写在前面：

- 题目来源为书院的代数I II作业以及书院的博资考题、北京大学代数学I实验班的考试题。
- 提示是经本人检验后能完成证明的，但不排除伪证使得提示失效的可能，且提示不代表最简洁的方法。
- 题目排列顺序与难度完全无关。
- 题目不排除出现typo的可能，如果发现了typo，请联系助教处理。

1 群论

问题 1. 对于群G，$a,b\in G$，假如有$a^5=e$，$a^3b=ba^3$，求证$ab=ba$。

提示：从$ab=aeb$开始算起，并利用$a^5=e$。

问题 2. *1.* 对于有限群G，$H\subset G$是真子群，请证明

$$G\neq\bigcup_{g\in G}gHg^{-1}$$

如果是无限群，这个结果还正确吗？

提示*:* 对有限群的情况，可以证明$|G|\neq|\bigcup_{g\in G}gHg^{-1}|$

2. 对于有限群G，其传递地作用在有n个元素的有限集X上，其中$n>1$，请证明存在$g\in G$使得其在X上没有不动点。

提示：考虑$X=\{g_1x,...,g_nx\}$并考虑$Stab(g_ix)$。

问题 3. 记$[n]=\{1,2,...,n\}$，请证明S_6不能传递地作用在$[7]$上。S_7能否传递地作用在$[8]$上呢？

提示：如下两个事实对证明有帮助：

- S_7的非平凡正规子群只有A_7
- $Aut(S_8)=Inn(S_8)$

问题 4. 定义$PGL(2;\mathbb{F}_3)=GL(2,\mathbb{F}_3)/D$，其中$D=\{\lambda I_2|\lambda\in\mathbb{F}_5^\times\}$，请证明$PGL(2,\mathbb{F}_3)\cong S_4$

提示：可以考虑$GL(2,\mathbb{F}_3)$在$(\mathbb{F}_3)^2$的所有一维子空间组成的集合上的作用。

问题 5. 令G是一个群，而$\mathbb{R}^\times$是$\mathbb{R}$中非零元素在域的乘法下组成的群，考虑$G \to \mathbb{R}$的所有映射构成的线性空间V。假设S是由有限个$G \to \mathbb{R}^\times$的群同态组成的集合，请证明S中的元素在V上线性无关。

提示：可以参考课程讲义引理*123*。

问题 6. 证明有限群G是循环群当且仅当对于任意正整数n，G至多只有一个阶数为n的子群。

提示*:* 对于$d||G|$，找一个阶为d的元素，并考虑其生成的循环群，其中有$\varphi(d)$个阶为d的元素。然后利用数论中的恒等式$\sum_{d|n}\varphi(d) = n$。

问题 7 (书院2023秋博资考)**.** 证明如果群G有有限指数的子群，那么G有有限指数的正规子群。

提示：可以先证明如果群G有两个有限指数的子群H和K，那么$H \cap K$也是G的有限指数子群。

问题 8. 请证明$GL(n, \mathbb{C})$没有有限指数的真子群。

提示：通过*Jordan*标准型证明如下的事实，然后使用上一个题目：对于每一个矩阵$M \in GL_n(\mathbb{C})$，以及任意正整数m，都存在$N \in GL(\mathbb{C})$使得$N^m = M$

问题 9. 对于$G = SL_2(\mathbb{Z})$，如果$A \in G$是有限阶的元素，那么A的阶可能为什么？

提示：如果$A \in G$是有限阶的，那么A的特征值一定是单位根，且必定形如$\zeta, \bar{\zeta}$，然后考虑$SL_2(\mathbb{Z})$中的矩阵的迹一定是整数。

问题 10. 设G是一个群，A, B是G的两个非空子集，若$|A| + |B| > |G|$,请证明$G = AB$。

提示：考虑集合$\{a^{-1}g|a \in A\}$，其中有$|A|$个元素，所以至少有一个元素在B中*(*由于$|B|$的元素个数*)*。

问题 11. 假设G是一个p-群，S是一个具有G-群作用的有限集合，记

$$S^G := \{s \in S : gs = s,\ \forall g \in G\}$$

证明$|S^G| \equiv |S|(mod\ p)$

提示：使用公式$|S| = |S^G| + \sum_{s \in S}[G : C(s)]$，其中$C(s) = \{g \in G;\ gs = s\}$

问题 12. 对于有限群G，假设p是$|G|$的最小素因子，H是G的指数p的子群，证明H是G的正规子群。

注记：请回顾对于$p = 2$的情形，命题为指数为2的子群一定为正规子群。

提示：考虑G在$\{gH|\ g \in G\}$*(*即H的左陪集*)*上的作用,这诱导了$G \to S_p$且核包含H，去证明H与这个同态的核一致，据此说明H是正规的。

问题 13. 请分类$SU(2)$之有限子群。

提示：可以查阅资料，去证明存在一个2 : 1的覆叠$SU(2) \to SO(3)$(这个覆叠具体是什么？)利用这个覆叠和课堂上证明的$SO(3)$之有限子群的结构来给出$SU(2)$之有限子群。

问题 14 (书院2025春博资考模拟). 假设G是一个非交换群，那么$Aut(G)$一定不是循环群。

提示：利用$Inn(G) \cong G/Z(G)$，并且证明G交换当且仅当$G/Z(G)$平凡。

问题 15 (北大代数学I实验班2024期末). 假设G是一个阶为$2^m k$的群，此处k为奇数且m为正整数，假设G包含一个阶恰为2^m的元素g，请证明G包含一个元素恰为k的子群。

提示：首先考虑左乘x，其定义了一个G中的元素置换$\pi_x : G \to G$，先证明π_g为奇置换，然后据此说明使得π_h为偶置换的全部$h \in G$构成一个群H，且H的元素恰有$2^{m-1}k$个，并且存在一个阶恰为2^{m-1}的元素，据此说明G包含一个元素个数为k的子群。

问题 16 (北大代数学I实验班2024期末). 假设G是一个有限群，固定$|G|$的一个素因子p，记$K = \cap N_G(P)$，其中相交取遍G的全体$Sylow\text{-}p$子群P，$N_G(-)$为其正规化子，证明：

1. K是G的正规子群。
2. G和G/K的$Sylow\text{-}p$ 子群数量一样。

提示：第一问直接使用正规子群的定义检验即可。第二问：对于G的$Sylow$-子群Q，考虑其在$\overline{G} = G/K$中的像$\overline{Q} = Q/(Q \cap K)$定义$N = N_G(Q)$为其正规化子，同理定义$N_{\overline{Q}}(\overline{Q})$，根据$Sylow$定理只用证明$|G/N| = |\overline{G}/N_{\overline{G}}(\overline{Q})|$,这是由于$\overline{N} = N_{\overline{G}}(\overline{Q})$,而这一点可以通过互相包含来证明，这也就说明了$Sylow$子群个数相同。

问题 17 (书院2024秋博资考). 请指出最小的有限单群，并证明你的结论。

提示:这个群为A_5，先证明A_5是单群(可以通过A_5之共轭类给出)，然后证明任何小于60阶群都不是单群，对于pq,p^2以及p^3阶群，可以直接使用结论。而对于其他情况，先写出其$Sylow\text{-}p$子群的可能数量，如果为1即无需证明，而当$Sylow$子群数量过多时，可以通过证明元素个数太多给出矛盾，$Sylow$子群数量太少时，通过$G \to S_k$是单射给出矛盾(其中S_k)为这k个$Sylow$子群的置换群，而根据$Sylow$定理,G共轭作用在$Sylow\text{-}p$子群上的作用是传递的。

问题 18 (书院2025 4月新领军). 请计数$GL_3(\mathbb{F}_5)$ 中满足$A^2 = I$的个数。

提示：注意到其$Jordan$标准型(使用PID上的$Jordan$标准型定理)必为对角阵，且特征值为1或者4，然后使用轨道—稳定化子公式计算每种情况下的元素个数即可。

问题 19 (蝴蝶引理/Zassenhaus引理). 假设G是一个群，$N_1 \subset H_1$,$N_2 \subset H_2$是G的子群，且N_1, N_2分别为H_1, H_2的正规子群，那么$N_1(H_1 \cap N_2)$和$N_2(N_1 \cap H_2)$分别是$N_1(H_1 \cap$

H_2)和$N_2(H_2 \cap H_1)$的正规子群，并且存在典范的群同构：

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \cong \frac{N_2(H_1 \cap H_2)}{N_2(N_1 \cap H_2)}$$

提示：先证明$H_1 \cap N_2$在$H_1 \cap H_2$中正规，再证明$N_1(H_1 \cap N_2)$在$N_1(H_1 \cap H_2)$中正规。为证明存在典范同构，我们只需要证明

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \cong \frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)} \cong \frac{N_2(H_1 \cap H_2)}{N_2(N_1 \cap H_2)}$$

问题 20. 本题我们研究群的自由积。如果两个群G和H分别写成生成元和关系

$$G = \langle X|R\rangle, \quad H = \langle Y|S\rangle$$

那么G和H的自由积定义为$G * H = \langle X \sqcup Y|R \sqcup S\rangle$。

1. 证明*Ping-Pong* 引理：假设G有两个阶数不全为2的子群H_1和H_2且H_1,H_2生成群G，假设群G在集合A上有作用，且存在A的两个不相交的非空子集A_1,A_2使得$\forall h_1 \in H_1\backslash\{e\}$, $h_1(A_2) \subset A_1$, $\forall h_2 \subset H_2\backslash\{e\}$, $h_2(A_1) \subset A_2$，那么G同构于$H_1 * H_2$

2. 请证明$SL(2,\mathbb{R})$中由矩阵$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$和$\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$生成的子群同构于这两个生成元的自由群。
提示：考虑$\mathbb{R}^2$中的子集$\{(x,y)|\ |x| < |y|\}$以及$\{(x,y)\ |y| < |x|\}$

3. 请证明$PSL(2,\mathbb{Z}) \cong C_3 * C_2$，其中$C_n$为$n$阶循环群。
提示：考虑元素$M_3 = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$和$M_4 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$并考虑$PSL(2,\mathbb{Z})$在$\mathbb{R}^2$中所有过原点的直线的集合上的作用，并分成斜率$\leq 0$的部分以及其他。

问题 21. 我们令$G_1 = G/C(G)$，且$G_{n+1} = G_n/C(G_n)$，如果存在m使得G_m为平凡群，那么称G是幂零群。请回答下面的关于幂零群的问题。

1. 请证明p-群一定是幂零群。

2. 请证明有限群是幂零群当且仅当它是其$Sylow$子群之直积。

3. 如果G是一个幂零群，那么G的子群和商群也是幂零群。

4. 有限群G是幂零群当且仅当它同构于U的某一个子群，其中U为$\mathbb{F}$上对角线为1的$n \times n$上三角矩阵构成的群。

5. 如果G幂零，并且$[G,G] = G$，那么G是平凡群。

提示：

1. 请证明p-群的中心非平凡，然后使用归纳法。
2. 请证明幂零群的任意p-sylow子群至多只有一个。这是因为如果有$k>1$个，可以证明对于每一个$G_{i+1}=G_i/C(G_i)$，其都有不少于k个p-sylow子群，与幂零矛盾。
3. 可以参考任何一本讲解幂零群的教材。
4. 请先对p-群证明，将p-群G视为S_n的子群，再视为$GL_n(\mathbb{F}_p)$的子群，然后使用本题的(2)证明对所有的有限群均成立。为证明U之子群全部幂零，只需要证明U幂零，U的$C(U_i)$是什么呢？可以具体计算出。
5. 请证明如下引理:如果$[G,G]=G$，那么$[G/C(G),G/C(G)]=G/C(G)$

问题 22. 请计算$GL(n,\mathbb{F})$的导出子群。

问题 23 (北大代数学I实验班2021期中)**.** 设$K\subset H$为群G之子群且满足K为H之正规子群。

1. 请证明H在共轭作用下保持$C_G(K)$不动，其中$C_G(K)$代表了K在G中的中心化子。
2. 假设H也是G的正规子群,且$C_H(K)=1$，请证明H与$C_G(K)$交换。

提示：第一问使用定义即可，第二问去证明$hch^{-1}c^{-1}\in C_H(K)=1$即可，证明此的方法为利用公式$H\cap C_G(K)=C_H(K)$

问题 24 (北大代数学I实验班2021期中)**.** 假设G是一个有限群，$Syl_p(G)$为其$Sylow\ p$-子群之集合。

1. 如果S,T是$Syl_p(G)$中的不同元素且使得$|S\cap T|$(代表$S\cap T$的元素个数)取得最大值，请证明$N_G(S\cap T)$没有正规的$Sylow$-p子群。
2. 证明：对于任意的$S,T\in Syl_p(G)(S\neq T)$，$S\cap T=1$成立当且仅当对于G的任一非平凡p-子群p，$N_G(P)$包含一个正规$Sylow$-p子群。

