多项式的分裂域.

证明 证明是非本质的，留给感兴趣的读者，当然也可参考 B.B Xu 的讲义. ♣

借助这个结论我们有：

命题 4.4.1: 正规扩张的一个传递性

若 E/F 正规，则对任意 $E/K/F$，有 E/K 正规.

证明 几乎是显然的，因为 E 是 F 上一族多项式的分裂域，从而这些多项式自然可以看成 K 上的，利用上面定理即知命题成立. ♣

联想到代数扩张的传递性，E/K 代数，K/F 代数，则 E/F 代数，但正规扩张不具备这样的传递性，如考虑 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$，则注意到 $\mathbb{Q}(\sqrt[4]{2})$ 是 $x^2 - \sqrt{2}$ 在 $\mathbb{Q}(\sqrt{2})$ 的的分裂域，进而为正规扩张，$\mathbb{Q}(\sqrt{2})$ 是 $x^2 - 2$ 在 $\mathbb{Q}$ 上分裂域，进而也是正规扩张，但是注意到在 $\mathbb{Q}$ 上，对不可约多项式 $x^4 - 2$，$\mathbb{Q}(\sqrt[4]{2})$ 并不是其分裂域！因此 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 并非正规扩张.

上面这个反例也进一步让我们熟悉了如何判断正规扩张，正向判断只需取出一个多项式说明分裂即可，判断否定则选取一个不可约多项式论证其不分裂即可.

事实上正规扩张的“正规”也并非空穴来风，在下一章 Galois 理论中，我们将会看到，对子群 $H < \mathrm{Gal}(E/F)$，H 为正规子群当且仅当 $\mathrm{Inv}(H)/F$ 是正规扩张.

可分扩张

定义 4.4.2: 可分多项式

设 F 为域，若不可约多项式 $p(x) \in F[x]$ 在其分裂域上无重根，则称 $p(x)$ 在 F 上**可分**；若 $f(x) \in F[x]$ 的每个不可约因式都可分，则称 $f(x)$ 在 F 上**可分**，否则称 $f(x)$ **不可分**.

进一步，我们有可分元与可分扩张的定义：

定义 4.4.3: 可分元、可分扩张

设 E/F 为代数扩张，任取 $\alpha \in E$，我们称其为 F 上的**可分元**，如果 $\mathrm{Irr}(\alpha, F)$ 可分，也即在其分裂域上 (可不一定是 E！) 无重根. 进一步，如果任意 $\alpha \in E$ 均为可分元，则称 E/F 为**可分扩张**.

我们不难有可分扩张的传递性：

定理 4.4.3: 可分扩张的传递性

设 E/F 可分，则对 $E/K/F$ 有 E/K，K/F 均可分.

证明 注意到论证可分，我们目前就只有定义一个路子，定义无非就是说任取一个元素，看它极小多项式在分裂域上有没有重根，因此对 K/F 而言，证明其可分是显然的，因为 $\alpha \in K \subseteq E$，从而 $\mathrm{Irr}(\alpha, F)$ 自然在其分裂域上可分.

论证 E/K 可分本质就一个观察，任取 $\alpha \in E$，我们已经有 $\mathrm{Irr}(\alpha, F)$ 是可分的 (时刻注意可分是针对其分裂域而言的，不同多项式可分落脚的分裂域不一定相同)，而$\boxed{\mathrm{Irr}(\alpha, K) \mid \mathrm{Irr}(\alpha, F)}$，因此不难有这个多项式在其分裂域上无重根. ♣

类似于正规扩张，一个多项式分裂域就能判别，我们希望对可分扩张也有这样的有限刻画，于是下面两个结果如我们所愿：

命题 4.4.2: 可分元的单扩张是可分扩张

设 $F(\alpha)/F$ 代数，α 在 F 上可分，则 $F(\alpha)/F$ 可分.

证明 设 K/F 为 $\mathrm{Irr}(\alpha, F)$ 的分裂域，而 $\mathrm{Irr}(\alpha, F)$ 可分，从而 K/F 是可分多项式的分裂域，进而为 Galois 扩张，因此为可分扩张.(这里的证明有循环论证的嫌疑，但是对于熟悉理论并记忆而言，记住这个证明是最有益的). ♣

利用归纳法，我们实际上有

定理 4.4.4: 有限扩张是可分扩张当且仅当生成元可分

对有限扩张 $F(\alpha_1,\cdots,\alpha_n)/F$，其为可分扩张当且仅当 $\alpha_1,\cdots,\alpha_n$ 在 F 上可分.

面这个定理一个饶有趣味的推论是说，任给两个可分元 α,β，它们做四则运算仍为可分元，同代数扩张一样，任给两个代数元做四则运算仍为代数元，这一点直接从定义都不容易看出 (你甚至很难写出 $\alpha+\beta$ 的极小多项式！)，但利用一些巧妙的代数转化，一切却变得那么轻松，真如魔术一般.

$\star$ $\star$ $\star$ $\star$ $\star$ $\star$ $\star$ $\star$

为了研究可分扩张，本质上就是讨论每个元素是否可分，也即讨论其对应极小多项式在分裂域上是否有重根，但找分裂域总是一个麻烦的操作，既然本质是看有无重根，那引入形式微商，借助高等代数即可给出一个轻松的判别方法:

定理 4.4.5: 多项式有无重根的判别法

域 F 上多项式 $f(x)$ 在其分裂域上无重根当且仅当 $(f(x),f'(x))=1$.

证明与高代如出一辙，接受它也并不是件困难的事，因此判断一个元素是否可分，只需要拿出它的极小多项式和它的导数磕一磕即可.

特别地，对不可约多项式，我们有

命题 4.4.3: 不可约多项式无重根

设 $p(x)\in F[x]$ 不可约，则 $p(x)$ 在其分裂域上有重根当且仅当 $p'(x)=0$.

证明 本质就一句话，$p(x)$ 不可约，从而 p 与 p' 互素，若有重根则必然导致 $p|p'$，即 $p'=0$. ♣

进一步，$p'=0$ 过于苛刻，以至于在特征为 0 的域上:

命题 4.4.4: 特征为 0 的域是完备域

若 $\mathrm{Ch}F=0$，则 $F[x]$ 上任何不可约多项式都是可分的，从而 F 上的任何多项式都是可分的 (回顾定义). 如果一个域所有多项式都可分，则称这样的域为**完备域**.

注: 完备域取自 perfect，为什么这样的域完美? 因为每个代数扩张自然都是可分扩张，完全不需要去验证任何事，这对后面 Galois 扩张的判别时大大简化了手续，只需判断正规性即可.

上面这个命题表明特征为 0 的域都是完备域，很好，那么我们自然要问，完备域特征一定为 0 吗? 于是我们下面研究特征为 p 的那些域，想要看它们何时完备，就是要去研究那些不可分多项式，希望他们尽可能不出现，为此我们得先研究它们的结构.

设 $\mathrm{Ch}F=p$ 为素数，考虑 $f(x)\in F[x]$ 为不可分不可约多项式，从而有 $f'(x)=0$，这表明每个 $1\leq\ell\leq n$，$\ell a_\ell=0$，若 $p\not|\ell$，则有 $a_\ell=0$，因此可知 $f(x)$ 实际上只有 p 幂次项，也即存

在 $f_2(x)\in F[x]$ 使得 $f(x)=f_2(x^p)$，容易看见 f_2 也不可约，从而继续这么拆分下去，一定能找到一个可分不可约多项式 $h(x)$ 使得 $f(x)=h(x^{p^k})$. 从而若有 $h(x)$ 在其分裂域上可分解为

$$h(x)=c(x-\beta_1)(x-\beta_2)\cdots(x-\beta_r),\quad \beta_i\neq\beta_j, i\neq j,$$

因此我们有 $f(x)=c(x^{p^k}-\beta_1)\cdots(x^{p^k}-\beta_r)$，设 α_i 为 $x^{p^k}-\beta_i$ 的根，于是我们有：

定理 4.4.6: 特征为 p 的域上不可分不可约多项式结构

设 $\mathrm{Ch}F=p$，$f(x)\in F[x]$ 为不可分不可约多项式，则在分裂域上可分解为

$$f(x)=c(x-\alpha_1)^{p^k}(x-\alpha_2)^{p^k}\cdots(x-\alpha_r)^{p^k},$$

其中 $k\in\mathbb{N}$，当 $i\neq j$ 时 $\alpha_i\neq\alpha_j$，且

$$h(x)=c(x-\alpha_1^{p^k})\cdots(x-\alpha_r^{p^k})\in F[x]$$

为可分的不可约多项式.

借助上面这个定理，我们已经基本上确定所有不可分多项式的形状了，那么我们只需要看看有没有什么充要条件保证上面这种形状的多项式不出现，为此我们研究 F 上的 Frobenius 同态 Fr. 其中，$\mathrm{Fr}(a)=a^p$ 为 F 上的一个自同态，由此我们有

定理 4.4.7: 特征为 p 的域为完备域的充要条件

设 $\mathrm{Ch}F=p$，则 F 为完备域当且仅当 Fr 是同构，换言之即 $F=F^p$.

证明 一方面，若 Fr 是同构，从若存在不可分不可约多项式，则 $f(x)=a_mx^{mp^k}+\cdots+a_1x^{p^k}+a_0$，而 $F=F^p$，因此每个 a_i，存在 b_i 使得 $a_i=b_i^p$，因此有

$$f(x)=\sum_{\ell=0}^{m}b_\ell^px^{p^k}=\left(\sum_{\ell=0}^{m}b_\ell x^{p^{k-1}}\right)^p$$

可约，矛盾！因此我们可知每个不可约多项式都可分，即证为完备域.

