# 代数 IV 习题课讲义

**（无解答）**

中法数学英才班

授课教师: 许金兴

汇编整理: 王政 林斌

中国科学技术大学数学系

2023 年 4 月 18日

我的长诗题为《宗教大法官》，作品很荒唐，可是我想让你知道。

——《卡拉马佐夫兄弟》

# 前言

这份讲义的主体来自许金兴[1]老师在 2022 年春季学期开设的代数 IV 习题课。前半学期的主题为交换代数, 对应的正课教授为 David Alexandre RENARD[2]；后半学期的主题为 Galois 理论, 对应的正课教授为 Christophe Marie Jean MARGERIN[3]。限于正课时长, 这两个主题都没有机会在正课上深入，但这一遗憾在习题课中得到了一定程度上的弥补：许金兴老师补充了更多深入理论，如环（模）的局部化、Dedekind 整环、群上同调、伴随素理想、Galois 下降法等内容。于习题课的习题之外, 我们还整理了三次口试（同样由许金兴老师负责）和期中、期末两次考试中出现的题目（两次考试题目的原文为法语, 我们尽可能准确地翻译为了中文）以供参考，以时间顺序穿插在了习题课讲义中（2022-04-27 的讲义放在 2022-04-29 期中考试前是为了保持内容上的连贯性）。

本讲义的部分解答来自我的课堂笔记。必须指出的是，习题课的时长并不支持许老师在课堂上给出所有习题的解答（比如老师提供的六份阅读材料只能供同学课后参考），因此有相当多习题（这其中包括大多数较难的习题）的答案是在整理过程中给出的，这也是整理工作从 2022 年 7 月一直进行到 2023 年 4 月的一个原因。事实上最早只有我一人负责整理，但实在力所未逮，至 2022 年 9 月只完成了这份讲义的前 80 页，彼时的整理工作已接近停滞。所幸林斌同学在后来加入，他给出了相当多难题的证明（如代数不变量理论的所有六个习题、第三轮口试题目的习题 1.2等等），扫平了许许多多的障碍。没有林斌同学的帮助，这份讲义不可能如期完成。

其实直到今年寒假，我都不太确定能否在这学期内完成这份讲义。彼时我在准备所申院校的招生考试，林斌同学在做大创的论文，这份讲义又被搁置了许久。好在此后没有懈怠，努力在期中考试前结束了整理、编排工作。整项工作历时近十月，工作量大，繁琐劳神。事实上，我从一开始就没有采用一般的编排格式，导致讲义中的所有超链接都只能逐个手动添加。我本人也是第一次用 latex 编排正式稿件，此前的笔记或作业都是手写。尽管林斌同学已经纠正了我的大量格式错误，仍难免留下没有发现的问题，还望同学们见谅。

尽管欣喜难抑，也不宜再冗言。最后，衷心希望这份讲义能够帮助同学们更好地理解代数 IV 课程。祝同学们学习顺利！

[1] http://staff.ustc.edu.cn/ xujx02/
[2] https://perso.pages.math.cnrs.fr/users/david.renard/
[3] CMLS, École Polytechnique, F-91128 Palaiseau, France

**编排格式**　这份讲义按照讲义/习题/小问的格式编排，行距与排版尽可能与许金兴老师提供的习题文件保持一致。解答中引用同一题中的小问时我们会省略习题的编号，引用同一天讲义中的另一个习题时我们会省略讲义的日期，此外我们均会给出所引结论的具体位置。所有引用都提供了超链接。

**关于记号**　尽管整本讲义都是用中文编写，其中的一些记号还是遵从了法文习惯，如最大公约数的记号 $pgcd$( plus grand commun diviseur），域特征的记号 $Car$（Caractéristique)，环 $A$ 的可逆元集的记号 $A^{\times}$ 等。希望这不会造成太多的阅读障碍。

王政
2023 年 4 月 15 日

# 序

这份讲义是在 2021 年和 2022 年春季两次代数 IV 习题课教学过程中写成的。其主要目的是为两位法国老师（David Alexandre RENARD, Christophe Marie Jean MARGERIN）所教的正课提供更多的具体例子，补充更多的背景知识，以及介绍诸如局部化之类的常用技术。题目来源主要是两位法国老师提供的习题，历年丘赛试题，以及一些定理的证明过程所做的拆分。

贯穿整个讲义的一个例子是分圆整数环 $\mathbb{Z}[\zeta_N]$ 以及相应的分圆扩张 $\mathbb{Q}(\zeta_N)/\mathbb{Q}$. 在前半部分环与模中，通过考虑整扩张 $\mathbb{Z} \to \mathbb{Z}[\zeta_p]$, 证明了 $\mathbb{Z}[\zeta_p]$ 在每个非零素理想处的局部化为离散赋值环 (DVR), 进而利用整闭性质的局部性得到 $\mathbb{Z}[\zeta_p]$ 为整闭整环 (2022-03-16 习题 5)，其中判断和处理不分歧扩张和 Eisenstein 型完全分歧扩张的手法是经常用到的，值得通过这个具体例子反复体会。在后半部分，通过在 $\mathbb{Z}[\zeta_N]$ 的局部化这样的 DVR 上应用 Eisenstein 判别法，得到分圆多项式 $\Phi_N(x)$ 的不可约性，从而求出 $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ 的 Galois 群。从中我们能看到证明 $\Phi_N(x)$ 不可约，求出扩张次数 $[\mathbb{Q}(\zeta_N):\mathbb{Q}]$ 的下界，与尽可能多地找到 Galois 群 $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ 中的元素三者之间的等价性。而这三个问题又都有自己独特的处理思路 (Eisenstein 判别法，扩张次数的乘积性，Frobenius 元素的提升)，对这些联系的玩味也非常值得正在学习或刚学完这门课的同学去做。