提示：

1. 只需要证明$N_G(S\cap T)$中不止一个$Sylow$-p子群，我们假设$S'=N_S(S\cap T)$以及$T'=N_T(S\cap T)$,证明核心是证明它们是$N_G(S\cap T)$的$Sylow$-p子群，这一步可以使用反证法，用到的核心结果是对于p群S中的任何真子群，其在S中的正规化子必然严格大于它自己(请思考这是为什么！)然后补充证明$S'\neq T'$即可。

2. 对于充分性，用第一问的结论+反证法，假设存在非平凡的交集，选出一个阶最大的交集，记为$P = S_0 \cap T_0$且$S_0 \neq T_0$，然后考虑$N_G(S_0 \cap T_0)$即和第一问导出矛盾。对于必要性，则按照如下的思路一步步证明

   任何的非单位p-子群P都只属于唯一一个$Sylow\ p$-子群。

   证明$N_G(P) \subset N_G(S_P)$

   证明$N_G(P)$有唯一一个$Sylow$-p子群。

问题 25 (北大代数学I实验班2022期中). 如果群G的中心是平凡的，那么它的自同构群$Aut(G)$的中心也是平凡的。

提示：请考虑$Aut(G)$中的元素$Ad_g : h \to ghg^{-1}$然后去证明与这些交换的自同构ψ只能为$\psi = id$

问题 26 (北大代数学I实验班2022期中). 这是一个双传递的非平凡例子，假设$G = GL_2(\mathbb{F}_p)$

1. 给出一个G的$Sylow$-p子群，并且计算它的正规化子。

2. 证明G有$p+1$个不同的$Sylow$-p子群。

3. 证明G在所有$Sylow$-p子群构成的集合X上的作用是双传递的。

提示：具体举例可以考虑对角线为1的上三角矩阵构成的群N，然后通过$G/N_G(N)$计算不同的$Sylow$-p子群的个数。

为了证明双传递性(这是说G作用在$X \times X - \Delta$上是传递的，其中$\Delta \subset X \times X$是对角线元素)，考虑$(N, N^{op})$，其中$N^{op}$代表了对角线为1的下三角矩阵。考虑$(N, N^{op})$的稳定化子 $N_G(N) \cap N_G(N^{op})$，然后考虑含有$(N_G(N), N_G(N^{op}))$之轨道，计算元素个数即可。

问题 27 (北大代数学I实验班2022期中). 假设群G在集合X(可能是无限集)上作用，H是群G中指数有限的子群。对$x \in X$,用H_x和G_x表示群H和G在x处的稳定子群。证明：

1. H在X上有有限个轨道。

2. 如果群H在X上的作用是传递的，且对于某个$x \in X$有$H_x = G_x$，那么$H = G$。

3. 假如H正规，那么$[G_x : H_x]$(不管有限与否)不依赖于x之选择。

提示：

1. 直接将G写成陪集分解的形式$G = Hg_1 \sqcup Hg_2 \sqcup ... \sqcup Hg_r$，其中$g_1, g_2, ..., g_r \in G$

2. 使用反证法，假如$g_2 \notin H$, 考虑$g_2 x \in X$，其必然形如$hx = g_2 x$，于是$x = h^{-1} g_2 x$，据此说明$g_2 \in H$得出矛盾。

3. 去证明对于 $x' = gx$其中$g \in G$，那么$G'_x = gG_xg^{-1}$ 而且$H_{x'} = gH_xg^{-1}$，据此说明$[G_x : H_x] = [G_{x'} : H_{x'}]$

问题 28 (北大代数学I实验班2022期中). 请证明阶为*175*的群一定是交换群，然后给出所有互不同构的阶为*175*的群。

提示：去证明*Sylow 5*-子群和*Sylow 7*-子群都只有*1*个，据此说明正规性；然后再说明*Sylow 5*-子群也一定交换。

问题 29 (北大代数学I实验班2023期中). 请证明阶为*1947*的群一定是循环群。

提示：注意到$1947 = 3 \cdot 11 \cdot 59$，首先*Sylow-59*群$P_{59}$一定是一个正规子群，然后考虑共轭作用

$$\varphi : G \to \mathrm{Aut}(P_{59}) \cong \mathbb{Z}_{58}$$

据此说明$P_{59} \subset Z(G)$, 然后说明*Sylow-3*子群和*Sylow-11*子群都是唯一的。

问题 30 (北大代数学I实验班2023期中). 下面的习题是为证明一个看起来很显然的结果：$Aut(D_8) \cong D_8$，其中D_8代表了阶为*8*的二面体群。

1. 请证明$\#Aut(D_8) \leq 8$
2. 请证明D_8是D_{16}的正规子群，这里将D_8中的旋转元视为D_16中旋转元的平方。
3. 完成$Aut(D_8) \cong D_8$的证明。

提示：

1. 去证明对于D_8的任一自同构φ，$\varphi(r)$至多有两个选择，$\varphi(s)$至多有四个选择，其中r代表了旋转元，而s是反射元。
2. 直接验证可知。
3. 考虑共轭作用：$\varphi : D_{16} \to Aut(D_8)$，计算其核$Ker(\varphi) = \{1, r^4\}$，然后使用第一同构定理。

问题 31 (北大代数学I实验班2023期中). 对于素数p，假设G是一个p-群，假设A是一个G中的极大交换正规群。请证明A是G中的极大交换群。

提示：使用反证法，假设存在交换子群A'使得$A \subsetneq A' \subset G$且$A'$是交换群，令$H$为所有$gA'g^{-1}(g \in G)$生成的子群。注意到$H$中心化$A$，考虑投影映射$\pi : G \to \overline{G} = G/A$，并令$\overline{H} = \pi(H)$，利用有限$p$-的非平凡正规子群与中心的交非平凡，选出$\overline{n} \in \overline{H} \cap Z(\overline{G})$且$\overline{n} \neq 1$，然后令$N = \langle A, n \rangle$，其中$n$为$\overline{n}$之原像，去证明$N$是我们想要的目标。

问题 32 (北大代数学I实验班2021期末). 假设群G由两个元素生成，证明G至多有13个指数为3的子群。

提示：考虑G的指数为3的子群H，它诱导陪集分解$G = H \sqcup aH \sqcup bH$，于是得到两个$G$到$S_3$的同态(分别将$aH$视为$2$或者$3$)，且他们共轭。去说明存在如下的集合单射

$$\{G\text{的指数为}3\text{的子群}\} \hookrightarrow \{G\text{到}S_3\text{的同态}\}/\text{共轭}$$

于是只用说明这样的同态不超过13个，这是因为对于生成元$x, y \in G$，同态φ会被$\varphi(x)$和$\varphi(y)$所完全决定，而计算可能的对$(\varphi(x), \varphi(y)$的数量即可得到想要的结果。

注记：原题中还有一问是证明至多17，证明依旧是考虑G到置换群S_3的同态，但分析不用这么仔细，并且存在这样的群G使得G恰有13个指数为3的子群。

问题 33 (北大代数学I实验班2022期末). 令G是一个有限群，K是其正规子群，P是K的一个*Sylow-p*子群(p为素数)，试证明$G = KN_G(P)$

提示：去证明对于任一$g \in G$，总存在一个$k \in K$使得$k^{-1}g \in N_G(P)$，而这是通过$k^{-1}gPg^{-1}k = P$来说明的。

问题 34. $G = \mathrm{SL}_3(\mathbb{F}_p)$，其中$p$是一个奇素数，其中$l$是$p^2 + p + 1$的一个素因子。

1. 假设$l > 3$，证明l-*sylow*子群都是循环群。
2. 假设$l = 3$，证明l-*sylow*子群不是循环群。

提示：

1. 首先l-*sylow*子群的阶数是l^k，其中$k = \mathrm{ord}_l(p^2 + p + 1)$，然后通过域扩张$\mathbb{F}_{p^3}/\mathbb{F}_p$的范数映射构造一个阶为$p^2 + p + 1$的循环群，其为$\mathbb{F}_{p^3}^\times$的子群，通过其生成元$\gamma$的极小多项式的友阵(*Companion matrix*)构造这个循环子群到G的嵌入映射，最后利用*Sylow*子群之间互相共轭的结论。
2. 此时$p \equiv 1 (\mathrm{mod}\, 3)$，于是$3|p-1$，因此考虑$\omega \in \mathbb{F}_p^\times$且$\omega^3 = 1$,$\omega \neq 1$，通过考虑对角元为$\omega, \omega^{-1}, 1$的两个不同矩阵$A, B$，考虑它们生成的群，得到一个非循环的$3$-自群，即可得到矛盾。

问题 35. 假设G是一个*Abel*群，其由n个元素生成，证明G的每个子群也可以被至多n个元素生成。

提示：使用有限生成*Abel*群的结构定理。

问题 36. 证明每个有限群都同构于某个交错群A_n的子群。

提示：类比*Cayley*定理的证明，但这里是通过G作用在$X \times \{1, 2\}$上，而且G中的元素保持$1, 2$不变。

问题 37. 令G为一有限群，p为一素数，假设H是G的某个*Sylow-p*子群的一个子群，若$f(H)$记录包含H的*Sylow-p*子群的数量，证明$f(H) \equiv 1 \pmod{p}$。

提示：令H通过共轭作用在集合$\mathcal{S} = \mathrm{Syl}_p(G)$上，令$\mathcal{F}$为不动点集合，其元素个数$|\mathcal{F}| \equiv 1 \pmod{p}$，然后再考虑$\mathcal{C}$为满足条件的子群构成的集合，通过考虑$H$共轭作用在$\mathcal{C}$上来说明$|\mathcal{C}| \equiv |\mathcal{F}| \pmod{p}$

2 交换环论与模论

这一部分的环没有特殊声明的情况下均是交换的。

问题 38. 请确定下面环同态的同态核*:*

$$\mathbb{Z}[x] \to \mathbb{C} \quad f(x) \to f(\sqrt{2}+\sqrt{3}+\sqrt{5})$$

它是主理想吗？

提示：即为寻找$\sqrt{2}+\sqrt{3}+\sqrt{5}$之极小多项式。

问题 39. 请证明$A = \mathbb{R}[X,Y]/(X^2+Y^2+1)$是主理想整环，但不是*Euclid*整环。

提示：为证明其为主理想整环，证明A的素理想均形如$(ax+by+c)$，其中$(a,b) \neq (0,0)$，而x,y为$X,Y \in \mathbb{R}[X,Y]$在$mod\ X^2+Y^2+1$这一映射下的像。

为证明其不是*Euclid domain*，去证明如下引理：假设A是一个*Euclid domain,*那么存在素元$p \in A - \{0\}$使得$\pi(A^\times) = (A/pA)^\times$，其中$\pi : A \to pA$是典范满射。据此使用$A^\times = \mathbb{R}^\times$以及$(A/pA)^\times = \mathbb{C}^\times$，再说明$\mathbb{R}^\times \to \mathbb{C}^\times$必须是单射，再结合其为满射，得出矛盾。

问题 40. 对于$A = \mathbb{R}[X,Y]/(X^2+Y^2-1)$，$B = \mathbb{C}[X,Y]/(X^2+Y^2-1)$ 请证明*:*

1. X^2+Y^2-1是$\mathbb{R}[X,Y]$中的不可约元。

2. A不是唯一分解整环。

3. B是主理想整环。

4. 请给出A,B的单位。

提示：对于问题*1*，直接写出$X^2+Y^2-1 = (A(Y)X-B(Y))(C(Y)X-D(Y))$并证明矛盾。

对于问题*2*，证明$X^2 = (1+Y)(1-Y)$，并证明x为不可约元*(*其中x为X在商映射下的像*)*。

对于问题*3*，通过换元$X = \frac{e^{it}+e^{-it}}{2}$和$Y = \frac{e^{it}-e^{-it}}{2}$，证明$B \cong \mathbb{C}[z,z^{-1}]$。

对于问题*4*，利用范数$N : \mathbb{R}[x,y] \to \mathbb{R}[Y]$为$N(a(y)x+b(y)) = a^2(Y)+b^2(Y)(Y^2-1)$

注记：类似的问题可以提出很多，例如：请证明$\mathbb{C}[X,Y]/(X^3+Y^3-1)$不是唯一分解整环。但这个问题的证明很不初等，涉及到一些代数几何知识，有兴趣的同学可以思考并搜索学习。

问题 41. 对于$A=\mathbb{Z}+x\mathbb{Q}[x]$，其为$\mathbb{Q}[x]$的子环，证明其不为*Noetherian* $\mathbb{Q}[x]$模。

提示：证明其不满足升链稳定条件。具体为考虑$I_n=(\frac{x}{2^n})$

问题 42. 假设k是域，I是一个指标集，$A=\prod_{i\in I}k$

1. 若I是有限集，请刻画A的所有素理想。
2. 将上述问题推广到I为无限集的情况。

提示：对于有限乘积情形，使用$R\times R'$之理想的分类。对于无限情形，这个问题比较困难，可以查阅资料学习*Von-Neumann*环和超滤子的知识，并证明素理想与I上的*UltraFilter(*超滤子*)*一一对应。

问题 43. 假设$\mathfrak{a}$是A的非平凡理想，$S=1+\mathfrak{a}$，证明$\mathfrak{a}$在$S^{-1}A$中生成的理想包含于$S^{-1}A$的*Jacobson*根中。