另一方面，若为完备域，但 $F\neq F^p$，从而存在 $a\in F$ 使得不存在 $b\in F$，有 $a=b^p$，也即 x^p-a 在 F 上无根，设在分裂域上有根 α，进而可知在分裂域上 $x^p-a=(x-\alpha)^p$，我们希望寻找到矛盾，即要否定 F 是完备域，换言之找到一个不可分不可约多项式，显然 x^p-a 已经不可分，我们迫切希望它不可约，事实上确实如此，若不然则有 $f=gh$，$g(x)=(x-\alpha)^r$，$h(x)=(x-\alpha)^{p-r}$，说明 $\alpha^r,\alpha^{p-r}\in F$，不难发现 $\alpha\in F$，矛盾！因此我们完成了证明. ♣

注意到域同态总是单射，对有限集而言单射即双射，因此有

命题 4.4.5: 特殊的完备域

有限域一定是完备域.

更强大地，我们有

定理 4.4.8: 完备域的好性质

完备域的代数扩张也是完备域.

证明 如果完备域 F 特征为 0，那么无所需证，对特征为 p 的，设 E/F 代数，则 E 特征也为 p，为证 E 完备，只需证明 $\mathrm{Fr}(E)=E$，注意到已有 $\mathrm{Fr}(F)=F$，从而我们任取 $\alpha\in E$，只需证明 $F(\alpha)$ 完备即可，而注意到 $\mathrm{Fr}(F(\alpha))=F(\alpha^p)$，从而

$$[F(\alpha):F]=[F(\alpha):F(\alpha^p)][F(\alpha^p):F]=[F(\alpha):F(\alpha^p)][F(\alpha^p):F],$$

其中 $[F(\alpha^p):F]=[F(\alpha^p):F]$ 是利用了 Fr 为域同态，且 $\mathrm{Fr}(F)=F$(这是一个经典技巧！)，从而即完成了证明. ♣

那么自然要问了，莫非全都是完备域？那可不对哦，找一个超越扩张就行：

例 4.4.1. *有限域 $\mathbb{F}_p$ 的单超越扩张 $\mathbb{F}_p(t)$ 不是完备域，考虑 x^p-t 即可，用 Eisenstein 判别法证明其不可约，不可分是简单的.*

4.4.2 Some Meaningful Exercises

Problem 1. 设 $F(\alpha)/F$ 为单代数扩张：

1. 若扩张次数为 2，证明一定为正规扩张；
2. 举例说明扩张次数为 3，不一定为正规扩张.

证明 借助本题回顾正规扩张的判别法，注意是有限扩张，因此判断是否为分裂域只需要找到一个不可约多项式分裂即可，自然的，考虑 $f(x)=\mathrm{Irr}(\alpha,F)$，则 f 次数为 2，在 $F(\alpha)$ 中显然有 $f(x)=(x-\alpha)f_1(x)$，这里 $f_(x)=x-\beta$，从而 $\beta\in F(\alpha)$，也即分裂，即证.

而为了举例说明不一定是正规扩张，即要求存在不可约多项式不分裂，如 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$，显然 x^3-2 在 $\mathbb{Q}$ 上不可约，且在 $\mathbb{Q}(\sqrt[3]{2})$ 不分裂，因为有复根的存在. ♣

Problem 2. 记 E/F 为一个代数扩张. 证明：存在一个最大的中间域 K，满足 K/F 为正规扩张.

Problem 3. 设 F 为一个特征为素数 p 的域，记 E/F 为域扩张.

1. 证明 E/F 为纯不可分扩张当且仅当任意 $\alpha \in E \setminus F$，其极小多项式形如 $x^{p^s} - a$.
2. 证明若 E/F 为有限的纯不可分扩张，则存在 $m \in \mathbb{N}^*$ 使得 $[E : F] = p^m$.

证明 (1) 纯不可分扩张即指任意 $\alpha \in E - F$，有 α 在 F 上的极小多项式在其分裂域上不可分，也即有重根，从而一方面若极小多项式形如 $x^{p^s} - a$，则其在分裂域上有根 $\alpha^{p^s} = a$，因此在分裂域上，$x^{p^s} - a = (x - \alpha)^{p^s}$，因此有重根，也即不可分，即证纯不可分.

若 E/F 为纯不可分扩张，任取 $\alpha \in E \setminus F$，则由 α 为不可分元，因此其极小多项式为不可分的不可约多项式，因此在分裂域上其形如 $f(x) = (x - \alpha_1)^{p^k} \cdots (x - \alpha_t)^{p^k}$，且 $g(x) = (x - \alpha_1^{p^k}) \cdots (x - \alpha_t^{p^k})$ 为可分的不可约多项式，从而有 $f(\alpha) = g(\alpha^{p^k}) = 0$，由 α^{p^k} 为 g 的根，且 g 可分不可约，因此 α^{p^k} 为可分元，进而在 F 中，因此 $x - \alpha^{p^k} \in F[x]$ 为 g 的因式，而 g 不可约，因此 $g(x) = x - \alpha^{p^k}$，也即 $f(x) = x^{p^k} - \alpha^{p^k} \in F[x]$，即证.

(2) 设 $E = F(\alpha_1, \cdots, \alpha_n)$，我们对 n 用归纳法，$n = 1$ 时由 (1) 即知成立，而对一般的 n，注意到 $[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F]$，这里说明 $[E : F(\alpha_1)]$ 为 p 的幂次并不简单. ♣

Problem 4. 证明：纯不可分扩张的 Galois 群为平凡群.

证明 注意到任取 E/F 为纯不可分扩张，$\varphi \in \mathrm{Gal}(E/F)$，则有 $\varphi(\alpha)$ 与 α 为 F 上的共轭元，而 α 在 F 上极小多项式形如 $x^{p^s} - a$，α 为 p^s 重根，因此 $\varphi(\alpha) = \alpha$，即证 $\varphi = \mathrm{id}$，因此其 Galois 群为平凡群. ♣

5 Galois 理论

5.1 域的代数闭包

5.1.1 Notes

在上一章中，我们已经回答了对任给 $f(x) \in F[x]$，我们能找到其的一个分裂域 E 使得 $f(x)$ 在 E 上可以完全分解，那么再挑一个 $g(x)$，E 显然不一定为其分裂域，那么能否找到一个最大的分裂域呢？我们先给这个希望存在的域起一个名字：

定义 5.1.1: 域的代数闭包

设 K/F 为代数扩张，且使得任给 $f(x) \in F[x]$，均有 $f(x)$ 在 K 中分裂，我们称 K 为 F 的**代数闭包**.

通常情况下，我们也会用代数封闭去定义代数闭包：

定义 5.1.2: 代数闭包的另一定义

任给一个域 K，我们称之为**代数封闭**的，若任给 $f \in K[x]$，f 在 K 中有根. 进一步，任给一个域 F，我们称 F 的一个代数扩张是 F 的代数闭包，若K 是代数封闭的.

注：这两个定义是等价的，要紧的是前一定义蕴含后一定义 (因为看起来第二个定义要求更多一些哩！)，不妨假设 F 的代数闭包 K 不是代数封闭的，那么存在 $f(x) \in K[x]$ 在 K 中无根，不妨 f 在 K 上不可约，考虑 f 在 K 上的分裂域 E，有根 $\alpha \in E$，由 E/K，K/F 均为代数扩张，从而 E/F 为代数扩张，故 α 是 F 上的代数元，则考虑其在 $F[x]$ 上的最小多项式 g，g 在 K 中分裂，从而 $\alpha \in K$，矛盾！

5.1.2 Some Meaningful Exercises

5.2 Galois 群

5.2.1 Notes

Galois 理论的核心是帮助我们认识域上多项式 $f(x) \in F[x]$ 的根的情况，在其分裂域上我们能够显式的表示出这些根，但是它们之间的内在联系却并不清楚，一个自然的观察是：

命题 5.2.1: 域的自同构诱导出根集合的置换

设 E/F 为域扩张，$\alpha \in E$，为多项式 $f(x) \in F[x]$ 的根，则对任意 $\varphi \in \mathrm{Aut}(E/F)$，即保持 F 不动的 E 自同构，有 $\varphi(\alpha)$ 也为 $f(x)$ 的根.

由此可见，某种程度上若 E 为 $f(x)$ 的分裂域，那么研究 $\mathrm{Aut}(E/F)$ 这个结构，变相刻画了 $f(x)$ 之间根的关系，这一天才的想法是我们做后续讨论的核心，为此我们重述一些概念：

定义 5.2.1: Galois 群、共轭元

设 E/F 为域扩张，则我们考虑所有 E 上保持 F 不动的域自同构，也即这样的自同构 $\sigma : E \to E$，使得 $\sigma|_K = \mathrm{id}$，容易验证所有的 σ 关于复合运算构成群，称为 E/F 的 **Galois 群**，记为 $\mathrm{Gal}(E/F)$，我们称 $\alpha, \beta \in E$ 是**共轭**的，如果它们具有相同的极小多项式，也即 $\mathrm{Irr}(\alpha, F) = \mathrm{Irr}(\beta, F)$，显然我们有任意 $\alpha \in E$ 为 F 上代数元，$\sigma \in \mathrm{Gal}(E/F)$，$\alpha$ 与 $\sigma(\alpha)$ 共轭.

注意我们这里 Galois 群是对一般的域扩张定义的，为了求出一般域扩张对应的 Galois 群，一个自然的想法是对一些生成元先寻找域同态，再找出其中的域同构，但是下面这个定理告诉我们，对很好的扩张，域同态自动保证了同构：

定理 5.2.1: 代数扩张的一个重要性质

设 E/F 为代数扩张，则 $\mathrm{Hom}_F(E, E) = \mathrm{Aut}_F(E) = \mathrm{Gal}(E/F)$.