讲义中的绝大部分内容都是标准的例子或命题，只有少数几个地方的处理可能有一些新意。2022-06-01 习题 6给出了域扩张下范数的乘积性的一个纯线性代数证明，其中的想法也曾编为 2022 年科大九章杯数学竞赛的一个题目。??中，通过基变换到代数闭域的方法，对 Galoi 扩张中的一些重要命题用统一的想法给出了证明，其本质是利用域的平展覆盖处理一阶平展上同调相关的问题。这样处理的好处是思路较为直接，并且同样的思路可以应用到类似的问题中。

授课时，讲义中的相当一部分题目并没有给出答案，并且有一些我也不会做，但是不少同学给出了自己独到的解法。比如 2022-04-11 习题 4，法国老师给的参考答案证明比较内蕴，较难理解背后的想法，这个纯矩阵的证明思路是在习题课课堂上跟同学们一起讨论得到的，其中的第二问当场并没有得到证明，课后林斌同学在 QQ 群中给出了第一问的表述和证明，从而整个题目解答形成了现在的形式。又比如期末考试的问题13.3，刘祎名同学给出的证明是他在暑假发给我的。相比于具体知识的学习，这种钻研问题的精神和热情更为宝贵。在习题课上，我深切体会到了教学相长的含义。不少同学在学习过程中展现了极大的热情，其中的很多材料 (如单形的同调群) 是为了更详细回应同学的课后问题所写的。所以这份讲义更应该看作是代数 IV 正课、习题课授课老师和 19 级、20 级两届同学们共同完成的。

感谢王政、林斌两位同学的整理以及对所有题目进行的详细解答和注记。希望这份讲义能对同学们学习代数 IV 有所帮助。

许金兴<br>2023 年 4 月 18 日

# 目录

# 2022-02-28 环的单位与素理想, 幂零多项式

例 **1.** 设 $R=\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$

*1.* 存在环同构 $\varphi\colon \mathbb{Z}[X]/(X^2-2)\xrightarrow{\sim}R$ , 使得 $\varphi(X)=\sqrt{2}$.

*2.* 利用商环的万有性质和多项式环的万有性质, 证明对任意交换环 $A$, 有以下集合之间的双射:

$$\mathrm{Hom}(R,A)\backsimeq\{a\in A\mid a^2-2=0\}.$$

并且在这个对应下, 如果 $a\in A, a^2=2$, 则其对应的同态将 $\sqrt{2}$ 映到 $a$.

*3.* $Aut(R)=\{id,\sigma\}$. 其中 $\sigma(a+b\sqrt{2})=a-b\sqrt{2}$.

*4.* 以下映射保持乘法

$$N\colon R\to\mathbb{Z}$$

$$a+b\sqrt{2}\mapsto(a+b\sqrt{2})\cdot\sigma(a+b\sqrt{2})=a^2-2b^2.$$

*5.* 设 $x\in R$, 则 $x\in R^*\Leftrightarrow N(x)=\pm1$.

*6.* 设 $x\in R^*$, 则 $\pm x$, $x^{-1}$ 均在 $R^*$ 中.

*7.* $1+\sqrt{2}\in R^*$.

*8.* 设 $x\in R^*$ 且 $1\leq x<1+\sqrt{2}$, 则 $x=1$.

*9.*$R^*=\{(1+\sqrt{2})^n\mid n\in\mathbb{Z}\}$.

例 **2.** 设 $R=\mathbb{Z}[i\sqrt{5}]=\{a+bi\sqrt{5}\mid a,b\in\mathbb{Z}\}$. 设 $p\in\mathbb{Z}$ 为素数.

*1.* 存在环同构 $\varphi\colon \mathbb{Z}[X]/(X^2+5)\xrightarrow{\sim}R$, 使得 $\varphi(X)=i\sqrt{5}$.

*2.* 有以下环同构:

$$R/(p) \simeq \mathbb{Z}[X]/(X^2+5,p) \simeq \mathbb{F}_q[X]/(X^2+5).$$

*3.* 如果 $X^2+5=0$ 在 $\mathbb{F}_p$ 上无解, 则 $(p)$ 为 $R$ 中极大理想.

*4.* 如果 $X^2+5=0$ 在 $\mathbb{F}_p$ 上有两个互异根, 则 $R$ 恰有两个包含 $p$ 的素理想 $\mathfrak{P}_1, \mathfrak{P}_2$. 并且对于 $i=1,2$, 有 $R/\mathfrak{P}_i \simeq \mathbb{F}_p$. 特别地, $\beta_i$ 为 $R$ 中极大理想.

*5.* 如果 $X^2+5=0$ 在 $\mathbb{F}_p$ 上有一个二重根, 则 $R$ 恰有一个包含 $p$ 的素理想 $\mathfrak{P}$, 并且 $(p) \subsetneq \mathfrak{P}$. 特别地, $\mathfrak{P}$ 为 $R$ 中极大理想.

*6.* 3 不是 $R$ 中素元, 即 $(3)$ 不是 $R$ 中素理想.

*7.* 以下映射保持乘法

$$N\colon R \to \mathbb{Z}$$

$$a+bi\sqrt{5} \mapsto a^2+5b^2$$

*8.* 对于 $x \in R, x \in R^* \Leftrightarrow N(x)=1$.

*9.* 3 是 $R$ 中不可约元.

*10.* 对任意 $R$ 中的素理想 $\mathfrak{P}, \mathfrak{P} \cap \mathbb{Z} \neq (0)$, 从而存在素数 $p \in \mathbb{Z}$, 使得 $\mathfrak{P} \cap \mathbb{Z} = (p)$. 特别的, $\mathfrak{P}$ 为 $R$ 中极大理想.(利用*3*,*4*,*5*)

注: 以上两例中, 将 $R$ 表示为 $\mathbb{Z}[X]/(f(X))$ 的形式, 确定 $R$ 的自同态 (自同构) 的方法, $N$ 的构造及用来确定 $R^*$, 以及利用 $\mathfrak{P}$ 包含素数 $p$ 在商环中进行分析的方法, 都是具有典型意义的, 需要熟练掌握并自如应用.