提示：首先$\mathfrak{a}$生成的理想为$S^{-1}\mathfrak{a}$，使用如下证明过的判别方法:对于交换环R和其*Jacobson radical* $J(R)$,$x\in R$含于$J(R)$当且仅当其对于任一$y\in R$，均有$1-xy\in R^\times$，其中$R^\times$为R中的单位，

问题 44. 假设S是环A的乘法子集，假如其满足：如果$xy\in S$，那么$x\in S$且$y\in S$，称S为充盈的*(Saturated)*。请证明S是充盈的当且仅当$A-S$是一些素理想的并。

提示：证明充盈性是不困难的，为证明S充盈推出其为素理想的并，只需证明每个$A-S$中的元素落于一个包含于$A-S$的素理想中。对于$x\in A-S$，考虑集合族$\mathcal{F}=\{I\subset A|I\text{为理想},\ x\in I\ \text{且}\ I\cap S=\emptyset\}$, $\mathcal{F}$非空且使用*Zorn*引理去证明存在极大元，然后验证极大元是素理想。

问题 45. 设A为整环，证明：A是主理想整环当且仅当它的素理想都是主理想。

提示：考虑全体非主理想构成的集合，其不为空集，使用*Zorn*引理给出存在I是其中的极大元，证明其为素理想，从而为主理想，据此给出矛盾。

问题 46. 对于环A，假设$\mathfrak{p}$是它的素理想，定义$\mathfrak{p}$高度$ht(\mathfrak{p})$为包含于$\mathfrak{p}$的素理想构成的链的最大长度，即$\mathfrak{p}_0\subsetneq\mathfrak{p}_1\subseteq\ldots\subseteq\mathfrak{p}_m=\mathfrak{p}$，已知如下的*Krull*主理想定理：对于$R$为诺特环，$x\in R$既不是零因子也不是单位，那么含$x$的极小素理想高度均为*1*。

请利用这一定理证明：若A是*Noetherian*整环，那么A是唯一分解整环当且仅当高度为1的素理想都是主理想。

提示：为证明“当”的部分，*Noetherian*条件能给出分解的存在性，只需要证明任意不可约元x为素元即可。具体可以阅读*Stacks project Lemma 10.120.6*以及相关内容。

注记：更一般地，有*Kaplansky*定理来判定唯一分解性：一个整环A是一个唯一分解整环当且仅当下面两个条件成立：

1. A满足主理想条件：即每个非零素理想包含一个主素理想。
2. A中的每个不可约元素均为素元。

注记：之后还有一个问题将*Noether*整环改为了唯一分解整环，而把高度为1的条件删去。

问题 47. 假设A为局部环*(*即仅有唯一极大理想的环*)*,$\mathfrak{m}$为其极大理想,M为有限生成A模。

1. 若N是M的子模，满足$N+\mathfrak{m}M=M$，证明$N=M$。
2. $M/\mathfrak{m}M$是$A/\mathfrak{m}$-线性空间，设$x_1,...,x_n\in M$使得$\bar{x_1},...,\bar{x_m}$是$M/\mathfrak{m}M$的一组$A/\mathfrak{m}$-基，请证明$M=Ax_1+...+Ax_n$。

提示:这就是著名的*Nakayama*引理。对一般的环和理想也有类似结论，可以搜索学习。

问题 48. 令$A=\mathbb{Z}[x]$，n是整数且$n\neq 0,\pm 1$，令$\mathfrak{a}=<n,x>$证明$\mathfrak{a}$不是主理想，且假设$N=\mathfrak{a}\begin{bmatrix} n \\ x \end{bmatrix}\subsetneq A^2$是$A$-子模，考虑$A$-模$M=A^2/N$,证明$M_{tor}$并不是$M$的直和因子。

提示：第一部分的验证是平凡的，第二部分假设存在直和分解$M=M_{tor}\oplus\tilde{M}$，去证明对于元素$[(1,0)]\in M$给出矛盾，其中M中的元素为等价类$[(a,b)]=(a,b)+N$

注记：这是“*PID*上的一元多项式环不一定是*PID*”以及“非*PID*上没有有限生成模的结构定理”的经典反例。

问题 49 (形式幂级数)**.** 令$\mathbb{F}$是一个域，$\mathbb{F}[[x]]$是形式幂级数$f(x)=a_0+a_1x+a_2x^2+...,\ a_i\in\mathbb{F}$构成的集合，其上环结构定义类似于多项式环。

1. 请证明$\mathbb{F}[[x]]$是一个*Euclid*-整环。
2. 请找出$\mathbb{F}[[x]]$的单位。
3. 请找出$\mathbb{F}[[x]]$的所有理想。
4. 令$\mathbb{F}((x))$是全体*Laurent*级数 $f(x)=\sum_{i\geq n}a_ix^i,\ a_i\in\mathbb{F},\ n\in\mathbb{Z}$构成的集合，其上也有类似的环结构，请证明$\mathbb{F}((x))$是一个域。

提示：考虑如下的函数$\sigma:\mathbb{F}[[x]]\to\mathbb{N},\ \sigma(f)=i,$ 其中i是使得$a_i\neq 0$最小的x_i之次数。

问题 50. *1.* 请证明如果x是幂零元，那么$1+x$是单位。

2. 请证明如果环R有正特征$p \neq 0$，那么如果a是幂零元，那么$(1+a)$是幂等元，即存在m使得$(1+a)^m = (1+a)$。

提示：取$m = p^{n!}+1$，其中n使得$a^n = 0$

问题 51. 对于环R, R'，请证明$R \times R'$的素理想的集合与R,R'的素理想的集合的无交并之间有一一对应。

问题 52 (连续函数环的极大理想)**.** 假设X是闭区间$[0,1]$，且R为其上实值连续函数环。

1. 令$f_1, ..., f_n$为X上没有公共零点的连续函数，那么这些函数生成的理想是整个环R。

提示：可以证明$f_1^2 + ... + f_n^2$是单位。

2. 请给出R的极大理想与X上的点的一一对应。

提示：对于任意$x_0 \in X$，定义$\mathfrak{m}_{x_0}$为全体在x_0处取值为0的函数。对于任一极大理想$\mathfrak{m}$，考虑$I(\mathfrak{m}) = \{x \in X | f(x) = 0 \ for \ all \ f \in M\}$来证明$\mathfrak{m}$一定形如$\mathfrak{m}_{x_0}$,从而证明满射。

问题 53. 一个素数p可以被写成m^2+2n^2，其中$m, n \in \mathbb{Z}$当且仅当x^2+2在$\mathbb{F}_p$中有根。

提示：利用$\mathbb{Z}[\sqrt{-2}]$是一个*PID (*实际上它是*ED)*，来证明p在$\mathbb{Z}[\sqrt{-2}]$中是可约的即可，这只需要证明$\mathbb{Z}[\sqrt{-2}]/(p)$不是一个域。

问题 54. 求一组多项式方程$f^2 + g^2 = h^2$在$\mathbb{C}[t]$上的非平凡解，即$f, g, h \in \mathbb{C}[t]$满足$\deg f, \deg g, \deg h \geq 1$且$gcd(f, g, h) = 1$。并回答所有解可以是什么形式?

提示：请参考勾股方程的正整数解的形式之证明，首先要做分解$(f+ig)(f-ig) = h^2$。

问题 55 (书院2024春博资考)**.** 假设R是整环，$Aut(R)$是环R的自同构群，对于$Aut(R)$的有限子群G，定义

$$R^G = \{r \in R | g(r) = r \ , \forall g \in G\}$$

1. 证明R在R^G上整。

提示：对于$r \in R$，考虑$f(x) = \prod_{\sigma \in G}(x - \sigma(r))$

2. 证明对于$Aut(R)$的有限子群G和H，如果有$R^G = R^H$，那么$G = H$。

提示：考虑环R的分式域$Frac(R)$然后使用域的*Galois*理论。

问题 56 (书院2024春博资考)**.** 一般来说，极大理想的拉回不是极大理想。但假设A, B为域k上的有限生成代数，且环同态$f : A \to B$使得f限制在k上为恒等映射，那么对于任一B中的极大理想$\mathfrak{m}$，$f^{-1}(\mathfrak{m})$为A的极大理想。

提示：只需要证明$A/f^{-1}(\mathfrak{m})$是域，证明如下的引理：假设K/k是整环的整扩张，那么k是域当且仅当K是域。

问题 57 (书院2024秋博资考). 对于$p>5$为素数，$\alpha \in \overline{\mathbb{F}_p}\backslash\mathbb{F}_p$是一个元素，使得$\alpha^3=-1$，那么$p$在$\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$中不可约当且仅当$p\equiv 2(mod\ 3)$

提示：可以使用如下两个事实：$\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$是一个*Euclid*环，并且$(\alpha-\alpha^{-1})^2=-3$，最后使用二次互反律

$$(\frac{-3}{p})=(\frac{p}{3})$$

问题 58 (北大代数学I实验班2024期末). 假设R是一个唯一分解整环，假设R中所有非零的素理想都是极大理想。证明R是一个*PID*。

提示：对于I中的理想R，*UFD*性质给出其中每个元素都可以写成不可约元素的乘积，考虑素因子最少的元素$f=p_1p_2...p_r$，其中$p_1,...,p_r\in R$是不可约元素，去证明$I=(f)$。

注意到对于*non-associated* 素元 p,q，则存在a,b满足$ap+bq=1$。假设$g=p_{s+1}...p_rq_1...q_t$，且$p_1,...,p_s$和$q_1,...,q_t$之间两两互素，于是对于$(i,j)\in\{1,2,...,s\}\times\{1,2,...,t\}$，存在$a_{ij},b_{ij}$使得$a_{ij}p_i+b_{ij}q_j=1$，由于$p_{s+1}...p_r=p_{s+1}...p_r\prod_{i=1}^{s}\prod_{j=1}^{t}(a_{ij}p_i+b_{ij}q_j)$，与最小性矛盾。

注记：众所周知*PID*可以推出*UFD*，问题是反过来呢？这个问题给出了*UFD*和*PID*之间的差距。

问题 59 (北大代数学I实验班2021期末). 令R是一个交换环，若所有R的自由模的子模都是自由的，则R是一个主理想整环。

提示：先证明R整环，即通过假设$ab=0$并考虑$aR\subset R$推出矛盾。其次证明对于所有的理想，它作为R模均是自由且*rank*为*1*的，据此可说明R为*PID*。

问题 60 (北大代数学I实验班2023期中). 设R是一个唯一分解整环，且恰有两个互不相伴的素元p,q使得任一素元均与p或q相伴。

1. 对于正整数m,n，证明理想$(p^m,q^n)=R$。
2. 证明R是一个主理想整环。

提示：

1. 考虑p^m+q^n之素因子分解。
2. 假设I为R的一个非平凡理想，对于每个$x\in I$，x形如$u(x)p^{m(x)}q^{n(x)}$，并令$n:=\min_x n(x)$, $m:=\min_x m(x)$。去证明$I=(p^mq^n)$, 注意利用第一问的结论。

问题 61 (北大代数学I实验班2022期末). 请计数环$\mathbb{Z}[x]/(x^3+1,6)$中的素理想个数。

提示：利用如下的等式以及$R_1 \times R_2$的素理想结构即可。

$$\mathbb{Z}[x]/(x^3+1,6) \cong \mathbb{F}_3[x]/(x^3+1) \times \mathbb{F}_2[x]/(x+1) \times \mathbb{F}_2[x]/(x^2-x+1)$$

问题 62. 令R是一个主理想整环，M是有限生成的R-模，并且$F = \mathrm{Frac}(R)$，请证明$\mathrm{Hom}_R(M,F)$和$M \otimes_R F$作为F上的线性空间维数相同。、

提示：使用PID上的有限生成模的结构定理，去说明维数就是M的秩r。

问题 63 (虚二次数域的代数整数环的唯一分解性). 本题聚焦于研究虚二次数域，即$\mathbb{Q}[\sqrt{d}]$，且d是一个无平方因子的整数，满足$d<0$。

定义$\mathbb{C}$中的代数整数为

$$A = \{x \in \mathbb{C} | \text{存在} \mathbb{Z}[t] \text{中的首一多项式} f(t) \text{使得} f(x) = 0\}$$

1. 请证明A是$\mathbb{C}$的子环。

   提示：先证明两个引理：$a \in A$当且仅当a是某一个矩阵$M \in M_n(\mathbb{Z})$之特征值(考虑多项式$f(x)$对应的友阵)，并且证明对于两个矩阵B,C,其特征值分别为$\lambda_1,...,\lambda_n$和$\mu_1,...,\mu_n$,那么$B \otimes C$的特征值为$\lambda_i\mu_j$，其中$1 \le i,j \le n$。

2. 请证明$A \cap \mathbb{Q} = \mathbb{Z}$

3. 请证明$R := A \cap \mathbb{Q}[\sqrt{d}] = \begin{cases} \mathbb{Z}[\sqrt{d}] & for \quad d \equiv 2,3 (mod\ 4) \\ \mathbb{Z}[\frac{\sqrt{d}+1}{2}] & for \quad d \equiv 1 (mod\ 4) \end{cases}$