证明 为了澄清思路，首先需要注意的就是域同态永远要求是单射，为此我们只需证明是满射即可，任取 $\alpha \in E$，φ 为保持 F 的域同态，则设 f_α 为 α 在 F 上的极小多项式，设其在 E 上的根的全体为 $\alpha_1, \cdots, \alpha_n$(注意并不意味着是全体根！)，因此 φ 是 $\{\alpha_1, \cdots, \alpha_n\}$ 的一个置换，从而对有限扩张 $K = F(\alpha_1, \cdots, \alpha_n)$，$\varphi(K) \subseteq K$，而 $\varphi(K)$ 与 K 均为 F 上有限维线性空间，且 φ 单，因此 $\varphi(K) = K$，进而 $\alpha \in \mathrm{Im}(\varphi)$，因此 φ 为满射，即证为域同构. ♣

现在让我们回到对 Galois 群的研究上来，研究一个群的最好办法就是寻找它的子群，通过对子群分析从而实现对大群的认识，任取域扩张 E/F，选取其 Galois 群的一个子群 G，显然 G 是由一堆域的自同构组成的，因此我们自然会意识到，由于 G 略小于 $\mathrm{Gal}(E/F)$，那么或许它会固定一个比 F 略大的域！(注意理解这里大小的逆转)，由此我们自然有：

定义 5.2.2: 不变子域

任取 $\varphi \in \mathrm{Gal}(E/F)$，我们定义

$$\mathrm{Inv}(\varphi) := \{\alpha \in E | \varphi(\alpha) = \alpha\},$$

显然 $\mathrm{Inv}(\varphi)$ 构成 E 的一个子域，称其为 φ 的**不变子域**，也即 $\varphi|_{\mathrm{Inv}(\varphi)} = \mathrm{id}$，进一步，任取 G 为 $\mathrm{Gal}(E/F)$ 子群，从而可类似定义 $\mathrm{Inv}(G)$，注意到其实际上是 $\bigcap_{\varphi \in G} \mathrm{Inv}(\varphi)$，从而也为一个中间域，以后为了书写方便，我们也简记为 E^{φ} 和 E^{G}.

我们设 $\mathcal{G}$ 表示 $\mathrm{Gal}(E/F)$ 的全体子群，$\mathcal{I}$ 表示 E/F 的全体中间域，因此上述定义实际上给出了这两个集合之间的映射：

$$\mathrm{Inv} : \mathcal{G} \to \mathcal{I}, \quad G \mapsto \mathrm{Inv}(G),$$

自然的我们也能得到另一个方向的映射：

$$\mathrm{Gal} : \mathcal{I} \to \mathcal{G}, \quad K \mapsto \mathrm{Gal}(E/K).$$

一个自然的问题是这映射是互为逆映射吗？我知道你很急，我也很急，但是要想解决这个问题还有点远，我们先来逐步探索一些性质和条件，跳出子群子域的约束，我们先来做一些整体观察，为此先看几个例子是迫切且必要的：

例 5.2.1. 我们考虑 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$，显然这个域扩张次数为 2，我们先来求一下其 Galois 群，由于恰好有基 $\sqrt{2}$，从而任何一个自同构将会把 $\sqrt{2}$ 送到 x^2-2 的根里，也即 $\varphi \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ 会有两种选法，因此不难看到这个 Galois 群实际上是一个二阶群，即有 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})|$.

例 5.2.2. 我们再考虑 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$，仍然可见其扩张次数为 3，但任取一个自同构 φ，$\varphi(\sqrt[3]{2})$ 将会是 x^3-2 的根，但令人遗憾的是，在 $\mathbb{Q}(\sqrt[3]{2})$ 中，这个方程除了 $\sqrt[3]{2}$ 再没有别的根了，因此 $\varphi = \mathrm{id}$，换言之 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 是平凡群，我们有 $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] > |\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})|$.

上面的这两个例子为我们提供了一个很好的直觉，有时候 E 不是那么好，对于某个元素 α，虽然自同构 φ 会把 α 送到其共轭元，但这个共轭元会因为 E 不一定是极小多项式的分裂域而导致不在其中，这会大大缩小 $\mathrm{Gal}(E/F)$ 的可能性和大小，换言之，我们有

定理 5.2.2: Galois 群的大小被域扩张次数控制

对任意域扩张 E/F，我们有 $|\mathrm{Gal}(E/F)| \leq [E : F]$，这里不等关系考虑广义实数.

证明 若 $[E : F] = \infty$，则结论不证自明，我们不妨考虑为有限扩张，但我们实现并不能由此断言 $\mathrm{Gal}(E/F)$ 也是有限群，因此一个要小聪明的办法是任取 n 个 $\mathrm{Gal}(E/F)$ 中不同的元素 $\sigma_1, \cdots, \sigma_n$，我们去证明 $[E : F] \geq n$.

反证法，如果 $[E:F]=r<n$，那么设 $e_1,\cdots,e_r$ 是一组基，因此我们发现对于一个 E 上的线性方程组

$$\begin{cases}\sigma_1(e_1)x^1+\cdots+\sigma_n(e_1)x^n=0\\ \cdots\\ \sigma_1(e_r)x^1+\cdots+\sigma_n(e_r)x^n=0\end{cases},$$

由于未知量个数 n 大于方程的个数 r，从而未知量很自由，肯定有一组非零解，而回忆一下，$e_1,\cdots,e_n$ 不恰好是一组基吗，对任意 $\alpha=a^ie_i$，我们有 $x^i\sigma_i(\alpha)=x^i\sigma_i(a^je_j)=a^j(x^i\sigma_i(e_j))=a^j\cdot 0=0$，从而表明 $x^i\sigma_i=0$，也即我们任取了 n 个不同的域自同构，它们却总是 $E-$ 线性相关的，这好像顶荒谬！但澄清它并不容易，我们需要下面这个引理：

引理 5.2.3 (Dedekind 无关性定理)**.** *设 E/F 为域扩张，且 $\sigma_1,\cdots,\sigma_n\in\mathrm{Gal}(E/F)$ 且互不相同，则它们 $E-$ 线性无关，也即若有 $x^i\in E$ 使得 $x^i\sigma_i=0$，那么一定有 $x^i=0$.*

没别的手段，掏出归纳的武器罢，$n=1$ 是不言而喻的，假设 $n=k-1$ 已经证明，换言之任取 $k-1$ 个不同的域自同构，那么其线性无关，现在考虑 k 个不同的域自同构 σ_i，反证法若线性相关，则存在 $x^i\in E$，$x^i\sigma_i=0$，若 x^i 中有 0，那么利用归纳假设可知矛盾，因此 x^i 均不为 0.

故我们分别代入 $\alpha\in E$ 和 $a\alpha\in E$，那么 $x^i\sigma_i(\alpha)=0$，$x^i\sigma_i(a\alpha)=x^i\sigma_i(a)\sigma_i(\alpha)=0$，因此第一式乘上 $\sigma_k(a)$ 减去第二式，则有 $x^i(\sigma_k(a)-\sigma_i(a))\sigma_i(\alpha)=0$，这里 $1\le i\le k-1$，由 α 任意性即可得到 $x^i(\sigma_k(a)-\sigma_i(a))\sigma_i=0$，利用 σ_i 互不相同可知 $x^i(\sigma_k(a)-\sigma_i(a))$ 不全为 0，这又与归纳假设矛盾. 综上我们完成了引理的证明，进一步也即定理得证. ♣

上面这个定理给予了我们 Galois 群大小的一侧直观，前面的两个例子告诉我们不等式可以是严格的，因此一个有价值的问题是：对什么样的域扩张 E/F，才会有等号成立？换言之，什么时候会有另一个方向的不等式 $[E:F]\le|\mathrm{Gal}(E/F)|$ 成立？我们有：

命题 5.2.2: Artin 引理，给出另一方向的不等式估计

设 E 为域，$G<\mathrm{Aut}(E)$ 为一个有限子群，并记 $F=\mathrm{Inv}(G)$. 则有 $[E:F]\le|G|$.

证明 注意这个命题与上一定理的区别，上一定理对域扩张没有任何限制和要求，但这里我们要求域必须是某个有限群的不变子域，某种程度上，这便是一个取等条件.

设 $|G|=n$，$G=\{\sigma_1,\cdots,\sigma_n\}$，从而为证明 $[E:F]\le n$，回忆与扩张次数本质无非就是线性空间的维数，那么最朴素的想法就是证明任取 E 中 $n+1$ 个元素，证明它们线性无关便行咧！(不过是“虚张声势的线性代数”)

任取 $e_1,\cdots,e_n,e_{n+1}\in E$，考虑线性方程组：

$$\begin{cases}\sigma_1(e_1)x^1+\cdots+\sigma_1(e_{n+1})x^{n+1}=0\\ \cdots\\ \sigma_n(e_n)x^1+\cdots+\sigma_n(e_{n+1})x^{n+1}=0\end{cases},$$

注意！与上一定理不同，那里我们研究 Galois 群，关心 σ_i 的线性关系，但这里关心 e_i，从而两个地方的方程组会有一点区别.

显然这个方程组会有一组非零解 $(b^1,\cdots,b^{n+1})$，设 $\sigma_k=\mathrm{id}$，那么带回第 k 个方程，我们即有 $b^ie_i=0$，证毕？错误的，注意 $b^i\in E$，从而我们这里只证明出 e_i 是 $E-$ 线性相关的，这其实这相当于一句废话. 这表明任取一组解还不够！我们下面看看需要什么条件约束：

不失一般性设 $b^1\neq 0$，进而约定其为 1，这样已经保证了一个元素在 F 中，如果仍然有 $b^i\notin F$，不妨设为 b^2，因此一定存在 $\sigma\in G$ 使得 $\sigma(b^2)\neq b^2$(为什么一定存在？$F=\mathrm{Inv(G)}$ 阐明了原因，这里域取的“足够”大)，因此对任意 $1\leq i\leq n$，

$$\sigma\circ(\sigma_i(e_i)b^i)=(\sigma\sigma_i)(e_1)+(\sigma\sigma_i)(e_j)\sigma(b^j)=0,$$

注意这里 $\sigma(b^1)=1$，而 $\sigma\in G$，且 G 为有限群，从而 $\sigma\sigma_i=\sigma_{i'}$，且不难发现 $\sigma(b^j)$ 也是方程组的一个解！因此我们得到另一组解 $(\sigma(b^1),\cdots,\sigma(b^{n+1}))$.