例 **3.** 设 $A$ 为交换环, $f(X)=a_0+a_1X+\cdots+a_nX^n \in A[X]$, 其中 $a_i \in A$.

*1.* 如果 $a_0 \in A^*, a_1, \cdots, a_n$ 均为幂零元, 则 $f(X) \in A[X]^*$.

*2.* 如果 $A$ 为整环且 $f(X) \in A[X]^*$, 则 $a_0 \in A*$.

*3.* 如果 $f(X) \in A[X]^*$, 则 $a_0 \in A^*$, 且对任意 $A$ 中素理想 $\mathfrak{P}, a_1, \cdots, a_n$ 均在 $\mathfrak{P}$ 中.

*4.* 利用事实:$A$ 中所有素理想的交等于 $A$ 中所有幂零元形成的集合, 证明: 如果 $f(X) \in A[X]^*$, 则 $a_0 \in A^*$, 且 $a_1, \cdots, a_n$ 均为幂零元.

# 2022-03-02,03-07 环的整性, 素元与不可约元

例 **1.** 设 $p$ 为奇素数.

*1.* $\mathbb{F}_p^*$ 为 $p-1$ 阶循环群.

*2.* 存在唯一的非平凡群同态 $\mathbb{F}_p^* \to \{\pm 1\} \subset \mathbb{C}$. 将该同态记为:$a \mapsto (\dfrac{a}{p})$.

*3.* $\mathbb{F}_p^* \to \{\pm 1\} \subset \mathbb{F}_p^*, a \mapsto a^{\frac{p-1}{2}}$ 为非平凡群同态.

*4.* $\forall a \in \mathbb{F}_p^*$, 有 $\left(\dfrac{a}{p}\right) = a^{\frac{p-1}{2}}$.

例 **2.** 考虑 Gauss 整数环 $\mathbb{Z}[i]$.

*1.* $\mathbb{Z}[i]$ 为 Euclide 整环.

*2.* $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

*3.* 对于素数 $p \in \mathbb{Z}$,

• 当 $p = 2$ 时, 存在唯一的素理想 $\mathfrak{P} \in \operatorname{Spec} \mathbb{Z}[i]$, 使得 $\mathfrak{P} \cap \mathbb{Z} = (p)$(称为 $\mathfrak{P}$ 位于 $(p)$ 上方), 并且 $\mathfrak{P} = (1+i) \neq (p)$. $2 = (-i)(1+i)^2$ 为其唯一因子分解.

• 当 $p \equiv 3 \ mod\ 4$, 时, $(p)$ 为 $\mathbb{Z}[i]$ 中素理想. 此时 $p$ 为 $Z[i]$ 中不可约元.

• 当 $p \equiv 1 \ mod\ 4$, 时, 恰有两个 $\mathbb{Z}[i]$ 中的素理想 $\mathfrak{P}_1, \mathfrak{P}_2$ 位于 $(p)$ 的上方. 此时存在非零的 $a, b \in \mathbb{Z}$ 使得 $p = a^2 + b^2$, 而 $p = (a+ib)(a-ib)$ 为 $p$ 在 $\mathbb{Z}[i]$ 中的唯一因子分解, 并且 $\{(a+ib), (a-ib)\} = \{\mathfrak{P}_1, \mathfrak{P}_2\}$.

*4.* 设 $n$ 为正整数, 则存在整数 $a, b$ 使得 $n = a^2 + b^2$ 当且仅当 $n$ 的唯一因子分解中模 4 余 3 的素因子个数是偶数.

注: 本例事实上给出了 $\mathbb{Z}$ 中理想 $(p)$ 在 $\mathbb{Z}[i]$ 上的分歧情况.

例 **3.** 考虑环 $\mathbb{Z}[\sqrt{2}]$.

*1.*$\mathbb{Z}[\sqrt{2}]$ 为 Euclide 整环.

*2.* $i\sqrt{2}$ 为 $\mathbb{Z}[i\sqrt{2}]$ 中不可约元.

*3.* 设 $x, y \in \mathbb{Z}$ 且 $y^2+2=x^3$, 则

- $(y+i\sqrt{2}, y-i\sqrt{2})=1$;
- 存在 $z \in \mathbb{Z}[i\sqrt{2}]$, 使得有理想的等式 $(y+i\sqrt{2})=(z)^3$;
- $(x, y)=(3, \pm 5)$.

注: 本例是利用代数数论解简单不定方程的典范. 此处因为所考虑的环是 PID, 所以处理起来很容易. 一般情况下要利用 Dedekind 整环中理想的唯一分解, 来得到理想的关系, 并根据类数给出一些结果.

习题 **1.** 令 $j=\dfrac{-1+i\sqrt{3}}{2}$, 考虑 Eisenstein 环 $\mathbb{Z}[j]$.

*1.* $\mathbb{Z}[j]$ 为 Euclide 整环. 确定该环中所有单位及不可约元.

*2.* 对于素数 $p$, 分析 $\mathbb{Z}[j]$ 中位于 $(p)$ 上方的素理想个数.

*3.* 证明环同构:$\mathbb{Z}[j]/(j-1) \simeq \mathbb{F}_3$, $\mathbb{Z}[j]/(2+3j) \simeq \mathbb{F}_7$.

习题 **2.** 设 $p$ 为素数, $\zeta_p=e^{\frac{2\pi i}{p}} \in \mathbb{C}^*$ 为一个 p 次本原单位根.

*1.* 令 $\Phi_p(X):=X^{p-1}+X^{p-2}+\cdots+X+1$ 为 $\mathbb{Z}$ 系数多项式. 证明 $\Phi_p(X)$ 在 $\mathbb{Z}[X]$ 中不可约.