   提示：$a+b\sqrt{d} \in A$当且仅当$2a \in \mathbb{Z}$且$b^2d - a^2 \in \mathbb{Z}$。

4. 请证明对于$R = A \cap \mathbb{Q}[\sqrt{d}]$

   当$d=-1$时，R的单位为$\{\pm 1, \pm \mathrm{i}\}$

   当$d=-3$时，R的单位为$\{\pm 1, e^{\frac{\pi}{3}}, e^{\frac{2\pi}{3}}, e^{\frac{-\pi}{3}}, e^{\frac{-2\pi}{3}}\}$

   当$d<0,\ d \neq -1,-3$时，R的单位只有$\{\pm 1\}$

   提示：可以考虑如下的映射:

   $$N : R \to \mathbb{Z} : \quad a+b\sqrt{d} \to a^2 - b^2 d$$

   它满足$N(\alpha\beta) = N(\alpha)N(\beta)$

下面我们想问什么时候R是唯一分解的？

这个问题实际上有如下回答，$\mathbb{Q}[\sqrt{d}]$的代数整数环R是唯一分解整环当且仅当

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

这里我们来验证这些d满足题目要求。我们的主要思路是先证明对于这些R，R为UFD当且仅当它为PID，并且通过研究其理想类群*(ideal class group)*的结构来说明对于这些d，它们确实是唯一分解的。

1. 请证明$d \equiv 3(mod\ 4)$且 $d < 0, d \neq 1$时，以及$d \equiv 2(mod\ 4)$且$d \neq -2$时，R不是唯一分解的。

   提示：可以考虑分解$1 - d = 2\frac{1-d}{2} = (1 - \sqrt{d})(1 + \sqrt{d})$

$\mathbb{R}^2$中的格*(Lattice)*与R中理想

我们将R中的非零理想与$\mathbb{R}^2$中的格联系起来。

1. $\mathbb{R}^2$的离散子群只有如下三种

   $\{0\}$

   $\mathbb{Z}a$

   $\mathbb{Z}a + \mathbb{Z}b$其中$a, b$在$\mathbb{R}$上线性无关，此时称$\mathbb{R}^2$的一个格*(lattice)*

2. 如果I是R的一个非零理想，那么I是$\mathbb{R}^2$的一个格。

3. 如果$I \subset R$是$\mathbb{R}^2$中的一个格，那么I是R的理想当且仅当

   $\sqrt{d}I \subset I, \quad d \equiv 2, 3(mod\ 4)$

   $\frac{\sqrt{d}+1}{2}I \subset I, \quad d \equiv 1(mod\ 4)$

R中理想的乘积分解

本节中R始终为某个虚二次数域的代数整数环。

定义共轭映射为

$$\mathbb{Q}[\sqrt{d}] \to \mathbb{Q}[\sqrt{d}] : a + b\sqrt{d} \to a - b\sqrt{d}$$

而$\bar{I}$定义为I在共轭映射下的像。并且定义

$$IJ = \{\sum_{i=1}^{n} a_i b_i | a_i \in I\ b_i \in J\}$$

1. R的非零理想I都有如下性质*:*

   $$I\bar{I} = (n), \quad n \in \mathbb{Z}$$

   提示：由于I为$\mathbb{R}^2$中的格，记$I = (\alpha, \beta)$，那么$I\bar{I} = (n)$,其中$n := gcd(\alpha\bar{\alpha}, \beta\bar{\beta}, \bar{\alpha}\beta + \alpha\bar{\beta})$

2. 对于R的素理想P,如果$P|IJ$，那么$P|I$或者$P|J$

   提示：先证明$(0) \neq J \subset I$，那么存在理想I'使得$J = II'$，然后注意到$IJ \subset P$意味着$I \subset P or\ J \subset P$

3. 如果I是R的一个理想，那么R/I有限。据此说明如果$(0) \neq I$，那么含有I的理想只有有限多个。

   提示：去证明$R/I\bar{I}$有限即可。

4. 证明R的素理想均为极大理想。

   提示：利用结论“有限整环一定是域”

5. 证明R中的每个非平凡理想都可以分解成素理想的乘积，且这个分解在除去排序的意义下唯一。

   提示：使用反证法，如果$(0) \neq I$不是极大理想，那么$I = P_1 I'$其中P_1为一个包含I的素(极大)理想，再利用含有I的理想只有有限多个。

6. 证明R为唯一分解整环当且仅当R是主理想整环。

   提示：证明所有素理想都是主理想，然后使用上面两问的结论。

理想类群

对于虚二次数域的代数整数环R，定义R的类群(class group)为$\mathcal{C}(R) := \{I \neq 0, I是R的理想\}/\sim$，其中$I \sim I'$当且仅当存在$\alpha \in \mathbb{Q}[\sqrt{d}]$使得$I = \alpha I'$，并且用$[I]$来记$I$在$\mathcal{C}(R)$中的等价类。

1. $\mathcal{C}(R)$构成了一个Abel群，其中群结构定义为$[AB] := [A][B]$,其中单位元$[R]$由全体主理想组成。据此说明R是UFD当且仅当它的类群$\mathcal{C}(R)$是平凡群。

2. 对于R的一个理想I满足$I\bar{I} = (n)$，其范数定义为$N(I) = n$，请证明$N(IJ) = N(I)N(J)$以及若$I = (\alpha)$，那么$N(I) = N(\alpha)$。

3. 记$\Delta(L)$为格L的面积，请证明$N(I) = |R/I| = \Delta(R)/\Delta(I)$

   提示：去证明$[I : I\bar{I}] = [R : \bar{I}] = [R : I]$, 其中$[I : J] := |I/J|$，这是良定义的。实际上对于任意理想$I, J_1 \supset J_2$，都有

   $$[IJ_1 : IJ_2] = [J_1, J_2]$$

   可以验证这个结论对I为主理想成立，而根据分解性质，只用对素理想I证明，去证明$I\bar{I} = (p)$，其中p是素数，然后证明$[J_1 : IJ_1] = [J_2 : IJ_2] = p$;再利用指数的传递性，即$[J_1 : J_2][J_2 : J_3] = [J_1 : J_3]$。

4. 取α为$(0) \neq I$中范数最小的元素，那么$N(\alpha) \geq N(I)$，请证明$N(\alpha) \leq \mu N(I)$，其中$\mu = \begin{cases} 2\sqrt{\frac{|d|}{3}} & d \equiv 2,3(mod\ 4) \\ \sqrt{\frac{|d|}{3}} & d \equiv 1(mod\ 4) \end{cases}$

   提示：利用上一问的结果，并思考$\Delta(R)$对于不同的d具体是多少？

5. $C(R)$由范数为素数p且$\leq \mu$的理想生成。

   提示：素理想的范数一定为p或者p^2, 且如果为p^2，那么它一定为主理想。

6. 请任选两个d，使得$d \neq -1,-2,-3$且$\mathbb{Q}[\sqrt{d}]$的代数整数环R为唯一分解整环, 并证明你的结论。

   提示：如果选取$d \neq -67$，计算得$\mu = 4$，去证明$(2),(3)$为素(极大)理想即可，转化为证明$R/(2)$,$R/(3)$为域。

3 Galois理论

问题 64. 请证明多项式x^4+3x+3是$\mathbb{Q}[\sqrt[3]{2}]$上的不可约多项式。

提示：令α是x^4+3x+3的一个根，去证明$[\mathbb{Q}[\alpha,\sqrt[3]{2}],\mathbb{Q}[\sqrt[3]{2}]] = 4$

问题 65. 本题研究一些域的二次扩张。

我们称$\mathbb{F}$的域扩张K_1和K_2等价当且仅当存在一个域同构$\varphi : K_1 \to K_2$使得$\varphi|_F : F \to F$为恒等映射。

1. 对于$\mathbb{Q}$，请在同构的意义下分类其上的二次扩张。

2. 对于特征为2的域$\mathbb{F}$，请分类其上的二次扩张。

   提示：请证明二次扩张一定形如$K = F[\alpha]$,其中$\alpha^2 \in F$但是$\alpha \notin F$或者$K = F[\alpha]$，其中$\alpha^2 - \alpha \in F$但是$\alpha \notin F$，并且说明这两种情况不可能同构。

3. 请分类$\mathbb{F}_2(x)$的2次扩张。

   提示：先用上一问做分类，得到两类情况

问题 66. 假设K是F上的n-次多项式$f(x)$之分裂域，请证明$[K:F]|n!$ 并举例说明，存在这样的$f(x)$使得$[K:F] = n!$

提示：使用归纳法，分f作为$\mathbb{F}$多项式为可约/不可约两类情况处理。

问题 67. 请说明如下三个域之间是否同构？

1. $\mathbb{Q}(t)$上多项式$x^2 - t^3$的分裂域。

2. $\mathbb{Q}(t)$上多项式$x^2 - t^5$之分裂域。

3. $\mathbb{Q}(t)$上多项式$x^2 + t^2$之分裂域。

提示：因为这些域都是二次扩域，为证明不同构，只需要证明某一多项式在另一个扩域上没有根即可。

问题 68 (书院2024秋博资考). 请计数$\mathbb{F}_p[x]$上的首一不可约多项式的数量。其中$\mathbb{F}_p[x]$为p个元素的有限域。

提示：先证明讲义中的练习题32：假设$I(d)$为$\mathbb{F}_p[x]$中的d-次首一不可约多项式的数量，于是$q^n = \sum_{d|n} d \cdot I(d)$，然后使用$Mobius$反演公式。

问题 69. 请解决以下一系列问题：

1. 对于$Q(x) \in \mathbb{C}(x)$为一个非常值有理函数，请确定域扩张$[\mathbb{C}(x) : \mathbb{C}(Q(x))]$的次数。

2. 对于一个域 $\mathbb{F}$，请证明

$$Aut_{\mathbb{F}}(\mathbb{F}(x)) = \{x \to \frac{ax+b}{cx+d} | det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0\}$$

并且证明$Aut_{\mathbb{F}}(\mathbb{F}(x)) \cong PGL(2, \mathbb{F})$ 作为群同构。

提示：假设x在$Aut_{\mathbb{F}}(\mathbb{F}(x))$中的元素下的像为$\frac{f(x)}{g(x)}$，其中$f, g$互素，然后需要证明$[\mathbb{F}(x) : \mathbb{F}(\frac{f(x)}{g(x)})] = 1$，再利用上一问的结论。

3. 请找出一个$Aut_{\mathbb{F}}(x_1, ..., x_n)$中的同构于$PGL(n+1, \mathbb{F})$的子群，并且对于$n \geq 2$，找一个不在其中的元素。

提示：构造部分可以模仿上一问给的$Aut_{\mathbb{F}}(\mathbb{F}(x))$中的元素，而考虑$g : \mathbb{F}(x_1, ..., x_n) \to \mathbb{F}(x_1, ..., x_n)$，其中$x_1 \to x_1^{-1}$且$x_i \to x_i$对于任一$i$均成立，请证明其不在$PGL(n+1, \mathbb{F})$中。

4. 对于素数p，规定$\mathbb{F}_p$为p个元素的有限域，且$F = \mathbb{F}_p(t)$为$\mathbb{F}_p$上的有理函数域。考虑F的子域$C \subset F$使得F/C是有限$Galois$扩张

请证明在这些域扩张中，存在C_0使得任意C满足题目条件, 均有$C_0 \subset C$

请确定F/C_0的次数。

提示：使用$Aut_{\mathbb{F}_p(\mathbb{F}_p(t))} = PGL(\mathbb{F}_p, 2)$并且计算$PGL(\mathbb{F}_p, 2)$中的元素个数。

问题 70. 请找出域扩张$\mathbb{C}(t)/\mathbb{C}(t^n + \frac{1}{t^n})$的所有中间域，并对这些中间域找出本原元素。

提示：先证明这个域扩张的$Galois$群为D_n。

问题 71. 请证明如下两个习题：

1. 假设k为一个域，$f(x)$为$k[x]$中不可约多项式，并且K/k是一个有限正规域扩张，请证明如果$f(x)$在$K[x]$上有首一的不可约因子g,h，则存在$\sigma \in Aut_k(K)$使得$\sigma(f)=g$，并且对于K/k不是正规的情形给出反例。

   提示：考虑g的一个根α_1和h的一个根α_2，于是α_1,α_2在k上有公共极小多项式f，于是存在$\sigma: K \to K$使得$\sigma(\alpha_1)=\alpha_2$

2. 对于K/F为域的有限扩张，请证明K/F是正规扩张当且仅当对于任一不可约多项式$f(x)\in F[x]$，$f(x)$在$K[x]$中的不可约因子次数均相同。