现在对比两个解，聪明的读者，你现在知道对 $(b^1,\cdots,b^{n+1})$ 这个解做什么限制便可以得到矛盾吗？注意事实上两者做差，得到 $(0,\cdots,b^k-\sigma(b^k),\cdots)$ 也是解！凭空多出了个 0，因此一个巧妙的想法是，取 (b^i) 为方程组所有解中零的个数最多的！由此便导出矛盾. ♣

总结一下，我们得到了

推论 5.2.1

设 $G<\mathrm{Aut}(E)$ 为有限子群，$F=E^G$，则 $G=\mathrm{Gal}(E/F)$.

综合以上信息，我们对有限扩张认识的比较清晰了，其中容易看见对满足 $[E:F]=|\mathrm{Gal}(E/F)|$ 的扩张，性质是相对较好的，这也是我们未来研究的重点：

定义 5.2.3: Galois 扩张

设 E/F 为有限扩张，如果有 $[E:F]=|\mathrm{Gal}(E/F)|$，我们称其为**有限 Galois 扩张**.

等价地，我们有如下描述：

定理 5.2.3: 有限 Galois 扩张的等价描述

设 E/F 为有限扩张，则下面描述等价：

1. E/F 是有限 Galois 扩张；
2. $[E:F]=|\mathrm{Gal}(E/F)|$；
3. F 是 $\mathrm{Aut}(E)$ 的某个有限子群 G 的不变子域；
4. F 为 $\mathrm{Gal}(E/F)$ 的不变子域.

注意：虽然看起来上面第 3 个等价描述被第 4 个所覆盖，但事实上第 3 个在构造 Galois 扩张时非常有用，因为我们只需要对一个域 E，从 $\mathrm{Aut}(G)$ 里挑出一个有限子群 G，那么对 $F = \mathrm{Inv}(G) = E^G$，自然有 E/F 是 Galois 扩张！

现在有了有限扩张的案例，我们再回头来研究研究映射 Inv 和 Gal，稍稍回忆一下，它们分别是 $\mathcal{G} \to \mathcal{I}$ 和 $\mathcal{I} \to \mathcal{G}$ 的映射，前者把群变成域，看看哪些元在群作用下不变，后者把域变成群，看看哪些同构保持这些元素.

首先倒腾一下定义，我们有一些并不本质的性质：

命题 5.2.3: 一些集合与映射上的自然结果

设 $G < \mathrm{Gal}(E/F)$，任取 K 为 E/F 的中间域，我们有：

1. $G \subseteq \mathrm{Gal} \circ \mathrm{Inv}(G)$；
2. $K \subseteq \mathrm{Inv} \circ \mathrm{Gal}(K)$；
3. $\mathrm{Inv} \circ \mathrm{Gal} \circ \mathrm{Inv}(G) = \mathrm{Inv}(G)$；
4. $\mathrm{Gal} \circ \mathrm{Inv} \circ \mathrm{Gal}(K) = \mathrm{Gal}(K)$.

以上是纯粹集合论上的结果与性质，如果你热爱点集拓扑，那么相信聪明的你会喜欢完成这个证明，所以这里我就不给出证明了. 除此之外，还有如下两个比较明显的性质：

命题 5.2.4: Inv 与 Gal 的 “单调递减性”

设 E/F 为任一域扩张，则

1. 设 $G_1, G_2 < \mathrm{Gal}(E/F)$，则 $G_1 \subseteq G_2$ 当且仅当 $\mathrm{Inv}(G_1) \supseteq \mathrm{Inv}(G_2)$；
2. 设 K_1, K_2 是 E/F 的中间域，则 $K_1 \subseteq K_2$ 当且仅当 $\mathrm{Gal}(K_1) \supseteq \mathrm{Gal}(K_2)$.

事实上，更本质地，我们可以初步回答之前定义映射关心的问题：

定理 5.2.4: 映射的复合是否为单位映射？

设 E/F 为有限扩张，则映射

$$\mathrm{Gal} \circ \mathrm{Inv} : \mathcal{G} \xrightarrow{\mathrm{Inv}} \mathcal{I} \xrightarrow{\mathrm{Gal}} \mathcal{G}$$

为 $\mathcal{G}$ 即 $\mathrm{Gal}(E/F)$ 所有子群构成集合上的恒等映射.

证明 关键就一句话，任取 $G \in \mathcal{G}$，则对中间域 $K = \mathrm{Inv}(G)$，由于是有限扩张，G 为有限子群，从而 $G = \mathrm{Gal}(K) = \mathrm{Gal}(E/K)$，这便是我们想要证明的事情. ♣

5.2.2 Some Meaningful Exercises

Problem 1. 设 E/F 是一个有限 Galois 扩张，对 $\alpha \in E$，证明 $E = F(\alpha)$ 的充要条件为 α 在 $\mathrm{Gal}(E/F)$ 下的像两两不同.

证明 若 $E = F(\alpha)$，则 $\mathrm{Gal}(E/F)$ 中元素完全由 α 的像决定，因此不证自明；另一方面，注意到 α 在 $\mathrm{Gal}(E/F)$ 下的像两两不同，换言之，若有 $\varphi \in \mathrm{Gal}(E/F)$ 使得 $\varphi(\alpha) = \alpha$，则必有 $\varphi = \mathrm{id}$，由此对 $\psi \in \mathrm{Gal}(E/F(\alpha))$，则 $\psi \in \mathrm{Gal}(E/F)$ 且 $\psi(\alpha) = \alpha$，因此 $\psi = \mathrm{id}$，从而 $\mathrm{Gal}(E/F(\alpha))$ 平凡，进而由 E/F 为有限 Galois 扩张，从而有 $E/F(\alpha)$ 也为 Galois 扩张，故 $[E : F(\alpha)] = 1$，也即 $E = F(\alpha)$，即证. ♣

Problem 2. 设 F 是一个特征为 p 的域，对 $a \in F$，设多项式 $f(x) = x^p - x + a \in F[x]$ 不可约，求 $\mathrm{Gal}(E/F)$.

证明 设 f 在 E 中有根 α，从而 $f(\alpha + m) = 0$，也即 $f(x)$ 全部根为 $\{\alpha, \cdots, \alpha + p - 1\}$，因此可知 $E = F(\alpha)$，进而其为可分多项式的分裂域，从而为 Galois 扩张，即 $|\mathrm{Gal}(E/F)| = [E : F] = p$，因此由 p 为素数可知 $\mathrm{Gal}(E/F) \cong \mathbb{Z}_p$. ♣

Problem 3. 设 E/F 为一个有限 Galois 扩张，设 K_1, K_2 为 E/F 的两个中间域.

1. 证明：$K_1 \vee K_2 = E$ 当且仅当 $\mathrm{Gal}(E/K_1) \cap \mathrm{Gal}(E/K_2)$；
2. 若 K_1 为 F 的正规扩张，则 $\mathrm{Gal}(K_1 \vee K_2/K_2)$ 与 $\mathrm{Gal}(K_1/F)$ 的一个子群同构.

证明 (1) 我们证明一个更一般的结果，设 $K = K_1 \vee K_2$，则 $\mathrm{Gal}(E/K) = \mathrm{Gal}(E/K_1) \cap \mathrm{Gal}(E/K_2)$，显然左侧含于右侧，因为 $K_1, K_2 \subseteq K$，进而任取 $\sigma \in \mathrm{Gal}(E/K_1) \cap \mathrm{Gal}(E/K_2)$，则 $\sigma|_{K_1} = \mathrm{id}$，$\sigma\_K_2 = \mathrm{id}$，因此设 K_1, K_2 有基 α_i, β_j，则任意 $f = f(\cdots, \alpha_i, \cdots, \beta_j, \cdots) \in K$ 为 K_1, K_2 中元素的有理多项式，则 $\sigma(f) = f$，从而 $\sigma|_K = \mathrm{id}$，因此 $\sigma \in \mathrm{Gal}(E/K)$，即证.

(2) 思路是利用正规扩张，从而存在 F 上多项式在 K_1 中分裂，进而设全部根为 $\alpha_1, \cdots, \alpha_k$，则 $K_1 = F(\alpha_1, \cdots, \alpha_k)$，从而不难推理得到 $K_1 \vee K_2 = K_2(\alpha_1, \cdots, \alpha_k)$，因此考虑一个映射，$\varphi \in \mathrm{Gal}(K_1 \vee K_2/K_2)$ 送至 $\varphi_{K_1} \in \mathrm{Gal}(K_1/F)$，当然这其中有诸多细节需要验证. ♣

Problem 4. 求 $x^3 - 2 \in \mathbb{Q}[x]$ 的分裂域的 Galois 群，并对其所有子群求不变子域.

5.3 Galois 扩张与 Galois 对应

5.3.1 Notes

在上一节中，我们已经从有限扩张这一视角初步认识了 Galois 扩张，虽然直觉想起来，无非是指 $[E:F]=\mathrm{Gal}(E/F)$，但更本质地，似乎是说 F 是某个有限群的不变子域，而反过来，这个不变子域又恰好相对 $\mathrm{Gal}(E/F)$，从这个角度，我们自然得到了 $\mathrm{Gal}\circ\mathrm{Inv}$ 是恒等映射，但另一个方向似乎无从下手，这呼唤着我们进一步研究有限 Galois 扩张，抽象出更一般的性质.

设 E/F 是有限 Galois 扩张，$G=\mathrm{Gal}(E/F)$，我们希望看看这个扩张有没有更本质的刻画，换言之任取 $\alpha\in E$，它有什么特殊之处吗？设 $p(x)=\mathrm{Irr}(\alpha,F)$，自然 α 是 $p(x)$ 的根，我们考虑 α 在群 $\mathrm{Gal}(E/F)$ 作用下的轨道，也即 $\mathcal{O}_\alpha=\{\varphi(\alpha)|\varphi\in\mathrm{Gal}(E/F)\}=\{\alpha_1,\cdots,\alpha_n\}$，则对

$$f(x)=\prod_{i=1}^{n}(x-\alpha_i)\in E[x],$$

一个顶重要的观察是 $f(x)$ 各项系数为 $(-1)^k\sigma_k(\alpha_1,\cdots,\alpha_n)$，这里 σ_k 是 k 次齐次多项式，注意到任取 $\varphi\in\mathrm{Gal}(E/F)$，$\varphi(\sigma_k)=\sigma_k$，从而 $\sigma_k\in E^G=F$！这里运用了 $\varphi(\alpha_i)$ 是 α_i 的一个置换以及 σ_k 的对称性. 这竟然表明$f(x)\in F[x]$!