*2.* $\mathbb{Z}[\zeta_p] \simeq \mathbb{Z}[X]/(\Phi_p(X))$.

*3.* 对于素数 $q$, $(q)$ 为 $\mathbb{Z}[\zeta_p]$ 中素理想当且仅当 $p$, $q$ 满足什么条件?

习题 **3.** 设 $x, y \in \mathbb{Z}$ 且 $y^2+4=x^3$, 则 $(x, y)=(\pm 11, 5)$ 或 $(\pm 2, 2)$.

习题 **4.** (*2021* 丘赛试题) 求方程 $x^2+13=y^3$ 的所有整数解. (提示: 可以利用 $\mathbb{Q}(\sqrt{-13})$ 的类数 (class number) 为 2 这个事实).

# 2022-03-09 环的局部化

以下环均指交换环.

**定义 1.** 设 $A$ 为环, $A$ 中的子集 $S$ 称为一个乘法子集, 如果 $1 \in S$, 并且 $\forall s_1, s_2 \in S, s_1 s_2 \in S$.

设 $A$ 为环, $S$ 为 $A$ 中的一个乘法子集. 定义 $A \times S$ 中的关系如下:

$$(a, s_1) \backsim (b, s_2) \Leftrightarrow \exists s \in S, s(as_2 - bs_1) = 0.$$

**习题 1.** 验证这是一个等价关系.

**习题 2.** (局部化的万有性质)

$i$ 满足 $i(S) \subset A_S^*$, 且对任意环 $B$, 以及任意环同态 $\varphi\colon A \to B$, 如果 $\varphi(S) \subset B^*$, 那么存在唯一的环同态 $\bar{\varphi}\colon A_S \to B$, 使得 $\varphi = \bar{\varphi} \circ i$. 用交换图表表示如下:

$$\begin{tikzcd} A \arrow[d, "i"'] \arrow[dr, "\varphi"] & \\ A_S \arrow[r, dashed, "\exists!\bar{\varphi}"] & B \end{tikzcd}$$

**习题 3.** 如果乘法子集 $S$ 满足 $S \subset A^*$, 那么同态 $i\colon A \to A_S$ 为同构.

**例 1.** 常用的局部化有以下三类:

- 设 $f \in A$, 取乘法子集 $S = \{f^n \mid n \geq 0\}$, 则局部化 $A_S$ 也记为 $A_f$. 我们有

$$A_f = \{\frac{a}{f^n} \mid a \in A, n \geq 0\}.$$

• 设 $\mathfrak{P} \in \mathrm{Spec}A$, 取乘法子集 $S = A \backslash \mathfrak{P}$, 则局部化 $A_S$ 也记为 $A_{\mathfrak{P}}$. 我们有 $A_{\mathfrak{P}} = \{\frac{a}{s} \mid s \notin \mathfrak{P}\}$

• 设 $\varphi\colon A \to B$ 为环同态, $\mathfrak{P} \in \mathrm{Spec}A$, 取 $B$ 的乘法子集 $S = \varphi(A \backslash \mathfrak{P})$, 则局部化 $B_S$ 也记为 $B_{\mathfrak{P}}$. 我们有 $B_{\mathfrak{P}} = \{\frac{b}{\varphi(s)} \mid s \notin \mathfrak{P}\}$.

对于环同态 $\varphi\colon A \to B$, 对于 $A$ 中的理想 $I$, 记 $IB$ 为 $B$ 中由 $\varphi(I)$ 生成的理想. 对于 $B$ 中的理想 $J$, $\varphi^{-1}(J)$ 为 $A$ 中的理想, 有时也将 $\varphi^{-1}(J)$ 记为 $J \cap A$(虽然 $\varphi$ 不一定是单同态.

习题 **4.** 设 $A \to B$ 为环同态. 设 $I$ 为 $A$ 中的理想, $J$ 为 $B$ 中的理想.

*1.*$I \subset IB \cap A$

*2.*$(J \cap A)B \subset J$

*3.* 如果 $B = A_S$ 为局部化, 并且同态 $A \to B$ 为自然同态 $i\colon A \to A_S$, 则 $(J \cap A)A_S = J$. 特别地, $A_S$ 中的理想 $J$ 均具有形式 $IA_S$, 其中 $I$ 为 $A$ 中理想.

注: $J \mapsto J \cap A$ 给出映射 $i\colon \{B\text{的理想}\} \to \{A\text{的理想}\}$, 而 $I \mapsto IA_S$ 则给出反向映射 $s\colon \{A\text{的理想}\} \to \{B\text{的理想}\}$, 以上习题说明当 $B = A_S$ 且 $\varphi$ 为相应自然映射时, 我们有 $s \circ i = \mathrm{id}$. 由此得出 $i$ 为单射, 而 $s$ 为满射.

*4.* 如果 $A$ 为 Noether 环, 则局部化 $A_S$ 也为 Noether 环.

习题 **5.** 设 $A_S$ 为 $A$ 的局部化.

*1.* 对于素理想 $\mathfrak{P} \in \mathrm{Spec}A$, 如果 $\mathfrak{P} \cap S = \varnothing$, 则 $\mathfrak{P}A_S$ 为 $A_S$ 中的素理想.

*2.* 映射 $\mathfrak{P} \mapsto \mathfrak{P}A_S$ 和 $\mathfrak{Q} \mapsto \mathfrak{Q} \cap A$ 定义了以下两个集合之间的双射:

$$\{\mathfrak{P} \in \mathrm{Spec}A \mid \mathfrak{P} \cap S = \varnothing\} \leftrightarrow \mathrm{Spec}A_S.$$

习题 **6.** 设 $A$ 为环. $f \in \cap_{\mathfrak{P}\in \mathrm{Spec}A}\mathfrak{P}$.

1. $\mathrm{Spec}A_f = \varnothing$

2. $A_f$ 为零环.