   提示：使用上一问的结论，因为存在$\sigma(f)=g$,于是次数相同。

问题 72. 对于域F的单代数扩张$F[\gamma]$，则其只有有限个中间域$F\subset L\subset F[\gamma]$。

提示：假设f_L为γ在L上的极小多项式，请证明$L\to f_L$是单射，并且f_L只有有限种可能。

问题 73 (书院2025春博资考)**.** 对于有限域k满足$char\ k=p\neq 0$, $K=k(t,u)$且$F=k(t^p,u^p)$, 请证明如果k是无限域，那么存在无限个中间域$F\subset L\subset K$。

提示：去证明如果对于$a,b\in k$满足$F(t+au)=F(t+bu)$，那么$a=b$。具体方法为：如果$a\neq b$使得$F(t+au)=F(t+bu)$那么$F(t+au)=F(t+bu)=F(t,u)$然后计算次数。

问题 74. 对于特征为p的域F，考虑其有限扩张K/F，并令K^p为其*Frobenius*映射下的像，请证明K/F可分当且仅当$FK^p=K$

提示：如果$FK^p\neq K$，那么考虑K/K_s，其中K_s为可分闭包，取e_m为最大的正整数使得存在$x\in k$，$x^{p^{e}_m}\in K_s$但是$x^{p^{e_m-1}}\notin K_s$，据此说明矛盾。

问题 75. 对于一个特征为0的域F，去证明$F(X^2)\cap F(X^2-X)=F$，其中$F(X^2-X)$,$F(X^2)$均视为$F(X)$的子域。

提示：考虑$\sigma: x\to -x\in Aut_F(F(X))$固定$F(X^2)$，而$\tau: x\to -x+1\in Aut_F(F(X))$固定$F(X^2-X)$,于是$|\langle\sigma,\tau\rangle|=\infty$，然后分析域扩张$[F(\frac{f}{g}):F]$的次数。

问题 76. 对于可分首一n次多项式f_1,f_2,f_3，他们均是整系数的，且满足如下条件：

1. f_1在$mod\ 2$ 意义下不可约。
2. f_2在$mod\ 3$意义下形如一个1次和另一个$n-1$次不可约多项式的乘积。
3. f_3在$mod\ 5$意义下形如一个二次不可约多项式和*1*或*2*个奇数次不可约多项式的乘积。

我们令

$$f = -15f_1 + 10f_2 + 6f_3$$

证明f在$\mathbb{Q}$上的$Galois$群为置换群S_n。

提示:考虑$Dedekind$给出的通过mod_p计算$Galois$群的方法。

问题 77. 请证明存在无穷多对互素的正整数a, b使得$-4a^3 - 27b^2$是$\mathbb{Z}$中的平方数。

提示：构造$a = x_1x_2 + x_2x_3 + x_1x_3$，$b = -x_1x_2x_3$且$x_1 + x_2 + x_3 = 0$

问题 78. 假设α是一个代数整数，且$f(x)$是其在$\mathbb{Q}$上的极小多项式，假设$f(x)$在$\mathbb{C}$中的根的模长均为1，请证明α是单位根。

提示：考虑α之幂次，然后注意到这些α^k的极小多项式的系数是有界的。目标是去证明α^k只有有限种选择方式，而这是通过证明其极小多项式f_k只有有限种选择所给出的。

问题 79 (Brauer). 本题的最终目标是证明如下的结果：如果一个$\mathbb{Q}$上的p次不可约多项式$f(x)$恰有$p-2$个实根，那么其不是根式可解的，其中p为素数。

1. 对于素数p，H为S_p中一个阶为p的子群，请找出H在S_p中的正规化子。

   提示：请计数S_p之p-$sylow$子群的个数，然后使用关于$N_{S_p}(H)$(即正规化子)的$Sylow$定理，给出$N_{S_p}(H) = p(p-1)$,然后具体构造出这个群。

2. 对于有限群G，其自由作用在集合X上，令H为G的一个正规子群，请证明X中的每个H轨道都是等长的。即为$\forall x, y \in X$,均有$|Hx| = |Hy|$

3. 令p是一个素数，G为对称群S_p的一个可解子群，并满足$p||G|$，请证明G的$Sylow$-p子群在G中正规。

   提示：注意到G包含一个p循环，那么其在$[p]$上的作用是传递的，令H为1的稳定化子，而$G^{(n)}$为其n次导出子群，即$G^{(0)} = G$，且$G^{(k+1)} = [G^{(k)}, G^{(k)}]$，去证明$|G^{(n)} \cap H| = 1$，据此说明$G^(n)$是$G$的一个$Sylow$-$p$子群，然后得到本题结论。

4. ***Galois*定理** 假设F是一个特征为0的域，如果$f(x) \in F[x]$是一个p次不可约多项式，且p为素数，那么f根式可解当且仅当对于f的任意两个根$\alpha_i.\alpha_j$，均有$K = F[\alpha_i, \alpha_j]$。

   提示：使用$Galois$理论翻译，只需要证明任一传递子群$G \subset S_p$可解当且仅当G中有不少于两个不动点的元素均为单位元。

   对于可解推出不动点的情况，可以考虑G如果可解，那么其一定包含于一个p-$cycle$的稳定化子，然后具体计算，如果G满足后一条件，那么考虑$G \to \{(x, y) \in [p] \times [p] | x \neq y\}$ $g \to (g(1), g(2))$，那么其为单射，于是$|G| \leq p(p-1)$，据此说明$Sylow$-p子群都正规，于是G可解。

5. ***Brauer***对于素数$p \geq 5$,请证明若$\mathbb{Q}$上的p次不可约多项式$f(x)$恰有$p-2$个实根，那么其不是根式可解的。

   提示：使用上一问的结果，选两个实根即可。

问题 80. 请找出$Aut_{\mathbb{Q}}(\mathbb{C})$中的共轭这一元素的中心化子。

提示：对于这样的σ，先说明$\sigma|_{\mathbb{R}} \in Gal_{\mathbb{Q}}(\mathbb{R})$，再说明$Gal_{\mathbb{Q}}(\mathbb{R})$是平凡的。

问题 81. 对于F为$\mathbb{Q}$的*Galois*扩张，令α为F中的一个元素，满足$\alpha F^{\times 2}$不被$Gal(F/\mathbb{Q})$在$F^{\times}/F^{\times 2}$的作用下固定，并令$\alpha = \alpha_1, ..., \alpha_n$为$\alpha$在$Gal(F/\mathbb{Q})$下的轨道。证明

1. $F[\sqrt{\alpha_1}, ..., \sqrt{\alpha_n}]/F$是*Galois*扩张，且*Galois*群交换，含于$(\mathbb{Z}/2\mathbb{Z})^n$中。
2. $F[\sqrt{\alpha_1}, ..., \sqrt{\alpha_n}]/\mathbb{Q}$是*Galois*扩张，且*Galois*群是$(\mathbb{Z}/2\mathbb{Z})^n \rtimes Gal(F/\mathbb{Q})$中的非交换子群。

   提示：对于第一问，先证明它是某个多项式的分裂域，然后考虑每个α_i可能的像。对于第二问，先证明F在$Gal([\sqrt{\alpha_1}, ..., \sqrt{\alpha_n}]/\mathbb{Q})$的作用下不变

问题 82. 令K是$\mathbb{Q}$的一个有限扩张，请证明K中只有有限个单位根。

提示：对于某个K中的d次单位根ξ，注意到$[\mathbb{Q}(\xi), \mathbb{Q}] = \varphi(d)$，其中$\varphi(d)$为$d$的数论函数，代表了小于$d$且与$d$互素的数的个数。

问题 83. 请证明每一个有限*Abel*群均可以实现为某个*Galois*扩张$K/\mathbb{Q}$的*Galois*群。

提示：请先证明如下数论上的事实*(Dirichlet theorem)*：对于素数p_1和任意$\alpha_1 \in \mathbb{Z}_{\geq 0}$，总能找到素数$q_1$使得$p_1^{\alpha_1} | q_1 - 1$，然后使用分圆扩张。事实上，这样的素数$q_1$有无限多个。

问题 84. 令F是一个特征不为2的域，并令$\alpha \in F^{\times} \backslash (F^{\times})^2$，并且$a, b \in F$。如果$K = F[\sqrt{\alpha}]$是$F$的一个二次扩张，且$L = K[\sqrt{a + b\sqrt{\alpha}}]$是$K$的一个二次扩张，那么$L/F$是*Galois*扩张且*Galois*群是循环群当且仅当存在某个$c \in F^{\times}$使得$a^2 - b^2\alpha = c^2\alpha$。

提示：请回顾*Galois*理论练习题中判别$\mathbb{Q}(\sqrt{1+\sqrt{2}})$以及$\mathbb{Q}(\sqrt{2+\sqrt{2}})$是否为*Galois*扩张的解法。

问题 85. 请证明不存在$\mathbb{Q}(\sqrt[n]{p})$和$\mathbb{Q}(\sqrt[n]{q})$之间的非平凡域同构。

提示：直接证明，考虑$\sqrt[n]{p}$的像$a_0 + a_1\sqrt[n]{q} + a_2(\sqrt[n]{q})^2 + ... + a_{n-1}(\sqrt[n]{q})^{n-1}$，$n$次方后比较系数给出矛盾。

注记：这里的素数条件是不可或缺的，否则可以轻易地给出反例。

问题 86. 假设K是一个特征p的域，$\phi : K \to K$是*Frobenius*映射，若$a \in K - \mathrm{Im}(\phi)$，证明$X^p - a \in K[X]$是不可约的。

提示：$X^p - a$在其分裂域中的分解只能形如$X^p - a = (X - \alpha)^p$。

问题 87. 假设p为素数，$\mathbb{F}$为恰含有p^d个元素的有限域，证明对于任意非零的域同态$f:\mathbb{F}\to\mathbb{F}$，存在整数$n$使得$f(x)=x^{p^n}$对于任意$x\in\mathbb{F}$均成立。

提示：先说明$f\in\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$，然后利用$\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$的结构*(*其是一个循环群$\langle\sigma\rangle$，其中生成元$\sigma$为*Frobenius*映射*)*。

问题 88. 请指出多项式x^4-7在如下域之上的分裂域，并指出分裂域相比于原来的域的域扩张次数*:*

1. $\mathbb{Q}$
2. $\mathbb{F}_5$
3. $\mathbb{F}_{11}$

提示：在$\mathbb{F}_5$上，$x^4-7=x^4-2$；而在$\mathbb{F}_{11}$中，$x^4-7=x^4+4=(x^2+2x+2)(x^2-2x+2)$，然后考虑其判别式是否是$\bmod 11$的二次剩余。

问题 89. 请证明多项式$P(x)=x^5-9x^3+15x+6$在环$\mathbb{Q}[\sqrt{2},\sqrt{3}][x]$中不可约。

提示：先证明它在$\mathbb{Q}[x]$上是不可约的，这可以使用*Eisenstein*判别法，然后考虑若可约，取一个根α使得$P(\alpha)=0$并考虑$\mathbb{Q}\subseteq\mathbb{Q}[\sqrt{2},\sqrt{3}]\subseteq\mathbb{Q}[\sqrt{2},\sqrt{3}](\alpha)$，利用*4*和*5*互素。

问题 90. 假设$f(x)\in K[x]$为次数为n的不可约多项式，L/K是有限域扩张，$m=[L:K]$，且$\gcd(m,n)=1$，那么$f(x)\in L[x]$是不可约的。

提示：考虑域扩张序列$K\subset L\subset L[\alpha]$和$K\subset K[\alpha]\subset L[\alpha]$

问题 91. 假设$S\subset K[x]$，L/K是S的分裂域，证明若F为L中K的子扩张，则L也是S中多项式在F上的分裂域。

提示：去证明下面两点：

1. S中的每一个多项式都在L中分解为一次的因子。
2. L是由F和S中的多项式的所有根生成的最小域。

问题 92 (北大代数学I实验班2024期末)**.** 固定素数p，假设L/K是特征p的域的一个有限扩张。记σ为域L的*p-Frobenius*自同态。

1. 考虑L/K的中间域

$$K\subseteq\ldots\subseteq K\sigma^3(L)\subseteq K\sigma^2(L)\subseteq K\sigma(L)\subseteq L$$

证明对于所有非负整数n，均有

$$[K\sigma^n(L):K\sigma^{n+1}(L)]\geq[K\sigma^{n+1}(L):K\sigma^{n+2}(L)]$$

2. 证明：如果$[L:K\sigma(L)]\leq p$，那么域扩张L/K可以由一个元素生成。

提示：第一问使用

$$[K\sigma^n(L):K\sigma^{n+1}(L)]=[\sigma(K)\sigma^{n+1}(L):\sigma(K)\sigma^{n+2}(L)]$$

这是由于$\sigma(K)\sigma^{n+1}(L)/\sigma(K)\sigma^{n+2}(L)$作为域扩张同构于$K\sigma^n(L)/K\sigma^{n+1}(L)$。