现在我们不难注意到，由 $f(x)$ 和 $p(x)$ 在 $E[x]$ 上有公共解 α，因此它们一定不互素 (Bezout 定理)，而 $p(x)$ 不可约，进而 $p(x)\mid f(x)$，而不难由 $f(x)$ 定义知道 $f(x)|p(x)$，这意味着 $f(x)=p(x)$！因此我们知道，对于有限 Galois 扩张而言，任取 $\alpha\in E$，我们有它在 F 的极小多项式满足：

- 可以分解成一次因式的乘积；
- 每个一次因式都不同，从而无重根.

因此回忆我们在上一章中引入的可分扩张与正规扩张，也即

定义 5.3.1: 可分扩张与正规扩张回顾

1. 称代数扩张E/F 为**正规扩张**，若 E 中任何元在 F 上的极小多项式在 E 中分裂，等价地，可以理解为 $F[x]$ 上不可约多项式 $p(x)$ 只要在 E 中有一个根，则 $p(x)$ 在 E 中分裂；
2. 称代数扩张E/F 为**可分扩张**，如果任意 $\alpha\in E$ 都是可分元，换言之即 $\mathrm{Irr}(\alpha,F)$ 可分 (注意不是分裂！)，也即在其分裂域上无重根.

总结起来，我们便得到了有限 Galois 扩张一个十分本质的描述：

定理 5.3.1: Galois 扩张的内蕴定义

有限 Galois 扩张 E/F 是可分、正规扩张，且 E 是 F 上一个可分多项式的分裂域.

因此沿着我们的思路，我们不难推广 Galois 扩张的定义，从有限扩张推广到代数扩张：

定义 5.3.2: Galois 扩张

称代数扩张E/F是 **Galois 扩张**，如果 E/F 是一个可分正规扩张.

下面我们来列举一些例子，这些例子足以阐明判断一个域扩张的一般化思路：

例 5.3.1. $\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}$ 是 Galois 扩张，注意到我们有两种切入角度，由于这是有限扩张，从而可以考虑去计算 $|\mathrm{Gal}(E/F)|$ 与 $[E:F]$，如果两者相等即证，另一种角度便是从可分正规扩张的角度出发，注意到正规非常容易，因为这是 x^3-2 的分裂域，可分也十分容易，因为 $\mathrm{Ch}\mathbb{Q}=0$! 由此可知这为 Galois 扩张.

注意上述定义的推广只是我们主线任务的副产品，我们最初的目标是研究映射 Gal 和 Inv，现在有了可分性和正规性这两大武器，我们可以自如的证明如下 Galois 基本定理：

定理 5.3.2: Galois 基本定理

设 E/F 是有限Galois 扩张，$G=\mathrm{Gal}(E/F)$，则

1. 映射 Gal 和 Inv
$$\mathrm{Gal}:\mathcal{I}\to\mathcal{G},\quad \mathrm{Inv}:\mathcal{G}\to\mathcal{I},$$
均为双射，且互为逆映射，则 G 的子群与 E/F 的中间域之间存在一一对应，称为 **Galois 对应**；

2. 对任意 $H<G$，我们有
$$|H|=[E:\mathrm{Inv}(H)],\quad [G:H]=[\mathrm{Inv}(H):F];$$

3. H 是 G 的正规子群当且仅当 $\mathrm{Inv}(H)/F$ 是正规扩张，且此时有
$$\mathrm{Gal}(\mathrm{Inv}(H)/F)\cong G/H.$$

注意：判断一个扩张是否为 Galois 扩张最经济的办法是看它是否为一个可分多项式的分裂域!

证明 1. $\mathrm{Gal}\circ\mathrm{Inv}=\mathrm{id}_{\mathcal{I}}$ 已在上一节的末尾证明，现在我们来看另一侧，任取 $E/K/F$，由 E/F 为有限 Galois 扩张，从而为正规可分扩张，更好用的，是 $F[x]$ 上可分多项式 $f(x)$ 的分裂域，进一步 $f(x)$ 可视为 K 上的可分多项式，因此不难有 E/K 为 Galois 扩张，现令 $H=\mathrm{Gal}(K)=\mathrm{Gal}(E/K)$，自然有 $E^H=K$，因此有 $\mathrm{Inv}\circ\mathrm{Gal}=\mathrm{id}_{\mathcal{G}}$，即为所证.

2. 不难知道 $E/\mathrm{Inv}(H)$ 为Galois 扩张 (这些应当内化为显然)，从而自然满足 $\mathrm{Gal}(E/\mathrm{Inv}(H))=H$，故有 $|H|=|\mathrm{Gal}(E/\mathrm{Inv}(H))|=[E:\mathrm{Inv}(H)]$，另一个方向的等式注意到 $E/\mathrm{Inv}(H)/F$ 即可.

3. 为了记号上的方便，我们记 $K = \mathrm{Inv}(H)$，因此我们现在要考察任取 $\varphi \in G$，群 $\varphi H \varphi^{-1}$ 到底是个啥，为了搞清楚本质就是弄懂这个群的不变子域是什么，由于子域 K 在 H 作用下不动，那自然想到对$\varphi(K)$ 即是 $\varphi H \varphi^{-1}$ 的不变子域，换言之两者是一一对应的，因此 H 正规当且仅当 $\varphi H \varphi^{-1} = H$，同时对应到子域上，当且仅当 $\varphi(K) = K$，这表明 $\varphi|_K$ 可以看成是 K 上的 $F-$ 自同构 (注意原来 φ 是让整个 E/F 动！).

因此我们有 $\varphi \mapsto \varphi|_K$ 是 G 到 $\mathrm{Gal}(E/K)$ 的同态，且核为 H，又每个 $\psi \in \mathrm{Gal}(K/F)$ 都可以延拓为 G 中元素，从而这是满同态，进而 $\mathrm{Gal}(E/K) \cong G/H$，而 $[G : H] = [K : F]$(上一条的结果)，故 K/F 是 Galois 扩张，毋庸置疑的，为正规扩张. ♣

推论 5.3.1: 一个简单的推论

若 E/F 为有限 Galois 扩张，则 E/F 有有限个中间域.

证明 阐明是容易的，只需要注意的中间域一一对应于 Galois 群的一个子群，而有限群的子群总是有限的，这便完成了证明. ♣

上述证明核心是利用了 Galois 扩张的一一对应，于是自然要问去掉命题还成立么?

例 5.3.2 (有限扩张不一定中间域有限). 考虑 $F = \mathbb{F}_p(t_1, t_2)$，$E/F$ 为 $(x^p - t_1)(x^p - t_2)$ 的分裂域，从而设 $\alpha_1, \alpha_2 \in E$，且 $\alpha_i^p = t_i$，因此有 $E = F(\alpha_1, \alpha_2)$，因此 $[E : F] = p^2$，下面我们说明任意 $a \neq b \in F$ 有 $F(a\alpha_1 + \alpha_2) \neq F(b\alpha_1 + \alpha_2)$，若不然，则有 $\alpha_1, \alpha_2 \in F(a\alpha_1 + \alpha_2)$，从而其实际上为 E，这表明扩张次数为 p^2，但注意到 $(a\alpha_1 + \alpha_2)^p = a^p t_1 + t_2 \in F$，从而扩张次数不超过 p，矛盾！因此这些讨论表明 E/F 有无数多个中间域.

5.3.2 Some Meaningful Exercises

5.4 多项式的 Galois 群

5.4.1 Notes

定理 5.4.1: 多项式不可约的一个判别法

多项式 $f(x)$ 不可约，当且仅当 $\mathrm{Gal}(E/F)$ 在其根集上的作用是可递的.

命题 5.4.1: 一些多项式的 Galois 群

1. 若 $f(x)$ 有且仅有两个复根，则 $\mathrm{Gal}(E/F) \cong S^p$;
2. 对三次多项式 $f(x) = x^3+ax^2+bx+c$, 若对 $D(f) = a^2b^2-4a^3c-4b^3+18abc-27c^2$, 若 $\sqrt{D(f)} \in F$，则 $\mathrm{Gal}(E/F) \cong A_3$，反之则同构于 S^3.

5.5 有限域

5.5.1 Notes

作为 Galois 理论的一个有趣应用，我们现在来考虑有限域，换言之即域 E 且 $|E|<\infty$，则其素域 $E_0\subseteq E$ 也有限，而我们知道素域无非就 $\mathbb{Q}$ 与 $\mathbb{F}_p$，因此可知有限域特征一定非 0.

自然我们要问，特征为 p 的有限域 E 长什么样呢？一个简单的结果是

命题 5.5.1: 有限域的阶

设 $\mathrm{Ch}E=p$，$|E|<\infty$，则存在 $n\in\mathbb{N}$ 有 $|E|=p^n$.

证明 注意到有 $[E:\mathbb{F}_p]$ 为有限扩张，若扩张次数为 n 即证. ♣

那是否所有的幂次都恰能取到呢？即 $|E|=p^n$ 这样的域是否存在且唯一？为此，我们先插入一条看似毫不相干的引理，我们断言$E^\times$ 其实是 p^n-1 阶循环群:

证明 我们证明一个更广的结论，对任意域 E，G 为 $E^\times$ 的有限子群，则 G 为循环群，注意到 G 为 Abel 群，因此可知若其最大元素阶为 m，$m\leq|G|$，则任意 $b\in G$，$b^m=1$，否则若有元素阶为 n 不为 m 因子，则有 $[m,n]$ 阶元素，便矛盾了. 进而考虑 $x^m-1=0$，则其在 G 上恰有 $|G|$ 个根，表明 $|G|\leq m$，因此 $m=|G|$，这便是我们想要阐明的. ♣

而注意到对任意 $\beta\in E^\times$，有 $\beta^{p^n-1}=1$，这恰好说明 E 中元素均为 $x^{p^n}-x\in\mathbb{F}_p[x]$ 的根，也即其分裂域，而由分裂域存在且唯一，我们有如下有限域的结构定理:

定理 5.5.1: 有限域的结构定理

任意 $n\in\mathbb{N}^*$，存在唯一阶为 p^n 的域 $E/\mathbb{F}_p$，且为 $x^{p^n}-x$ 的分裂域，$E^\times$ 为 p^n-1 阶循环群，并且 $E/\mathbb{F}_p$ 为单扩张，生成元为 $E^\times$ 的生成元.