3. $f$ 为幂零元.

4. $\cap_{\mathfrak{P}\in \mathrm{Spec}A}\mathfrak{P} = \{f \in A \mid f \text{ 为幂零元}\}$

利用局部化的万有性质, 证明如下局部化与商的交换性:

习题 **7.** 设 $S$ 为环 $A$ 的乘法子集, 设 $I$ 为 $A$ 的理想. 记 $\bar{S} \in A/I$ 为 $S$ 在商映射 $A \to A/I$ 下的像.

1. $\bar{S}$ 为 $A/I$ 中的乘法子集.

2. 有环同构 $A_S/IA_S \simeq (A/I)_{\bar{S}}$.

特别地, 对于素理想 $\mathfrak{P} \in \mathrm{Spec}A$, 有域同构 $A_\mathfrak{P}/\mathfrak{P}A_\mathfrak{P} \simeq Frac(A/\mathfrak{P})$(在习题 7中取 $I = \mathfrak{P}, S = \mathrm{Spec}A\backslash\mathfrak{P}$). 将这个域记为 $\kappa(\mathfrak{P})$, 称为 $A$ 在素理想 $\mathfrak{P}$ 处的剩余类域.

## 阅读材料: 环的局部化几何意义与函数芽环

对于环 $A$, 我们将 $f \in A$ 看作空间 $\mathrm{Spec}A$ 上的"函数", 其在点 $\mathfrak{P} \in \mathrm{Spec}A$ 处的"取值"定义为 $f$ 在剩余类域 $\kappa(\mathfrak{P})$ 中的像, 即 $f(\mathfrak{P}) := \bar{f} \in \kappa(\mathfrak{P})$. 对于 $A$ 中的理想 $I$, 其中元素的"公共零点"集合为 $V(I) := \{\mathfrak{P} \in \mathrm{Spec}A | f(\mathfrak{P}) = 0, \forall f \in I\} = \{\mathfrak{P} \in \mathrm{Spec}A | I \subset \mathfrak{P}\}$. 我们定义 $\mathrm{Spec}A$ 中的闭集为形如 $V(I)$ 的集合, 容易验证这样定义了 $\mathrm{Spec}A$ 上的一个拓扑, 称为 *Zariski* 拓扑. 对于 $f \in A$, 定义 $D(f) := \{\mathfrak{P} \in \mathrm{Spec}A | f(\mathfrak{P}) \neq 0\} = \{\mathfrak{P} \in \mathrm{Spec}A | f \notin \mathfrak{P}\}$.

习题 **8.** $\{D(f)|f\in A\}$ 为 $\mathrm{Spec}A$ 中的一组开集基 (*basis*), 即 $\mathrm{Spec}A$ 中任意开集均为一些 $D(f)$ 的并集.

习题 **9.** 对于 $f\in A$, 有集合的一一对应: $D(f)\leftrightarrow \mathrm{Spec}A_f$. 通过这个一一对应, 可以将 $A_f$ 看作 $D(f)$ 上的函数环, 对于 $\dfrac{a}{f^n}\in A_f$, 对于 $\mathfrak{P}\in D(f)$, 取值为 $\dfrac{a}{f^n}(\mathfrak{P}):=a(\mathfrak{P})/f(\mathfrak{P})^n$. 此为 $A_f$ 的几何解释, 即看作开子集 $D(f)$ 上的函数环.

为了解释在一个素理想处的局部化 $A_{\mathfrak{P}}$, 我们先看一般的拓扑空间在一个点处的函数芽环. 设 $X$ 为拓扑空间, $x\in X$. 定义集合

$$\{(f,U)|U\text{为}x\text{在}X\text{中的一个开邻域, }f\text{为}U\text{上的一个实值连续函数}\}$$

上的一个关系如下: $(f,U)\sim(g,V)\Leftrightarrow$ 存在 $x$ 的开邻域 $W$ 满足 $W\subset U\cap V$, 并且 $f|_W=g|_W$. 容易验证这是一个等价关系. 我们将商集记作 $\mathcal{C}_{X,x}$, 并将其中的一个元素 $[(f,U)]$ 记作 $f_x$, 称作 $x$ 处的一个连续函数芽. 定义 $\mathcal{C}_{X,x}$ 上的加法和乘法运算如下:

$$\mathcal{C}_{X,x}\times\mathcal{C}_{X,x}\to\mathcal{C}_{X,x}$$

$$([(f,U)],[(g,V)])\mapsto[(f,U)]+[(g,V)]:=[(f|_{U\cap V}+g|_{U\cap V},U\cap V)]$$

$$\mathcal{C}_{X,x}\times\mathcal{C}_{X,x}\to\mathcal{C}_{X,x}$$

$$([(f,U)],[(g,V)])\mapsto[(f,U)]\cdot[(g,V)]:=[(f|_{U\cap V}\cdot g|_{U\cap V},U\cap V)]$$

容易验证上述定义是良好的, 并且在这些运算下 $\mathcal{C}_{X,x}$ 成为交换环.

习题 **10** $\mathcal{C}_{X,x}^* = \{[(f,U)|f(x) \neq 0\}$.$\mathcal{C}_{X,x}$ 中的唯一极大理想是 $\{[(f,U)|f(x) = 0\}$.

注: 具有唯一极大理想的环称为局部环.

习题 **11.** 在 $\mathcal{C}_{X,x}$ 的定义中, 将开集 $U, V, W$ 均换为一个固定的开集基中的元素, 得到的还是函数芽环 $\mathcal{C}_{X,x}$.

注: 我们关心的只是函数在 $x$ 附近的行为, 函数芽环研究的是一种局部性质.