对于第二问，注意到$K\sigma^n(L)/K\sigma^{n+1}(L)$是素数$p$的整数次幂，由于$p\geq[L:K\sigma(L)]\geq[K\sigma(L):K\sigma^2(L)]\geq ...$于是存在某个正整数$n$使得

$$[L:K\sigma(L)]=...=[K\sigma^{n-1}:K\sigma^n(L)]=p$$

$$K\sigma^n(L)=K\sigma^{n+1}(L)=K\sigma^{n+2}(L)=...$$

分别证明$L/K\sigma^n(L)$和$K\sigma^n(L)/K$由一个元素生成(前者可以直接构造出，后者是通过证明$K\sigma^n(L)/K$是可分扩张)，据此说明α,β作为L中的元素生成了域扩张L/K且β是可分元，据此再证明L/K由一个元素生成。

问题 93 (北大代数学I实验班2024期末). 设L/K是一个*Galois*扩张，且*Galois*群为一个σ生成的n阶循环群，假设$n=ab$且$gcd(a,b)=1$，令F_1为σ^a之固定域，F_2为σ^b之固定域，假设$F_1=K(\alpha)$且$F_2=K(\beta)$，证明$L=K(\alpha+\beta)$。

提示:使用反证法，假设$L\neq K(\alpha+\beta)$，那么$K(\alpha+\beta)$被某个σ^i所固定，据此给出矛盾。

问题 94 (北大代数学I实验班2021期末). 设域F满足$\mathbb{Q}\subseteq F\subset\mathbb{C}$并且$F/\mathbb{Q}$是一个有限交换*Galois*扩张，且$\alpha\in F$的极小多项式为$f(x)\in\mathbb{Q}[x]$且满足$|\alpha|=1$

1. 证明F在复共轭下保持稳定。
2. 证明$f(x)$的任一复根β都满足$|\beta|=1$
3. 记$f(x)=x^n+a_{n-1}x^{n-1}+...+a_0$，证明对所有的$0\leq i<n$都有$|a_i|\leq 2^n$
4. 证明F只含有有限多个绝对值为*1*的代数整数。
5. 证明上面的代数整数都是单位根。

提示:

1. 使用*Kronecker-Weber*定理，给出F包含于某个$\mathbb{Q}[\xi_N]$
2. 记复共轭为c，然后利用$f(x)$不可约，即存在$\sigma\in Gal(F/\mathbb{Q})$使得$\sigma(\alpha)=\beta$，然后利用$c$和$\sigma$交换即可。

3. 将$f(x)$写为$f(x)=\prod_{i=1}^{n}(x-\alpha_i)$并且满足每一个$|\alpha_i|\leq 1$，展开后使用三角不等式。

4. 去说明α的极小多项式的系数绝对值均小于2^n

5. 考虑$1,\alpha,\alpha^2,...,\alpha^n...$

问题 95 (北大代数学I实验班2021期末). 设k为一特征$p>0$的完美域，设$F=k(t)$为k上单变元的函数域，证明F的任一有限扩张都是单扩张，即存在$\alpha\in E$使得$E=F(\alpha)$。

提示：根据本原元素定理，有限可分扩张一定是由一个元素生成的，我们证明如下的结果:令E在F上由一个元素生成，那么下面两者必有一个成立:

1. E/F是可分扩张

2. $k(t^{1/p})\subseteq E$

问题 96 (北大代数学I实验班2021期末). 设$f(x)\in\mathbb{Q}[x]$为一个4次首一不可约多项式，其根为$\alpha,\beta,\gamma,\delta$。

1. 通过计算证明$\alpha\beta+\gamma\delta$,$\alpha\gamma+\beta\delta$,$\alpha\delta+\beta\gamma$是一个首一三次多项式$g(x)\in\mathbb{Q}[x]$的根,且二者判别式满足$disc(g)=disc(f)$。

2. 证明f在$\mathbb{Q}$上的$Galois$群必然是如下五个群之一 $S_4,A_4,Z_4,D_8,Z_2\times Z_2$

3. 对于上面的哪些群，g是不可约的？

提示:

1. 第一问通过直接计算得到$g(x)=x^3-a_2x^2+(a_1a_3-4a_4)x+(a_4(a_1^2-2a_2)+a_3^2-2a_2a_4)$

2. $g(x)$不可约当且仅当$Galois$群作用在集合$\{\alpha\beta+\gamma\delta,\alpha\gamma+\beta\delta,\alpha\delta+\beta\gamma\}$上是传递的。

问题 97 (北大代数学I实验班2022期末). 证明多项式x^4+1在任何一个正特征域上是可约多项式。

提示：去证明x^4+1对于任何一个素数p都是在$\mathbb{F}_{p^2}$上完全分裂的。然后通过x^4+1在任何$\mathbb{F}_p$上的分裂域至多$deg2$来说明矛盾。

问题 98 (北大代数学I实验班2022期末). 令F是一个域，$f(x)\in F[x]$是不可约多项式。设K是$f(x)$在F上的分裂域，并假设存在某个元素$\alpha\in K$使得$\alpha,\alpha+1$都是$f(x)$的根。

1. 证明F的特征不能为0。

2. 证明存在某个K/F的中间域E使得$[K:E]$等于F的特征。

提示：

1. 试着说明$f(x)$整除$f(x)-f(x-1)$，据此说明这只可能在正特征情形下发生，请思考这里如何应用到$f(x)$不可约。

2. 首先说明$f(x)=g(x^p)$, 并令$g(x)$在K内的分裂域为L，在$L[x]$中$g(x)=(x-\alpha_1)...(x-\alpha_r)$，然后去说明从$K$变为$L$只需要加入$\alpha_1^{1/p},...,\alpha_r^{1/p}$，然后考虑$K(\alpha_1^{1/p},...,\alpha_{r-1}^{1/p})$即可。

问题 99 (北大代数学I实验班2022期末). 设p是一个素数，q为p的幂次，设$\mathbb{F}_q$为含有q个元素的有限域，$\mathbb{F}_{q^n}$为其次数为n的有限扩张。

1. 证明q-*Frobenius*元素$\sigma(x)=x^q$是循环群$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$的生成元。

2. 考虑范数映射 $N:\mathbb{F}_{q^n}\to\mathbb{F}_q$

$$N(x)=x\sigma(x)\sigma^2(x)...\sigma^{n-1}(x)$$

证明N是满射。

3. 证明$N^{-1}(1)$作为$\mathbb{F}_q$-线性空间生成$\mathbb{F}_{q^n}$

提示：

1. 去说明$\langle\sigma\rangle$是阶为n的群，于是得到$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)=\langle\sigma\rangle$

2. 计数$\mathrm{Ker}\,N$中的元素为$1+q+q^2+...+q^{n-1}$，因此$\mathrm{Im}(N)$中的元素个数为$q-1$，据此说明满射。

3. 通过计数$N^{-1}(1)$中的元素个数说明矛盾。

问题 100 (北大代数学I实验班2022期末). 设$\mathbb{Q}\subset K_1\subseteq K_2\subseteq...\subseteq K_n$是$\mathbb{C}$中的一列域扩张，使得对于每个$i\geq 0$，$K_{i+1}$是$K_i$的三次*Galois*扩张，请证明$\mathbb{Q}(\sqrt[3]{2})$不包含在$K_n$中。

提示：考虑$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$的正规闭包，其扩张的次数是*3*的幂次吗*?*

问题 101. 本题目中我们构造一个*Galois*群为$\mathbb{Z}_7\rtimes\mathbb{Z}_3$的*Galois*扩张。

1. 给出两个不同的映射$\varphi_1,\varphi_2:\mathbb{Z}_3\to\mathbb{Z}_7$，并说明它们给出的半直积$\mathbb{Z}_7\rtimes_{\varphi_1}\mathbb{Z}_3$和$\mathbb{Z}_7\rtimes_{\varphi_2}\mathbb{Z}_3$是同构的，这使得$\mathbb{Z}_7\rtimes\mathbb{Z}_3$没有疑义。

2. 证明$\sqrt[7]{5}$在$\mathbb{Q}$上的分裂域同构于$\mathbb{Z}_7\rtimes(\mathbb{Z}/7\mathbb{Z})^\times$

3. 找一个E的子域F使得$\mathrm{Gal}(E/F)\cong\mathbb{Z}_7\rtimes\mathbb{Z}_3$

提示：

1. 为证明同构，可以把得到的半直积写成生成元和生成关系的形式，它们是

$$\langle \tau, \sigma | \tau^7 = 1, \sigma^3 = 1, \sigma\tau\sigma^{-1} = \tau^2 \rangle$$

$$\langle \tau', \sigma' | \tau'^7 = 1, \sigma'^3 = 1, \sigma'\tau'\sigma'^{-1} = \tau'^4 \rangle$$

然后证明它们同构，这可以通过直接给出映射来说明。

2. 分裂域E实际上是$\mathbb{Q}(\sqrt[7]{5}, \zeta_7)$

3. 利用$Galois$对应，选择的子域是$F = \mathbb{Q}(\sqrt{-7})$

问题 102. 请找到$S = \mathbb{C}[x,y]/(x,y)^2$的三个理想$I, J, K$，使得$I \cap (J+K) \neq (I \cap J) + (I \cap K)$。

提示（原题的$Hint$）：你可以将$(x,y)/(x,y)^2$视为$\mathbb{C} \cong \mathbb{C}[x,y]/(x,y)$上的$2$维线性空间。

提示：选择$(x), (y), (x+y)$即可。

注记：事实上，对于主理想整环R，都会有$I \cap (J+K) = (I \cap J) + (I \cap K)$，左边包含于右边是平凡的，而反过来需要用到$PID$的性质，使用最大公约数和最小公倍数算一算。

问题 103. 令$F \subseteq E$是特征为0的域，并且假设$0 \neq \alpha \in E$，并且$E = F(\alpha)$，假设存在N使得$\alpha^N \in F$，并令n是满足上述条件最小的正整数。

1. 请证明任一满足条件的正整数$m > 0$都是n的倍数。

2. 假如E中的单位根均落在F中，证明$[E:F] = n$

提示：

1. 使用带余除法。

2. 通过说明扩张次数$d = [E:F] \geq n$和$d = [E:F] \leq n$，一个重要的观察是α的极小多项式的所有根都形如$\alpha\zeta_j$，其中ζ_j是某个n次单位根。

问题 104. 设F是一个域,$f(x)$是一个不可约多项式，其在F上的分裂域为E，选取$\alpha \in E$使得$f(\alpha) = 0$，此外，对于某个固定的整数$n \geq 1$，设$g(x)$是$\mathbb{F}[x]$中的一个不可约多项式，使得$g(\alpha^n) = 0$

1. 证明$\deg(g)$整除$\deg(f)$，且$\deg(f)/\deg(g) \leq n$。

2. 证明若上述不等式取等，且F的特征不整除n，证明E包含一个n次单位根。

提示：

1. 去证明$\deg(f) = [F(\alpha) : F(\alpha^n)] \cdot \deg(g)$

2. 先说明$f(x) = cg(x^n)$, 然后说明如果α是$f(x)$的一个根，那么$\alpha\zeta$也是$f(x)$的一个根，其中ζ代表了某个n次单位根。

问题 105. 令K是域F的有限*Galois*扩张，它的*Galois*群为G，假设有一个中间域$E \neq F$使得任何一个中间域$E' \neq F$都满足$E \subseteq E'$，证明G是一个循环群且它的阶是素数的幂次。

提示：使用*Galois*理论翻译为“一个有唯一极大真子群的有限群必然是循环群”，这是通过选择不包含于极大真子群H的元素x并考虑其生成的循环群来说明，另外若阶不是素数的幂次，可以具体构造出两个极大真子群。

4 Hurwicz 定理的证明 (ENS)

问题 106. 我们考虑 $\mathbb{R}[x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n]$ 中的形如

$$(x_1^2 + x_2^2 + \cdots + x_n^2)(y_1^2 + y_2^2 + \cdots + y_n^2) = z_1^2 + z_2^2 + \cdots + z_n^2$$

的恒等式，其中 z_i 是 x_j 和 y_k 的实系数线性组合。*Hurwicz* 证明了，如果这样的恒等式存在，那么 $n = 1, 2, 4, 8$。

A 第一部分

设 $m, n > 1$ 为正整数，其中 m 为奇数。设 $g_1, g_2, \cdots, g_m$ 是 $\mathbf{GL}(n, \mathbb{C})$ 中的元素，满足 $g_i g_j = -g_j g_i$ 对所有 $i \neq j$ 成立。

本部分中，我们将证明 $n \equiv 0 \pmod{2^{\frac{m-1}{2}}}$。我们记 G 为 $\mathbf{GL}(n, \mathbb{C})$ 中由 $g_1, g_2, \cdots, g_m$ 生成的子群。我们首先确定 G 的中心 $Z(G)$ 以及 G 的导出子群 $\mathbf{D}(G)$。对于 $I \subseteq \{1, 2, \cdots, m\}$，设 $I = \{i_1, i_2, \cdots, i_k\}$ 并且 $i_1 < i_2 < \cdots < i_k$。我们记 $g_I = g_{i_1} g_{i_2} \cdots g_{i_k}$，约定 $g_\varnothing = I_n$。记 $\eta = g_{1,2,\cdots,m} = g_1 g_2 \cdots g_m$。我们将使用记号 $a = \pm b$ 表示 $a = b$ 或者 $a = -b$。