注意到 E 是一个多项式的分裂域，我们敏锐的嗅到 $(x^{p^n}-1)'=-1$，因此这个多项式可分，进而为可分多项式的分裂域，换言之即为 Galois 扩张. 于是我们便自然好奇 Galois 群的结构:

命题 5.5.2: 有限域的 Galois 群

$\mathrm{Gal}(E/\mathbb{F}_p)$ 为 n 阶循环群，生成元为 Frobenius 同构 Fr.

证明 首先注意到 E 为有限域，从而为完备域 (任意多项式都可分)，进而有 Fr 为同构，注意到任意 $\beta\in E$ 均满足 $\beta^{p^n}=\beta$，因此 $\mathrm{Fr}^n=\mathrm{id}$，又注意到 $E^\times$ 有 p^{n-1} 阶元，因此 Fr 的阶为 n，又由 $E/\mathbb{F}_p$ 为 Galois 扩张，从而 $|\mathrm{Gal}(E/\mathbb{F}_p)|=[E:\mathbb{F}_p]=n$，又有 n 阶元，因此不难知命题成立. ♣

进一步，我们关心有限域的中间域的结构，于是有

命题 5.5.3: 有限域的子域

设域 $|E|=p^n$，若 F 为 E 的子域，则存在 $m\in\mathbb{N}$，$|F|=p^m$ 且 $m\mid n$；反之任意 $m\mid n$，存在 $F\subseteq E$ 为子域，且 $|F|=p^m$，且 $\mathrm{Gal}(E/F)=(\mathrm{Fr}^m)$.

证明 若 F 为 E 的子域，则 $F^\times$ 为 $E^\times$ 子群，从而 $p^m-1\mid p^n-1$，而熟知 $(p^m-1,p^n-1)=p^{(m,n)}-1$，从而可知 $m|n$. 另一方面可用 $\mathrm{Gal}(E/\mathbb{F}_p)\cong\mathbb{Z}_n$，且 $\mathbb{Z}_n$ 子群与中间域一一对应得到. ♣

有限域的结构特点可以帮助我们研究有限域上的不可约多项式，首先我们有如下结论：

命题 5.5.4: 有限域上不可约多项式存在性

任意 $n\in\mathbb{N}$，存在 n 次首一不可约多项式 $f(x)\in\mathbb{F}_p[x]$.

证明 注意到设 $E/\mathbb{F}_p$ 为 $x^{p^n}-x$ 的分裂域，则由之前的讨论，$E=\mathbb{F}_p(\alpha)$ 为单扩张，从而 $f(x)=\mathrm{Irr}(\alpha,\mathbb{F}_p)$ 即为 n 次不可约多项式. ♣

注意：这里不可约次数为 n 是因为其等于扩张次数 $[E:\mathbb{F}_p]$，可不是 p^n 哦！

命题 5.5.5: 对不可约多项式一个有趣的观察

任意 $m|n$，$f(x)\in\mathbb{F}_p[x]$ 为 m 次不可约多项式，则 $f(x)\mid x^{p^n}-x$.

证明 设 $K=\mathbb{F}_p[x]/(f(x))$，从而可知这是一个阶为 p^m 的域，从而由有限域结构定理，可知其也为 $x^{p^m}-x$ 的分裂域，从而任意 $\alpha\in K$，$\alpha^{p^m}-\alpha=0$，从而 $\alpha^{p^n}=\alpha$，也即任意 $\alpha\in K$，$\alpha^{p^n}-\alpha=0$，从而 $f(x)\mid x^{p^n}-x$，即证. ♣

现在，利用上述结论，我们可以给出 $x^{p^n}-x$ 的不可约分解：

定理 5.5.2: $x^{p^n}-x$ 的不可约分解

任意 $n\in\mathbb{N}$，记 $\Omega_n=\{f(x)\in\mathbb{F}_p[x]|f\text{不可约},\deg f\mid n\}$，则 $x^{p^n}-x=\prod\limits_{f\in\Omega_n}f(x)$.

证明 注意到若 f 不可约，且 $f|x^{p^n}-x$，从而由 $\mathbb{F}_p[x]/(f(x))$ 为 $E/\mathbb{F}_p$ 的中间域，从而 $\deg f\mid n$，结合上一个命题不难得到结果. ♣

例 5.5.1. 在 $\mathbb{F}_2[x]$ 上分解 x^8+x，注意 $x^8+x=x^{2^3}-x$，从而我们只需要找到 $\mathbb{F}_2[x]$ 上所有次数为 $1,3$ 的不可约多项式即可，事实上，简单的讨论即有，不超过 3 次的不可约多项式全体为 x，$x+1$，x^2+x+1，x^3+x^2+1，x^3+x+1，因此有 $x^8+x=x(x+1)(x^3+x^2+1)(x^3+x+1)$.

5.6 本原元

5.6.1 Notes

这一节与主线剧情关系并不大，可以先略去.

定理 5.6.1: 有限可分扩张都是单扩张

设 E/F 是有限可分扩张，则 E/F 是单代数扩张，即存在 $\alpha \in E$ 使得 $E = F(\alpha)$. 这样的 α 称为 E/F 的**本原元**.

5.7 根式扩张

5.7.1 Notes

定义 5.7.1: 根式扩张

考虑域扩张 E/F，称 $\alpha \in E$ 是一个n **次根**，若有 $\alpha^n \in F$，进一步称一个域扩张 E/F 为一个**根式扩张**，若存在一个根式扩张塔

$$E = E_s/\cdots/E_1/E_0 = F,$$

满足对任意 $0 \leq i \leq s-1$，存在 $n_i \in \mathbb{N}^*, \alpha_{i+1} \in E_{i+1}$，满足 $\alpha_{i+1}^{n_i} \in E_i$，且 $E_{i+1} = E_i(\alpha_{i+1})$.

一言以蔽之，根式扩张描述的就是不断去根号的过程，如扩张塔 $\mathbb{Q}(\sqrt{3+\sqrt{2}})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$，自然地，我们可以借助根式扩张来定义根式解：

定义 5.7.2: 根式解

设 $f(x) \in F[x]$，称 $f(x)$ **根式可解**，若存在 E/F 为根式扩张，且 f 在 E 上分裂.

那么对任意一个域，我们关心给定一个多项式 $f(x)$，是否根式可解？在讨论一般情形之前，我们先讨论一些特殊多项式，这会为我们带来一些心理上和技术上的准备：

- 分圆扩张：$x^n - 1$；
- 循环扩张：$x^n - a$；
- Kummer 扩张：$(x^n - a_1)\cdots(x^n - a_k)$.

分圆扩张

定义 5.7.3: 分圆扩张

设 E 是 $f(x) = x^n - 1 \in F[x]$ 的分裂域，称 $f(x)$ 的根为n **次单位根**，易见 E 中所有的 n 次单位根构成一个循环群，其中任何 n 阶元 θ_n 称为 n **次本原单位根**. 若 E 中有n 次本原单位根，则称 E/F 是n **次分圆扩张**，E 是一个n **次分圆域**.

注 1：E 中所有单位根构成循环群是可以直接验证的；

注 2：若存在 n 次本元单位根，才称为分圆扩张，换言之有些时候本原单位根不一定存在，为什么？不是都构成循环群了嘛，循环群的阶不是 n 嘛？这便要注意，虽然 f 是 n 次，但这不代表 f 无重根，自然循环群阶不超过 n，下面这个例子说明地更透彻一些.

例 5.7.1 (本原单位根不一定存在). 要想举出这样的例子，对特征为 0 的域是断然不行的，因为 x^n-1 必然没重根，从而对特征为 p 的域，我们有其含有 n 次本原单位根，当且仅当 $(n,p)=1$，从有无重根的角度看这是显然的，人生苦短，证明就略去啦.

我们上面给出了若干定义，下面要做的事就是研究它们，比如

命题 5.7.1: 本原单位根

θ_n^k 是本原单位根当且仅当 $(k,n)=1$，进而共有 $\varphi(n)$ 个.

证明 证明是群论的基本技术，不再赘述. ♣

命题 5.7.2: 分圆扩张

若 E/F 为 n 次分圆扩张，从而 E 为单扩张 $F(\theta_n)$，且 $x^n-1=(x-1)\cdots(x-\theta_n^{n-1})$.

现在设 $R_n:=\{\theta_n^k|(n,k)=1\}$ 为全体 n 次本原单位根，$R=(\theta_n)$ 为根集，一个基本的观察是分圆扩张是可分多项式 x^n-1 的分裂域，从而为 Galois 扩张，因此我们引入 Galois 群：

命题 5.7.3: 一些基本性质

任意 $\varphi\in\mathrm{Gal}(E/F)$，$\alpha\in R$，有 $\varphi(R)=R$，$o(\varphi(\alpha))=o(\alpha)$，进而 $\varphi(R_n)=R_n$.

利用 φ 在 R_n 上的保持性，我们不难有如下定义

定义 5.7.4: 分圆多项式

任意 $n\in\mathbb{N}$，$\mathrm{Ch}F\nmid n$，定义 n 阶**分圆多项式**为

$$\Psi(x)=\prod_{\theta\in R_n}(x-\theta)=\prod_{(k,n)=1}(x-\theta_n^k)\in F[x],$$

注意到系数在 F 中是通过 φ 在 R_n 上的保持性得到的，其次数为 $\varphi(n)$.