下面将拓扑空间取成 $\mathrm{Spec}A$, 点取作 $\mathfrak{P}$, 开集基取作 $\{D(f)|f \in A\}$, 将 $D(f)$ 上的函数取为 $A_f$ 中的元, 则出现的函数芽环就是 $A_{\mathfrak{P}}$. 具体而言, 考虑集合 $\{(a, D(f))|\mathfrak{P} \in D(f), a \in A_f\}$. 定义该集合上的等价关系:$(a, D(f)) \sim (b, D(g)) \Leftrightarrow \exists D(h)$, 使得 $\mathfrak{P} \in D(h) \subset D(f) \cap D(g)$, 且 $a|_{D(h)} = b|_{D(h)}$, 这里 $a|_{D(h)}$ 是指 $a$ 在自然同态 $A_f \to A_h$ 下的像, $b_{D(h)}$ 的意思相同. 在这个等价关系下, 商集合同样在自然定义的加法和乘法下成为环. 不难验证, 这个环同构于局部化 $A_{\mathfrak{P}}$. 此为 $A_{\mathfrak{P}}$ 的几何解释.

# 2022-03-14 环的整扩张与 Hilbert 零点定理

以下环均指交换环.

**定义 1** 设 $\varphi\colon A\to B$ 是环同态. 称 $b\in B$ 在 $A$ 上整 (integral), 如果 $\exists n\geq 1$ 和 $a_0,\cdots,a_{n-1}\in A$, 使得

$$b^n+\varphi(a_{n-1})b^{n-1}+\cdots+\varphi(a_1)b+\varphi(a_0)=0.$$

如果 $\forall b\in B$, $b$ 均在 $A$ 上整, 就称 $B$ 在 $A$ 上整, 也称 $\varphi\colon A\to B$ 为环的整扩张 (注意 $\varphi$ 不一定是单同态).

**习题 1.** 设 $\varphi\colon A\to B$ 为环的整扩张.

*1.* 设 $J\subset B$ 为 $B$ 的理想, 则 $A/J\cap A\to B/J$ 为整扩张.(注意记号 $J\cap A:=\varphi^{-1}(J)$)

*2.* 设 $S\subset A$ 为乘法子集, 则 $A_S\to B_S$ 为整扩张.(注意记号 $B_S$ 为 B 在 $\varphi(S)$ 处的局部化.)

**习题 2.** *1.* 设 $\varphi\colon A\hookrightarrow B$ 为整环之间的单同态, 同时也是整扩张. 则 $A$ 为域 $\Leftrightarrow$ $B$ 为域.

*2.* 设 $A\to B$ 为环的整扩张. 设 $J\subset B$ 为 $B$ 的理想, 则 $J$ 为 $B$ 的极大理想 $\Leftrightarrow J\cap A$ 为 $A$ 的极大理想.

*3.*设 $A\hookrightarrow B$ 为整环之间的单同态, 同时也是整扩张. 设 $\mathfrak{P}$ 为 $B$ 的素理想, 并且 $\mathfrak{P}\neq(0)$, 则 $\mathfrak{P}\cap A\neq(0)$.

习题 **3.** (Hilbert 零点定理的弱形式) 设 $\mathfrak{m}$ 为 $\mathbb{C}[x,y]$ 的极大理想 (从而非零), 并且设 $\mathfrak{m}$ 包含一个不可约多项式 $f$, 使得 $f$ 看作 $y$ 的多项式为首一且次数大于 0, 即 $f$ 形如 $y^n + c_{n-1}(x)y^{n-1} + \cdots + c_0(x)$.

*1.* $\mathbb{C}[x] \to \mathbb{C}[x,y]/(f)$ 为整环之间的单同态, 且为整扩张.

*2.* $\mathfrak{m}/(f)\cap\mathbb{C}[x]$ 为 $\mathbb{C}[x]$ 中极大理想, 从而存在 $a\in\mathbb{C}$, 使得 $\mathfrak{m}/(f)\cap\mathbb{C}[x] = (x-a)$.

*3.* $\mathfrak{m}/(f, x-a)$ 为 $\mathbb{C}[x,y]/(f, x-a)$ 中的极大理想, 并且 $\mathbb{C}[x,y]/(f,x-a) \simeq \mathbb{C}[y]/(f(a,y))$.

*4.* 存在 $a,b\in\mathbb{C}$, 使得 $\mathfrak{m} = (x-a, y-b)$.

*5.* 设 $g(x,y)\in\mathbb{C}[x,y]$ 为非零多项式, 则存在正整数 $k$ 和非零复数 $\lambda\in\mathbb{C}^*$, 使得作如下变量代换后, $\tilde{g}(x',y') = g(x,y)$, 且 $\lambda\tilde{g}(x',y')$ 为关于 $y'$ 的首一且次数大于零的多项式:

$$\begin{cases} x = x' + y'^k \\ y = y' \end{cases}$$

*6.* 设 $g(x,y)\in\mathbb{C}[x,y]$ 为非零多项式, 且为关于 $y$ 的首一且次数大于零的多项式. 设 $h(x,y)\in\mathbb{C}[x,y]$ 为 $g(x,y)$ 的一个不可约因子, 则 $h(x,y)$ 也为关于 $y$ 的首一且次数大于零的多项式.

*7.* $\mathbb{C}[x,y]$ 的任意极大理想均形如 $(x-a, y-b)$, 其中 $a,b\in\mathbb{C}$.

*8.*(Hilbert 零点定理, 弱形式) $\mathbb{C}[x_1,\cdots,x_n]$ 的任意极大理想均形如 $(x_1-a_1,\cdots,x_n-a_n)$, 其中 $a_1,\cdots,a_n\in\mathbb{C}$.

习题 **4.** (选做, Hilbert 零点定理的强形式) 一个 $\mathbb{C}$-代数 $A$ 称为有限生成 $\mathbb{C}$-代数, 如果存在 $n$ 以及理想 $I\subset\mathbb{C}[x_1,\cdots,x_n]$, 使得 $A\simeq\mathbb{C}[x_1,\cdots,x_n]/I$, 即 $A$ 同构于多项式环的商.