A1) 在 $m = 3, n = 2$ 的时候给出满足题目关系的一个 G 的例子。

A2) 对于 $I, J \subseteq \{1, 2, \cdots, m\}$，记 $K = (I \cup J) \backslash (I \cap J)$，证明：$g_I g_J = \pm g_K$。

A3) 证明：$G = \{\pm g_I \mid I \subseteq \{1, 2, \cdots, m\}\}$，并且对于所有 $g \in G$，$g^2 = \pm I_n$。

A4) 设 $I \subseteq \{1, 2, \cdots, m\}$，证明：$g_i g_I g_i^{-1} = (-1)^{|I|} \varepsilon g_I$，其中

$$\varepsilon = \begin{cases} -1, & i \in I; \\ 1, & i \notin I. \end{cases}$$

A5) 证明：如果 $g = \pm g_I$，其中 $|I| \neq 0$ 或者 m，则 g 所在共轭类为 $\{g, -g\}$。如果 $I = 0$ 或者 $I = m$，则 $g \in Z(G)$。

A6) 证明：$Z(G) = \{\pm I_n, \pm\eta\}$。根据 $\eta = I_n$ 与否，$|Z(G)| = 2$ 或者 $|Z(G)| = 4$。

A7) 证明：$|G| = 2^{m-1}|Z(G)|$，并且 G 中每个元素可以唯一写为 zg_I，其中 $z \in Z(G)$，$I \subseteq \{1, 2, \cdots, m-1\}$。

A8) 证明：G 的共轭类个数为

$$|Z| + \frac{|G| - |Z|}{2} = 2^{m-2}|Z| + \frac{|Z|}{2}.$$

A9) 证明：$\mathbf{D}(G) = \{\pm I_n\}$。

A10) 证明：恰好存在 $\frac{|G|}{2} = 2^{m-2}|Z(G)|$ 个 $G \to \mathbb{C}^*$ 的群同态。

A11) 证明：方程 $2^m = a^2 + b^2$ 的唯一解为 $a = b = 2^{\frac{m-1}{2}}$，其中 $a, b \geqslant 1$ 为正整数。

A12) 证明：在同构意义下，G 有 $\frac{|Z|}{2}$ 个维度大于 1 的不可约表示，并且它们的维度为 $2^{\frac{m-1}{2}}$。

A13) 证明：在 $\mathbb{C}^n$ 上，没有 G 的共同特征向量。

A14) 证明：$2^{\frac{m-1}{2}}$ 整除 n。

B 第二部分

我们在 $\mathbb{R}^n$ 上考虑 Euclidean 范数。假设存在 $\mathbb{R}^n$ 上的乘法 $\star$ 满足 $\|x \star y\|^2 = \|x\|^2\|y\|^2$，我们希望证明 $n = 2, 4, 8$。我们固定一组标准正交基 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$。

B1) 给出 $n = 2$ 和 $n = 4$ 的例子，并描述构造 $n = 8$ 的例子的方法。

B2) 对于 $x \in \mathbb{R}^n$，我们考虑 $m_x : y \mapsto x \star y$，并记 $M(x)$ 为 m_x 在给定标准正交基下的矩阵。证明：

$$^tM(x)M(x) = \|x\|^2 I_n.$$

B3) 由此推出 $M(\varepsilon_i) \in \mathbf{O}(n)$ 对所有 $i = 1, 2, \cdots, n$ 成立，并且

$$^tM(\varepsilon_i)M(\varepsilon_j) + {}^tM(\varepsilon_j)M(\varepsilon_i) = 0,$$

对所有 $i \neq j$ 成立。

B4) 设 $g_i = M(\varepsilon_i)^t M(\varepsilon_n) \in \mathbf{O}(n)$，其中 $i < n$。证明：$g_i^2 = -I_n$ 并且 $g_i g_j = -g_j g_i$ 对所有 $i \neq j$ 成立。

B5) 证明 Hurwicz 定理。

5 一些小题

问题 107 (ENS). 我们考虑 $SL(2,\mathbb{Z})$ 中的矩阵 M。

1. 如果 $\mathrm{ord}(M) = 4$，则在 $GL(2,\mathbb{Z})$ 中与

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

共轭。

2. 如果 $\mathrm{ord}(M) = 3$，则在 $GL(2,\mathbb{Z})$ 中与

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

共轭。

问题 108 (ENS). 假设 $A \in GL(n,\mathbb{Z})$，如果对于某个所有根均为单根并且模长不大于1的 $P \in \mathbb{C}[X]$，有 $P(A) = 0$，证明：$A = 0$。

问题 109 (ENS). 设 $p > 2$ 为素数，n 为正整数，证明：从 $GL(n,\mathbb{Z})$ 到 $GL\left(n, \mathbb{Z}/p\mathbb{Z}\right)$ 的自然映射为单射。

问题 110 (ENS). 证明：$GL(n,\mathbb{Z})$ 在同构意义下只有有限多种子群。

问题 111 (ENS). 设 $p > 2$ 为素数，考虑 $M \in GL(2, \mathbb{Z}/p\mathbb{Z})$，如果 M 给出 $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$ 上的一个置换，求 $\det M$。

问题 112 (ENS).

1. 计算 $GL\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ 和 $SL\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ 的阶数。

2. 证明：不存在 $SL\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ 到 $\mathbb{Z}/2\mathbb{Z}$ 的满同态。

3. 证明：$SL\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ 不存在 12 阶子群。

4. 证明：存在 $SL\left(2,\mathbb{Z}/3\mathbb{Z}\right)$ 到 $\mathfrak{A}_4$ 的满同态。

问题 113 (ENS). 假设 $A=\mathbb{Z}/2^n\mathbb{Z}$，考虑群 $G=SL(2,A)$。证明：G 中元素的阶不会大于 $3\times 2^{n-1}$。

问题 114 (X). G 是一个有限群，$|G|=m$，$\phi\in\mathrm{Aut}(G)$ 是一个自同构，满足

- 如果 $\phi(g)=g$，则 $g=e$，即 ϕ 没有非平凡的不动点；
- 对于某个正整数 $n\neq m$，$\phi^n=\mathrm{id}_G$。

1. 计算 $g\phi(g)\phi^2(g)\cdots\phi^{n-1}(g)$；

2. 如果 $n=2$，证明：G 是交换群；

3. 如果 $n=3$，证明：$g\phi(g)=\phi(g)g$ 对任意 $g\in G$ 成立。

问题 115 (ENS). 我们不诉诸于 *Sylow* 定理来证明 *Cauchy* 定理。

1. 假设 G 是一个 p-群，并且 G 作用在有限集 E 上。记

$$E^G=\{x\in E\mid g\cdot x=x,\forall g\in G\},$$

证明：$|E^G|\equiv|E|\pmod p$。

2. 假设 H 是一个有限群，p 是一个素数并且整除 H 的阶数。证明：H 中有 p 阶元素。（提示：考虑 $\mathbb{Z}/p\mathbb{Z}$ 在 $\{(x_1,x_2,\cdots,x_p)\in H^p\mid x_1x_2\cdots x_p=e\}$ 上的作用）

问题 116 (X). 假设 G 是一个有限群，考虑 $E=\{(x,y)\in G^2\mid xy=yx\}$，若 $|E|>\frac{5}{8}|G|^2$，证明：G 是交换群。

问题 117 (ENS). 假设 G 是一个无限群，$H<G$ 是一个子群，并且 $[G:H]=\infty$。若

$$H\cup H_1\cup H_2\cup\cdots\cup H_n=G,$$

证明：

$$H_1\cup H_2\cup\cdots\cup H_n=G.$$

问题 118 (ENS). *1.* 假设 G 是一个有限群，$H<G$ 是一个真子群。证明：存在 $x\in G$，使得 x 所在共轭类 C_g 与 H 无交。

2. 如果去掉 G 为有限群的条件，请举出反例说明上述结论不再正确。

问题 119 (X)**.** 假设 $G < O(3)$ 是三维正交群的一个有限子群。考虑 $\mathcal{T} = \{Gx : x \in \mathbb{S}^2\}$，其中 Gx 是 x 在 G 作用下的轨道。

1. 证明：如果 $y \in Gx$，则 $|\mathrm{Stap}_G(x)| = |\mathrm{Stab}_G(y)|$，所以 $\nu(T) = |\mathrm{Stab}_G(x)|$ 是 $\mathcal{T}$ 上的良定义的函数，其中 $T = Gx$。

2. 证明：
$$2|G| - 2 = \sum_{T \in \mathcal{T}} |T|(\nu(T) - 1).$$

3. 找到 $\nu(T)$ 的所有可能值。

问题 120 (ENS)**.** 对于群 G，令 C 为由 $\{g^2 \mid g \in G\}$ 生成的子群，D 为导群。

1. 证明：$D < C$。

2. 证明：如果 $G = \langle x \mid x^2 = e \rangle$，即 G 由对合元素生成，则 $C = D$。

3. 对于 $G = O(2, \mathbb{Q})$，证明：D 是 $SO(2, \mathbb{Q})$ 的真子群。

问题 121. 假设 G 是 $\mathfrak{S}_p$ 的一个子群，其中 p 是素数。证明：存在 G 到 $\mathbb{Z}/p\mathbb{Z}$ 的同态当且仅当 G 平凡或者由一个 p-循环生成。

问题 122 (ENS)**.** 假设 $P \subseteq \mathbb{Z}^2$ 是一个非空子集，记
$$-P = \{(-x, -y) \mid (x, y) \in P\},$$
$$P + Q = \{(a + c, b + d) \mid (a, b) \in P, (c, d) \in Q\}.$$
试找出所有集合 P 满足

1. $P \cup (-P) = \mathbb{Z}^2$,

2. $P \cap (-P) = \{0\}$,

3. $P + P \subseteq P$.

问题 123. 假设 A 是一个（不一定交换的）环，并且 $x^3 = x$ 对于所有 $x \in A$ 成立。

1. 找出 A 的所有幂零元。

2. 如果 $e \in A$ 是幂等元，即 $e^2 = e$，证明：$ea = ae$ 对所有 $a \in A$ 成立。因此 $a^2 \in Z(A)$ 对于所有 $a \in A$ 成立。
（提示：考虑 $b = ea(1 - e)$，并计算 b^2）

3. 证明 A 是交换环。

问题 124 (ENS)**.** 我们称一个环 A 是**正规的**，如果对于任意 $a \in A$，存在 $u \in A$，使得 $aua = a$。

1. 是否所有除环都是正规的？$\mathbb{Z}$ 是正规的吗？

2. 找出 $\mathbb{Z}/n\mathbb{Z}$ 是正规环的充要条件。

3. 假设 K 是一个域，证明：$M_n(K)$ 是正规的。对于

$$J = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ & 0 & 1 & \cdots & 0 & 0 \\ & & \ddots & & \vdots & \vdots \\ & & & \ddots & \vdots & \vdots \\ & & & & 0 & 1 \\ & & & & & 0 \end{pmatrix},$$

找到对应的 U。

4. 证明：正规环的中心是正规的。

问题 125 (ENS)**.** 给定正整数 k，我们定义数列

$$s_n = \frac{1}{4} \sum_{\substack{a \in \mathbb{Z}[i] \\ a\bar{a} = n}} a^k.$$

1. 证明：$s_n \in \mathbb{Z}$，并且如果 k 不是 4 的倍数，那么 $s_n = 0$。

2. 对于 $k = 4$，计算 s_5, s_{13}, s_{65}。

3. 证明：如果 $(m, n) = 1$，那么 $s_m s_n = s_{mn}$。

问题 126. 我们考虑 A 作为 $\mathbb{C}^{(1,\infty)}$ 的子集，其中

$$A = \{x \mapsto P(x) + Q(x)\sqrt{x^2 - 1} \mid P, Q \in \mathbb{C}[X]\}.$$

1. 证明：A 是一个环，并且每个 $z \in A$ 唯一决定了 P, Q 使得 $z = P(x) + Q(x)\sqrt{x^2 - 1}$。

2. 证明：$z = P(x) + Q(x)\sqrt{x^2 - 1} \in A$ 是单位，当且仅当 $N(z) = P(X)^2 - Q(X)^2(X^2 - 1) \in \mathbb{C}^*$。

3. 证明：存在 $z_0 \in A$，使得

$$U = \{z \in A \mid N(z) = 1\} = \{\pm z_0^n \mid n \in \mathbb{Z}\}.$$

4. 找到所有满足 $(P, Q) \in \mathbb{C}[X]^2$，使得 $P(X)^2 - Q(X)^2(X^2 - 1)$。

问题 127. 假设 A 是一个环，我们称 $\nu : A \to \mathbb{R} \cup \{\infty\}$ 是 A 上的一个赋值，如果

1. $\nu(xy) = \nu(x) + \nu(y)$，

2. $\nu(x + y) \geqslant \min\{\nu(x), \nu(y)\}$，

3. $\nu(x) = \infty$ 当且仅当 $x = 0$。

请找出 $\mathbb{Q}$ 上的所有赋值。

问题 128. 假设 K 是一个域，并且 $\mathrm{char}(K) = 0$，我们称一个函数 $|\cdot| : K \to \mathbb{R}_+$ 是一个 **绝对值**，如果对于 $x, y \in K$，