但是我们为什么要引入这么一个看起来奇怪的东西呢？注意到我们考虑 $\mathrm{Gal}(E/F)$ 的结构，一个基本的观察是其完全由 $\sigma(\theta_n)$ 确定，毕竟是单扩张嘛，即存在唯一的 $k\in\{0,1,\cdots,n-1\}$，且 $(k,n)=1$ 使得 $\sigma(\theta_n)=\theta_n^k$，从而若设 U_n 为 $\mathbb{Z}/n\mathbb{Z}$ 的乘法可逆元，则上述给出了一个 $\mathrm{Gal}(E/F)$ 到 U_n 的一个单同态！从而 $\mathrm{Gal}(E/F)$ 同构于 U_n 的一个子群. 但若 F 本身已包含 n 次单位根，E/F 的 Galois 群平凡，如 $F=\mathbb{C}$，其 4 次分圆域仍为 $\mathbb{C}$，因此不为 U_4.

那么何时，$\mathrm{Gal}(E/F)\cong U_n$ 呢？下面这个命题并不意外：

定理 5.7.1: $\mathrm{Gal}(E/F)\cong U_n$ 的充要条件

设 $E=F(\theta_n)$ 为 n 次分圆域，则 $[E:F]=\varphi(n)$等价于$\mathrm{Gal}(E/F)\cong U_n$等价于$\Psi_n(x)$ 是 F 上不可约多项式.

证明 我们只需要说明 (2) 推 (3) 即可，另外两个都是直接的，注意到 $\mathrm{Gal}(E/F)\cong U_n$ 当且仅当 $\mathrm{Gal}(E/F)$ 作用在 R_n 上是可递的，从而考虑 θ_n 的极小多项式 $p(x)$，不难说明 $p(x)$ 与 $\Psi_n(x)$ 相伴，从而可知其不可约. ♣

因此这个命题表明，研究 $\mathrm{Gal}(E/F)$ 的一个核心切入点就是看 $\Psi_n(x)$ 的可约性，但是先不说可不可约，我们甚至还不知道 $\Psi_n(x)$ 长什么样！好在我们有：

命题 5.7.4: 分圆多项式的递推

x^n-1 可以分解为

$$x^n-1=\prod_{d|n}\Psi_d(x),$$

特别地，若 p 为素数，则

$$\Psi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+\cdots+x+1,$$

进一步，我们可以得到分圆多项式的递推关系：

$$\Psi_n(x)=\frac{x^n-1}{\prod\limits_{d|n,d\neq n}\Psi_d(x)}.$$

证明 注意到 $\theta_d=\theta_n^{n/d}$ 即可，余下的不过是初等数论. ♣

为了研究 $\Psi_n(x)$ 的不可约性，我们先从最基本最熟悉的数域 $\mathbb{Q}$ 上考虑，此时有 $\Psi_1(x)=x-1$，$\Psi_2(x)=x+1$，$\Psi_3(x)=x^2+1+1$，$\Psi_4(x)=x^2+1$，惊讶地发现，它们虽然都在 $\mathbb{Q}$ 上，但是它们系数全为整系数，而且更重要的，无论 n 是何值，看起来 $\Psi_n(x)$ 都是不可约的！这确实是一个一般的结论：

定理 5.7.2: 有理数域上的分圆多项式

$\Psi_n(x)\in\mathbb{Z}[x]$ 且在 $\mathbb{Q}$ 上不可约，进而 $\mathrm{Gal}(\mathbb{Q}(\theta_n)/\mathbb{Q})\cong U_n$.

证明 人生苦短，接受它也不是什么难事对吧. ♣

熟知地，我们有如下结构定理 (利用中国剩余定理)

定理 5.7.3: 单位群的结构

设 $n = p_1^{k_1} \cdots p_t^{k_t}$，则 $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus \cdots \mathbb{Z}/p_t^{k_t}\mathbb{Z}$，且进一步有同时考虑其中可逆元，即 $U_n = U_{p_1^{k_1}} \oplus \cdots \oplus U_{p_t^{k_t}}$.

循环扩张

我们这一节在分圆扩张的基础上，考虑多项式 $x^n - a \in F[x]$，当然同之前的讨论一样，我们希望其可分，也即 $\mathrm{Ch}F \nmid n$，设 K/F 是其分裂域，借助我们在 $\mathbb{Q}$ 上的直觉，不难知道 $x^n - 1$ 应当也是在 K 上分裂的，并且 K 事实上是个二元扩张，形如 $\mathbb{Q}(\theta_n, \sqrt[n]{a})$.

事实上，记 $R = \{\alpha_1, \cdots, \alpha_n\}$ 为 $x^n - a$ 的根集，则注意到任意 i, j，有 $(\alpha_i \alpha_j^{-1})^n = aa^{-1} = 1$，因此 $\alpha_i \alpha_j^{-1}$ 为 $x^n - 1$ 的根，进而若记 $\varepsilon_j = \alpha_1 \alpha_j^{-1}$，则可知 $\varepsilon_1, \cdots, \varepsilon_n$ 互不相同，因此恰好构成 $x^n - 1$ 的根集，也即 $x^n - 1$ 在 K 上分裂.

注意到 $\mathrm{Ch}F \nmid n$，因此可知存在本原单位根 θ_n，设 $\alpha = \alpha_1 \in R$，则可知 $R = \{\alpha, \alpha\theta_n, \cdots, \alpha\theta_n^{n-1}\}$，因此我们确实有根式扩张塔 $K = F(\alpha, \theta_n)/F(\theta_n)/F$，这便阐明了我们从 $\mathbb{Q}$ 中收获的直觉.

鉴于在上一小节中，我们已经研究清楚 $F(\theta_n)/F$ 的相关结构了，便没必要重走老路了，于是下面的重心落在研究 $K/F(\theta_n)$ 上：

定理 5.7.4: $K/F(\theta_n)$ 的结构

对 $\mathrm{Ch}F \nmid n$，我们有 $\mathrm{Gal}(K/F(\theta_n))$ 为循环群，且 $|\mathrm{Gal}(K/F(\theta_n))| \mid n$，进一步当且仅当 $x^n - a \in F(\theta_n)[x]$ 不可约时，才有 $|\mathrm{Gal}(K/F(\theta_n))| = n$.

证明 任取 $\varphi \in \mathrm{Gal}(K/F(\theta_n))$，则可知 φ 完全由 α 的像决定，不妨设 $\varphi(\alpha) = \theta_n^k \alpha$，则有 $\varphi(\theta_n^j) = \theta_n^{j+k}\alpha$，这自然产生了一个群同态 $\Theta : \mathrm{Gal}(K/F(\theta_n)) \to S_n$，满足 $\Theta(\varphi) = (1 \cdots n)^k$，从而可知 $\mathrm{Gal}(K/F(\theta_n))$ 同构于由 $(1 \cdots n)$ 生成的 S_n 的循环子群的一个子群，因此即可知命题前半部分成立. 另一方面，我们知道 $x^n - a$ 不可约当且仅当其根集在 $\mathrm{Gal}(K/F(\theta_n))$ 作用下时可递的，因此不难知道后半部分也成立. ♣

但是研究 $x^n - a$ 在 $F(\theta_n)$ 的不可约性比较复杂，我们只能以一个浅显的特殊情况给出一些讨论，如 $n = q$ 是一个不同于 $\mathrm{Ch}F$ 的素数，我们有如下结果：

命题 5.7.5: 一个特例

考虑 $x^q - a \in F[x]$，则

1. $x^q - a$ 或者在 F 中有根，或者压根就不可约；
2. 若 $x^q - a$ 在 F 上有根，则其直接在 F 上分裂当且仅当 F 包含 θ_q.

证明 有兴趣的时候再补上罢. ♣

注意到在 $K/F(\theta_n)$ 中，一个显著特征是其 Galois 群为循环群，因此这类比较简单的域扩张也十分值得讨论一下，为此我们给出一个定义：

定义 5.7.5: 循环扩张

一个有限 Galois 扩张 E/F 为一个**循环扩张**，若其 Galois 群为循环群.

例 5.7.2 (循环扩张的例子)**.** 想举出循环扩张的例子，自然会想以 $\mathbb{Q}$ 为地基，一个自然的想法便是 $\mathbb{Q}(\sqrt[n]{2})$，看着就像 n 次扩张，但是仔细

5.8 可解群与根式可解

5.8.1 Notes

在这一节中，我们终于可以完全回答方程可否根式解的问题，即证明五次以上方程没有根式解，如果非要一言以蔽之，那么关键便是在说明当 $n \geq 5$ 时，A_n 不是可解群，下面我们先回忆一下可解群的相关性质：

定义 5.8.1: 可解群

设 G 为群，定义 $G^{(1)} = [G,G] = \langle [a,b] | a,b \in G \rangle$，也即为 G 的换位子群，进一步可以归纳定义 $G^{(k)} := [G^{(k-1)}, G^{(k-1)}]$，因此我们称 G 为一个**可解群**，若存在 $k \in \mathbb{N}^*$，满足 $G^{(k)} = \{e\}$.

一些基本的观察是：

命题 5.8.1: 可解群的基本性质

对任意群 G，有 $[G,G] \lhd G$，且 $G/[G,G]$ 为 Abel 群.

现在先让我们形式上的澄清一些观念，如为什么要如此引入可解群的概念？它又与根式可解有什么关系？注意到一个方程根式可解，那么它势必会形如嵌套根号的形式，而我们因此引入了根式扩张塔 $E = E_0/E_1/E_2/\cdots/E_k = F$，来反应不断消去根号的过程，与此对应的，我们如果考虑在这个过程中的 Galois 群变化，不难发现其与可解群 $G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \cdots \rhd G^{(k)} = \{e\}$ 有着大体类似的结构！

因此借助这个观察，方程有无根式解，就是说能否有限次将根号全部去掉，这无疑对应着 Galois 群是否能够最终可解，这是 Galois 一一对应所保证的.

有时候，更便捷的我们会选择如下方式去定义可解群：

定义 5.8.2: 可解群的等价定义

我们称 G 的一个子群列为**次正规子群列**，如果有 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_k = \{e\}$，因此称一个子群 G 为可解群，若存在其一个次正规子群有限列，且满足对任意 $1 \leq i \leq k$，G_{i-1}/G_i 为 Abel 群.