*1.* 设 $A$ 为有限生成 $\mathbb{C}$-代数, $f \in A$, 则有 $\mathbb{C}$-代数同构: $A[x]/(1-fx) \simeq A_f$. 特别地, $A_f$ 也为有限生成 $\mathbb{C}$-代数.

*2.* 设 $A$ 为有限生成 $\mathbb{C}$-代数, $f \in A$, 则 $A_f$ 中的极大理想一一对应到 $A$ 中不包含 $f$ 的极大理想.

*3.* 设 $A$ 为有限生成 $\mathbb{C}$-代数, $f \in A$. 如果对任意 $A$ 中的极大理想 $\mathfrak{m}$, 均有 $f \in \mathfrak{m}$, 则 $A_f$ 为零环, 从而 $f$ 为 $A$ 中幂零元, 即 $A$ 的全体极大理想之交为幂零根.

*4.*(Hilbert 零点定理, 强形式) 设 $I$ 为多项式环 $\mathbb{C}[x_1, \cdots, x_n]$ 中的理想, 设 $f \in \mathbb{C}[x_1, \cdots, x_n]$. 如果对任意 $a \in V(I) := \{x \in \mathbb{C}^n \mid g(x) = 0, \forall g \in I\}$, 均有 $f(a) = 0$, 则 $f \in \sqrt{I} := \{h \in \mathbb{C}[x_1, \cdots, x_n] \mid \exists m \geq 1, h^m \in I\}$.

# 2022-03-16 离散赋值环与 Dedekind 整环

以下环均指交换环.

**定义 1.** 设 $(A,m)$ 为局部环 (即环 $A$ 只有唯一的一个极大理想 $m$) 并且 $A$ 为 Noether 整环, $m$ 为非 0 主理想, 则称 $A$ 为离散赋值环 (discrete valuation ring, 简称 DVR).

**习题 1.** 设 $(A,m)$ 为离散赋值环, $m=(\pi)$, 则:

*1.* $A^*=A\backslash m$.

*2.* $\forall 0\neq a\in A$, 存在 $k\geq 0$ 为非负整数, 以及 $u\in A^*$, 使得 $a=\pi\cdot\pi^k$.

*3.* $A$ 为主理想整环 (PID) 从而为 (UFD).

*4.* $\mathrm{Spec}A=\{(0),m\}$

离散赋值环的例子:$\mathbb{Z}_p,\mathbb{C}[[x]]$, 以及 $\mathbb{Z}_{(p)}:=\{\dfrac{a}{b}\mid a\in\mathbb{Z},p\nmid b\}$($\mathbb{Z}_{(p)}$ 为 $\mathbb{Z}$ 在素理想 $(p)$ 处的局部化).

**定义 2.** 一个环 $A$ 称为 Dedekind 整环, 如果 $A$ 为 Noether 整环, 并且对任意一个非零素理想 $\mathfrak{P}\in\mathrm{Spec}A$, 局部化 $A_{\mathfrak{P}}$ 均为离散赋值环.

**习题 2.** 设 $A$ 为 Dedekind 整环, 则 $A$ 的每个非零素理想均为极大理想.

下面的习题给出了判断局部化 $A_{\mathfrak{P}}$ 为离散赋值环的一个方法.

**习题 3.** 设 $A=L_1\times\cdots\times L_n$ 为 $n$ 个域的乘积. 证明:

*1.* $A$ 中恰好有 $n$ 个素理想 $P_1,\cdots,P_n$, 并且 $P_i=\{(x_1,\cdots,x_n)\in A\mid x_i=0\}$.

*2.* $A_{P_i}\simeq L_i,\forall i=1,\ldots,n$.

*3.* $P_iA_{P_i}=(0), \forall i=1,\ldots,n$.

*4.* 设 $f(x)\in\mathbb{Z}[x]$ 为首一的不可约多项式, 记 $B=\dfrac{\mathbb{Z}[x]}{(f(x))}$. 设 $(0)\neq P\in \mathrm{Spec}B$ 且 $P\cap\mathbb{Z}=(p), p\in\mathbb{Z}$ 为素数, 以及 $\overline{f(x)}\in\mathbb{F}_p[x]$ 为 $\mathbb{F}_p$ 上无重根的多项式 (即 $\overline{f'(x)}$ 与 $\overline{f(x)}$ 在 $\mathbb{F}_p[x]$ 上互素). 证明:$B/(p)$ 为有限个域的乘积, 并且在 $B_P$ 中 $PB_P=(p)$ 为主理想.

注: 此处 $(p)B_P$ 指 $B$ 中理想 $(p)$ 在局部化中的像生成的理想, 命题最后结论的 $(p)$ 指 $p$ 在局部环 $B_P$ 中生成的主理想. 此处二者是相等的.

习题 **4.** $\mathbb{Z},\mathbb{Z}[i],\mathbb{Z}[\sqrt{2}],\mathbb{Z}[\sqrt[3]{2}]$ 均为 Dedekind 整环.

习题 **5.** 设 $p$ 为素数, $\zeta_{p^n}:=e^{\frac{2\pi i}{p^n}}\in\mathbb{C}^*$ 为一个 $p^n$ 次本原单位根.

*1.* $\Phi_p(x):=\dfrac{x^p-1}{x-1}=1+x+\cdots+x^{p-1}$ 为 $\mathbb{Z}[x]$ 中不可约多项式.

*2.* $\mathbb{Z}[\zeta_p]\simeq\mathbb{Z}[x]/(\Phi_p(x))$.

*3.* $\mathbb{Z}[\zeta_p]$ 为 Dedekind 整环.

*4.* $\mathbb{Z}[\zeta_{p^n}]$ 为 Dedekind 整环.