- $|x| = 0$ 当且仅当 $x = 0$；
- $|xy| = |x||y|$，即 $|\cdot|$ 是乘性的；
- $|x + y| \leqslant |x| + |y|$，即 $|\cdot|$ 满足三角不等式。

1. 对于特征 0 的域，我们可以视 $\mathbb{Q}$ 为其子域。如果 K 上的绝对值 $|\cdot|$ 满 $|n| \leqslant 1$ 对所有正整数成立，证明：$|\cdot|$ 是一个超距离（*ultra-metric*），即

$$|x + y| \leqslant \max\{|x|, |y|\}.$$

2. 对于 $\mathbb{C}(X)$ 上的绝对值 $|\cdot|$，如果 $|z| = 1$ 对所有 $z \in \mathbb{C}^*$ 成立，证明：以下可能性必居其一：

(a) $|f| = 1$ 对所有非零元素成立；

(b) 对于某 $a > 1$，$|f| = a^{\deg f}$ 对所有非零元素成立；

(c) 对于某 $a < 1$，$|f| = a^{\mathrm{val}\, f}$ 对所有非零元素成立，其中对于多项式 $P(X)$fi $\mathrm{val}\, P$ 为 $X = 0$ 作为 P 的根的重数；$\mathrm{val}\, \frac{P}{Q} = \mathrm{val}\, P - \mathrm{val}\, Q$。

问题 129 (X)**.** 在域 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ 中，我们考虑

$$s_k = \sum_{x \in \mathbb{Z}_p} x^k,$$

证明：s_k 等于 0 或者 -1，并得出 $s_k = 0$ 的充要条件。

问题 130. 证明：$\mathbb{R}[X^2, X^3] \ncong \mathbb{R}[X]$。

问题 131. *1.* 找到所有多项式 $P \in \mathbb{C}[X]$，使得存在正整数 p, q，$(P')^p \mid P^q$。

2. 在一般的特征 0 的域的多项式环上考虑上一问题。

问题 132 (X)**.** 对于多项式 $P, Q \in \mathbb{C}[X]$，如果 P 和 Q 具有相同的根（不计重数），并且 $P-1$ 和 $Q-1$ 也有相同的根（不计重数），证明：$P = Q$。

问题 133 (ENS)**.** 如果 $a_1, a_2, \cdots, a_n \in \mathbb{Z}$ 两两不同，其中 $n \geqslant 2$，证明：

$$P(X) = (X - a_1)(X - a_2) \cdots (X - a_n) - 1$$

在 $\mathbb{Z}[X]$ 中不可约。

问题 134. 分类所有多项式 $P \in \mathbb{C}[X]$，使得 $\mathbb{Q} \subseteq P(\mathbb{Q})$。

问题 135. 假设 K, L 是特征不为 2 的域，L/K 为 *Galois* 扩张并且扩张的 *Galois* 群为 K_4。证明：存在 $a, b \in K$，$L = K(\sqrt{a}, \sqrt{b})$。

问题 136. 我们希望研究所有满足以下条件的实系数多项式 P：

- P 的系数只有 $-1, 0, 1$；
- P 在 $\mathbb{R}$ 上分裂。

1. 证明：对于 $a_1, a_2, \cdots, a_n > 0$，

$$\sum_{1 \leqslant i, j \leqslant n} \frac{a_i}{a_j} \geqslant n^2.$$

2. 证明：$\deg P \leqslant 3$，从而找出所有满足条件的 P。

问题 137 (X)**.** 设 $P \in \mathbb{C}[X]$ 有单根 $z_1, z_2, \cdots, z_n$，求

1.

$$\sum_{k=1}^{n} \frac{1}{z_k P'(z_k)},$$

2.

$$\sum_{k=1}^{n} \frac{1}{P'(z_k)}.$$

问题 138. 设 A 为整环，证明：$A[X]$ 是 *PID* 当且仅当 A 是域。

问题 139. 证明：$\mathbb{C}[X, Y]/(X^3 - X - Y^2)$ 不是 *UFD*。

问题 140. 找到最小的 n，使得第 n 个分圆多项式的系数并非只有 $1, 0, -1$。

问题 141. 证明：多项式 $X^5 - X + 1 \in \mathbb{F}_{25}[X]$ 是不可约的。(提示：考虑 $\mathbb{F}_{25} = \mathbb{F}_5[X]/(X^2 + X + 1)$)

6 一些杂题

A 有限域上的二次型

我们考虑特征不为 2 的域 K，以及有限维 K-线性空间 E。其中 $\dim(E) = n$。设 q 为 E 上的二次型。

A1) 证明：存在 E 的一组基 $(e^i)_{i=1}^n$ 使得存在 $(a_i)_{i=1}^n \in K^n$ 满足

$$q\left(\sum_{i=1}^n x_i e^i\right) = \sum_{i=1}^n a_i x_i^2.$$

A2) 假设对于任意 $(a, b) \in (K^\times)^2$，方程 $ax^2 + by^2 = 1$ 在 K^2 中有解，并假设 q 是非退化的。证明：存在 E 的一组基和 $\alpha \in K$ 使得

$$q\left(\sum_{i=1}^n x_i e^i\right) = \sum_{i=1}^{n-1} x_i^2 + \alpha x_n^2.$$

A3) 假设 $K = \mathbb{F}_q$，q 为奇数。证明：K 满足上小题条件。

A4) 在商掉合同关系的意义下，分类 $\mathbb{F}_q$ 上所有非退化二次型。

B 一个非单扩张

设 K 是特征为 $p > 0$ 的域。考虑 $L = K(X, Y)$，$M = K(X^p, Y^p) \subseteq L$。

B1) 证明：$[L : M] = p^2$。

B2) 证明：对于 $P \in K[X, Y]$，$\frac{1}{P} = \frac{P^{n-1}}{Q}$，其中 $Q \in K[X^p, Y^p]$。

B3) 证明：对于任意 $x \in L \backslash M$，$[M(x) : M] = p$。

C 66 阶群的分类（Lyon）

假设 G 是一个 66 阶的群。

C1) 证明：G 有唯一的 11 阶子群。

C2) 证明：G 有唯一的 33 阶子群。

C3) 证明：G 有唯一的 3 阶子群。

C4) 证明：G 是 $\mathbb{Z}_{33}$ 与 $\mathbb{Z}_2$ 的半直积。

C5) 证明：将 $\mathrm{Aut}(\mathbb{Z}_{33})$ 写成循环群的直积。

C6) 找出 $\mathrm{Aut}(\mathbb{Z}_{33})$ 的所有二阶元，并分类所有 66 阶群。

D 一个不可约多项式（Lyon）

我们将证明 $\mathbb{Z}[X]$ 中的多项式 $P(X)$ 是不可约的。其中

$$P(X) = X^9 + 15X^8 - X^3 - 3X^2 + 9X + 23.$$

D1) 证明：$X^3 - X - 1$ 在 $\mathbb{F}_3[X]$ 中不可约。

D2) 证明：考虑 $X^4 + X + 1 \in \mathbb{F}_2[X]$ 中的一个根 α，证明：$\alpha \in \mathbb{F}_16$ 但是 $\alpha \notin \mathbb{F}_4$。从而证明 $X^4 + X + 1 \in \mathbb{F}_2[X]$ 是不可约的。

D3) 证明：$X^3 - X - 1$ 在 $\mathbb{F}_3[X]$ 中不可约。

D4) 在 $\mathbb{F}_2[X]$ 和 $\mathbb{F}_3[X]$ 中分解 $P(X)$ 的像。

D5) 证明 $P(X)$ 在 $\mathbb{Z}[X]$ 中不可约。

E 147阶群的分类（Lyon）

E1) 证明存在唯一的 7-Sylow 子群 K，并且它在 G 中正规。证明 K 只能同构于两个经典群中的一个，并描述它。

E2) 计算 $(\mathbb{Z}/49\mathbb{Z})^\times$ 的阶。

E3) 固定 $(\mathbb{Z}_{49})^\times$ 的一个生成元 g。分类其中所有三阶元。

E4) 证明 $(\mathbb{Z}/7\mathbb{Z})^2$ 的自同构群同构于 $GL_2(\mathbb{F}_7)$。

E5) 证明 $GL_2(\mathbb{F}_7)$ 中所有 3 阶矩阵都是可对角化的（可通过解 $X^3-1=0$ 在 $\mathbb{F}_7$ 中的根来完成）。从而推导出所有 3 阶矩阵在 $GL_2(\mathbb{F}_7)$ 中分成五个共轭类。

E6) 最后得出结论：至多存在 6 种不同构的 147 阶群。

E7) （附加题）存在 6 种不同构的 147 阶群。

F $GL_4(\mathbb{F}_2)$ 的结构（Lyon）

F1) 在交错群 $\mathfrak{A}_{n+2}$ 中，计算

$$\alpha = (12i)(12j), \quad 3 \le i, j \le n+2,\ i \ne j,$$

然后计算 $\alpha(12k)\alpha^{-1}$，其中 $k \notin \{1,2,i,j\}$。从而推导出 3-轮换 $(12i), 3 \le i \le n+2$ 生成 $\mathfrak{A}_{n+2}$。

F2) 记 $G_n = \langle x_1, \dots, x_n \mid x_i^3 = 1,\ \forall i;\ (x_i x_j)^2 = 1,\ i \ne j \rangle$。证明存在一个满同态 $G_n \to \mathfrak{A}_{n+2}$。

F3) 设 $H \le G_n$ 是由 x_i 生成的子群，其中 $1 \le i \le n-1$。证明集合

$$H \cup x_n H \cup x_n^2 H \cup x_1 x_n H \cup \cdots \cup x_{n-1} x_n H$$

在 x_i 左乘下封闭。然后推导出该集合就是整个 G_n。

(关于乘法封闭性，可以只做一些提示性的计算，只要足够令人信服即可。)

F4) 用归纳法（商集 G_n/H 的大小），证明 $G_n \simeq \mathfrak{A}_{n+2}$。

F5) 证明 $GL_4(\mathbb{F}_2)$ 的阶等于 $\mathfrak{A}_8$ 的阶。

F6) 证明群同构 $GL_4(\mathbb{F}_2) \simeq \mathfrak{A}_8$，其中考虑 $GL_4(\mathbb{F}_2)$ 中的以下矩阵：

$$b_1 = \begin{pmatrix} Z & 0 \\ 0 & Z^2 \end{pmatrix}, \quad b_2 = \begin{pmatrix} Z^2 & 0 \\ I & Z \end{pmatrix}, \quad b_3 = \begin{pmatrix} J_1 & I \\ I & J_2 \end{pmatrix}, \quad b_4 = {}^t b_2, \quad b_5 = \begin{pmatrix} K_1 & I \\ I & K_2 \end{pmatrix}, \quad b_6 = {}^t b_5,$$

其中

$$Z=\begin{pmatrix}0&1\\1&1\end{pmatrix},\quad J_1=\begin{pmatrix}1&0\\0&0\end{pmatrix},\quad J_2=\begin{pmatrix}0&0\\0&1\end{pmatrix},\quad K_1=\begin{pmatrix}0&0\\0&1\end{pmatrix},\quad K_2=\begin{pmatrix}1&0\\1&0\end{pmatrix}.$$

G X^4+1 在有限域中可约（Lyon）

考虑 p 为素数，我们将证明 $P(X)=X^4+1$ 在 $\mathbb{F}_{p^n}$ 中总是可约的。

G1) 证明当 $p=2$ 时结论成立。接下来假设 p 为奇素数。

G2) 证明：如果 a,b 是两个正整数且 $b\mid a$，那么环 $\mathbb{Z}_a$ 中存在一个阶为 b 的元素。

G3) 证明：乘法群 $\mathbb{F}_{p^2}^\times$ 中至少含有一个阶为 8 的元素。由此推导出多项式 X^4+1 在 $\mathbb{F}_{p^2}$ 中有一个根 α。

G4) 证明：对所有素数 p，多项式 X^4+1 在 $\mathbb{F}_p$ 上可约。（提示：考虑 α 在 $\mathbb{F}_p$ 上的极小多项式的次数）

G5) 得出结论。

H $SL_2(\mathbb{F}_3)$ 的结构（Lyon）

H1) 计算 $SL_2(\mathbb{F}_3)$ 的阶数。

我们记 $SL_2(\mathbb{F}_3)$ 的 Sylow-2 子群为 H_8。

H2) 描述群 H_8。计算 $GL_2(\mathbb{F}_3)$ 的阶以及 $SL_2(\mathbb{F}_3)$ 的阶。找出其阶为 2 的元素。证明阶为 4 的元素的特征多项式为 X^2+1，并找出所有这些元素。

H3) 证明群同构 $SL_2(\mathbb{F}_3)\simeq H_8\rtimes\mathbb{Z}_3$。（提示：首先证明 $SL_2(\mathbb{F}_3)$ 只有唯一的 2-Sylow 子群）