例 5.8.1 (A_3, A_4 是可解群). 注意到 $[S_n : A_n] = 2$，从而 A_n 总为 S_n 的正规子群，当 $n = 3$ 时，我们由 $A_3 = \mathbb{Z}_3$，为 *Abel* 群，因此有 $\{e\} \lhd A_3 \lhd S_3$，不难验证相邻商群为 *Abel* 群，这便表明 S_3 和 A_3 都是可解群.

当 $n = 4$ 时，考虑 A_4 的四元正规子群 *Klein* 群 K，则 $A_4/K = \mathbb{Z}_3$，从而也为 *Abel* 群，再考虑 K 的换位子群 $L = \{\mathrm{id}, (12)(34)\}$，从而不难有次正规序列 $\{e\} \lhd L \lhd K \lhd A_4 \lhd S_4$，也即

可知 S_4 和 A_4 都是可解群.

事实上，Burnside 很早就有，任意 $|G|<120$，且 $|G|\neq 60$，则 G 为可解群.

利用一些高超的群论技术，我们有

定理 5.8.1: 根式可解理论的核心技术

对任意 $n\geq 5$，A_n 不是可解群.

以及有：

定理 5.8.2: 可解群的进一步性质

1. 可解群的任意子群也是可解群；
2. 设 $H\lhd G$，则 G 可解当且仅当 H 可解且 G/H 可解.

证明 留给来者. ♣

定理 5.8.3: 判别是否可解

任取 $f(x)\in F[x]$，若 f 的 Galois 群 G_f 可解，且 $\mathrm{Ch}F\nmid |G_f(F)|$，则 f 有根式解.

5.9 Galois 覆盖

6 抽象代数结论拾遗

6.1 群论

命题 6.1.1

素数阶群一定为 Abel 群.

证明 不难证明素数 p 阶群一定同构于 $\mathbb{Z}_p$，从而为 Abel 群. ♣

命题 6.1.2

非 Abel 群的最小阶数为 6.

证明 由命题6.1，可知 $2,3,5$ 阶群均为 Abel 群，且 1 阶群显然，而对 4 阶群 G，若其有元素 g 阶为 4，则 $G=\{e,g,g^2,g^3\}$，显然为 Abel 群，若不然，则群中元素阶为 2，熟知这意味着其为 Abel 群，事实上，这两种群即 $\mathbb{Z}_4$ 与 K_4.

而对 6 阶群，不难发现 S_3 即不为 Abel 群，从而证明了命题. ♣

定义 6.1.1: 正规化子、中心化子

M 是群 G 的子集，则定义

$$N_G(M)=\{g\in G|gMg^{-1}=M\},$$

从而不难发现 $N_G(M)<G$，并称其为 M 的**正规化子**. 进一步，定义

$$C_G(M)=\{g\in G|gmg^{-1}=m,\forall m\in M\},$$

从而也不难发现 $C_G(M)\lhd N_G(M)$，进而 $C_G(M)<G$，并称其为 M 的**中心化子**.

Remark. 正规化子刻画了子集 M 的正规性，特别地当 $M<G, N_G(M)=G$，则 $M\lhd G$；中心 $C_G(G)=C(G)$ 刻画了 G 的交换性.

命题 6.1.3: 素数幂次阶群的特性 (1)

设 p 为素数，G 为 p^n 阶群，则 $|C(G)|>1$，即存在非平凡 (不为 e) 的中心元素.

证明 我们在前面的习题里已经证明了对一个子群 M，其共轭子集的个数为 $[G:N_G(M)]$，从而我们定义等价关系：$a\mathrm{R}b$ 当且仅当存在 $g\in G$ 使得 $b=gag^{-1}$，即按共轭关系进行划分，从而易见若 $a\in C(G)$，则 a 所在的共轭类仅有 a，而对其它共轭类有其元素个数为 $[G:C_G(b)]=p^k$，从而可知设 $|C(G)|=r$，则由 $G=\bigcup C(G)\bigcup\limits_{b\notin C(G)}C_G(b)$，从而我们有 $p^n=r+p^{i_1}+\cdots+p^{i_l}$，

从而可知 $p|r$，又 $r\geq 1$，从而非平凡的中心元素至少有 $p-1$ 个. ♣

Remark. 这个特性表明了，素数幂次阶群中至少有 p 个元素与所有元素可交换. 且这个证明也再次体现了利用等价关系进行划分，从而搭起元素与个数桥梁的技巧的重要性.

命题 6.1.4: 素数幂次阶群的特性 (2)

对每个素数 p，p^2 阶群 G 均为 Abel 群.

证明 若 G 中存在元素阶为 p^2，则可知 $G=\{1,g,\cdots,g^{p^2}\}\cong\mathbb{Z}_{p^2}$，从而为 Abel 群；

若 G 中不存在元素阶为 p^2，从而除幺元外，每个元素阶均为 p，从而由 $C(G)\geq p$，从而取 $a\in C(G)$，且 $a\neq e$，则 a 的阶为 p，取 $b\notin e,a,\cdots,a^{p-1}$，则有 $ab=ba$，从而任意 m,n,k,l，若 $a^mb^n=a^kb^l$ 则 $(m,n)=(k,l)$，从而 $G=\langle a,b\rangle$，即为 Abel 群. ♣

命题 6.1.5

设 A，B 是有限阶群 G 的两个非空子集，若

$$|A|+|B|>|G|,$$

证明：$G=AB$.

证明 一方面，不难看到 $AB\subseteq G$，另一方面，任意 $g\in G$，考虑 gA^{-1}，易见 $|A^{-1}g|=|A|$，从而 $|A^{-1}g|+|B|>|G|$，故 $A^{-1}g\cap B\neq\varnothing$，从而存在 $a\in A,b\in B$ 使得 $a^{-1}g=b$，即有 $g=ab\in AB$，故 $G\subseteq AB$，综上 $G=AB$. ♣

Remark. 糅合这个题和上一题，我们可以编出这个问题：

例 6.1.1. *设 G 为 2126 阶群，A,B 分别为 G 的 2022，105 阶子集，证明：$AB=BA$.*

命题 6.1.6: 一道坑题

证明：若群 G 满足其自同构群 $\mathrm{Aut}(G)$ 为循环群，则 G 为 Abel 群.

证明 $\mathrm{Aut}(G)$ 循环群这个条件过于抽象了，我们用弱一点的，我们有 $\mathrm{Inn}(G)<\mathrm{Aut}(G)$ 为循环群，从而我们熟知 $\mathrm{Inn}(G)\cong G/\mathrm{Ker}\ \mathrm{Ad}=G/C(G)$，从而可设 $N=C(G)$，则 G/N 为循环群，从而设其生成元为 aN，从而任意 $g,h\in G$，设 $g=a^sn_1$，$h=a^tn_2$，从而 $n_1,n_2\in N=C(G)$，因此其与任一元素均可交换，则有

$$gh=a^sn_1a^tn_2=a^tn_2a^sn_1=hg,$$

因为上述四个元素是两两可交换的，因此可知 G 为 Abel 群. ♣

7 高等代数难点回顾

7.1 一道选拔考试题的探讨

命题 7.1.1: 2021 伯苓选拔高代试题

设 $\boldsymbol{A}\in M_n(\mathbb{R})$，且 $\boldsymbol{A}^2=-\boldsymbol{I}_n$，若 $\boldsymbol{AB}=\boldsymbol{BA}$，证明：$\det(\boldsymbol{B})\geq 0$.

本题有两种解法，分别表现了对 $\boldsymbol{A}$ 标准型的两种理解与刻画，证法 1 是从类似于虚数单位的角度出发的，来自车车 dalao：

证明 由 $\boldsymbol{A}$ 为实矩阵，且特征值为 $\pm\mathrm{i}$，从而可知 $\boldsymbol{A}$ 的特征多项式为 $(\lambda^2+1)^m$，其中 $n=2m$，则可知 $\boldsymbol{A}$ 在 $\mathbb{C}$ 上的 Jordan 标准型为 $\boldsymbol{J}=\begin{pmatrix}\mathrm{i}\boldsymbol{I}_m & \\ & -\mathrm{i}\boldsymbol{I}_m\end{pmatrix}$(注意 $\boldsymbol{A}$ 可对角化).

而又不难发现矩阵 $\boldsymbol{I}=\begin{pmatrix} & \boldsymbol{I}_m \\ -\boldsymbol{I}_m & \end{pmatrix}$ 的 Jordan 标准型也为 $\boldsymbol{J}$，从而可知 $\boldsymbol{A}$ 相似于 $\boldsymbol{I}$，从而替换可得 $\boldsymbol{IB}=\boldsymbol{BI}$，则写成分块对角阵可得 $\boldsymbol{B}=\begin{pmatrix}\boldsymbol{B}_1 & \boldsymbol{B}_2\\ -\boldsymbol{B}_2 & \boldsymbol{B}_1\end{pmatrix}$，则有

$$\begin{vmatrix}\boldsymbol{B}_1 & \boldsymbol{B}_2\\ -\boldsymbol{B}_2 & \boldsymbol{B}_1\end{vmatrix}=\begin{vmatrix}\boldsymbol{B}_1 & \boldsymbol{B}_2\\ -\boldsymbol{B}_2+\mathrm{i}\boldsymbol{B}_1 & \boldsymbol{B}_1+\mathrm{i}\boldsymbol{B}_2\end{vmatrix}=\begin{vmatrix}\boldsymbol{B}_1-\mathrm{i}\boldsymbol{B}_2 & \boldsymbol{B}_2\\ \boldsymbol{O} & \boldsymbol{B}_1+\mathrm{i}\boldsymbol{B}_2\end{vmatrix}=|\boldsymbol{B}_1-\mathrm{i}\boldsymbol{B}_2||\boldsymbol{B}_1+\mathrm{i}\boldsymbol{B}_2|\geq 0$$

从而我们完成了证明. ♣