习题 **6.** 如果 $f(X,Y)\in\mathbb{C}[X,Y]$ 为不可约多项式, 并且不存在 $(a,b)\in\mathbb{C}^2$, 使得 $f(a,b)=\dfrac{\partial f}{\partial X}(a,b)=0$, 或不存在 $(a,b)\in\mathbb{C}^2$, 使得 $f(a,b)=\dfrac{\partial f}{\partial Y}(a,b)=0$, 则 $\dfrac{\mathbb{C}[X,Y]}{f(X,Y)}$ 为 Dedekind 整环.

## 阅读材料: Dedekind 整环的理想类群

以下设 $A$ 为 Dedekind 整环. 记 $\mathrm{Spec}_mA$ 为 $A$ 的所有非零素理想形成的集合, 其中的元素称为 $A$ 的一个素点. 对于 $P\in\mathrm{Spec}_mA$, 设 $\pi_P$ 为 DVR $A_P$ 的唯一极大理想

$PA_P$ 的生成元. 对任意非零的 $f \in Frac(A) = Frac(A_P)$, 存在唯一的 $u \in A_P^*$, 以及 $n \in \mathbb{Z}$, 使得 $f = u\pi_P^n$. 我们记 $v_P(f) = n$, 称为 $f$ 在素点 $P$ 处的赋值 (因而是所谓的离散赋值).

下面的习题说明 $f$ 在所有素点 $P$ 处的赋值在相差一个 $u \in A^*$ 的意义上确定了 $f$.

习题 **7.** 设 $f \in Frac(A)^* = Frac(A)\backslash\{0\}$.

*1.* 设 $g \in Frac(A)^*, P \in \mathrm{Spec}_m A$, 则 $v_P(fg) = v_P(f) + v_P(g)$, 以及 $v_P(f+g) \geq min\{v_P(f), v_P(g)\}$.

*2.* $\forall P \in \mathrm{Spec}_m A$, 有 $v_P(f) = 0 \Leftrightarrow f \in A_P^*$, 以及 $v_P(f) \geq 0 \Leftrightarrow f \in A_P$

*3.* $A = \cap_{P\in \mathrm{Spec}_m A} A_P$, 其中将 $A_P$ 均看作 $Frac(A)$ 的子环再取交集.

*4.* $(\forall P \in \mathrm{Spec}_m A, v_P(f) \geq 0) \Leftrightarrow f \in A$, 以及 $(\forall P \in \mathrm{Spec}_m A, v_P(f) = 0) \Leftrightarrow f \in A^*$.

习题 **8.** *1.* 设 $f \in A$ 且 $f \neq 0$, 则 $\{P \in \mathrm{Spec}_m A \mid f \in P\}$ 为有限集.

*2.* 设 $f \in Frac(A)^*$, 则 $\{P \in \mathrm{Spec}_m A \mid v_P(f) \neq 0\}$ 为有限集.

记 $Div(A)$ 为以集合 $\mathrm{Spec}_m A$ 中元素为基生成的自由 Abel 群, 该群称为 $A$ 的除子群, 其中的每个元素均形如 $\sum_{P\in \mathrm{Spec}_m A} n_P P$, 其中 $n_P \in \mathbb{Z}$ 且只有有限个 $P$ 使得 $n_P \neq 0$. 上面的习题说明以下群同态是良好定义的:

$$\varphi\colon Frac(A)^* \to Div(A)$$

$$f \mapsto (f) := \sum_{P\in \mathrm{Spec}_m A} v_P(f)P$$

形如 $(f) = \sum_{P\in \mathrm{Spec}_m A} v_P(f)P$ 的除子称为主除子 (principle divisor).

习题 **9.** $\ker\varphi = A^*$, 从而有 Abel 群的正合列:

$$1 \to A^* \to Frac(A)^* \xrightarrow{\varphi} Div(A)$$

定义 **3.** $A$ 的除子类群 $Cl(A)$ 定义为商群 $\operatorname{coker}\varphi = Div(A)/\operatorname{Im}(\varphi)$.

除子类群 $Cl(A)$ 也称为 $A$ 的理想类群, 其大小刻画了 $A$ 偏离主理想整环的程度. 以下为代数数论中的基本定理之一:

定理 设 $\mathcal{O}_K$ 为代数数域 $K$ 的代数整数环 (ring of algebraic integers), 则 $Cl(\mathcal{O}_K)$ 为有限 Abel 群.(可以参考 [**?**] 第一章 §2)

下面解释 $Cl(A)$ 与 $A$ 中理想的关系. 对于理想 $I \subset A$, 对于素点 $P \in \mathrm{Spec}_m A$, $IA_P$ 为 DVR $A_P$ 中的理想, 从而存在非负整数 $n_P \geq 0$, 使得 $IA_P = (\pi_P)^{n_P} = (PA_P)^{n_P}$. 注意到 $n_P = 0 \Leftrightarrow IA_P = A_P \Leftrightarrow I \not\subseteq P$. 由上面的习题, 若 $I \neq (0)$, 则只有有限个 $P$ 包含 $I$(考虑商环 $A/I$), 从而只有有限个 $P$ 使得 $n_P \neq 0$, 这样得到一个除子 $div(I) := \sum_{P\in \mathrm{Spec}_m A} n_P P$. 显然对于 $P \in \mathrm{Spec}_m A$, 有 $div(P) = P$.

习题 **10.** 设 $I, J$ 均为 $A$ 的非零理想, 则 $div(IJ) = div(I) + div(J)$.

习题 **11.** 本题的目标是给出 Dedekind 整环中理想的唯一分解, 并从理想类群的角度给出一个判断 Dedekind 整环 $A$ 是否是主理想整环的充要条件.

*1.* 设 $B$ 为环, $f \in B$, 并且对 $B$ 的任意极大理想 $m$, 在局部化 $B_m$ 中均有 $f = 0$, 则在 $B$ 中有 $f = 0$.

*2.* 设 $B$ 为环, $f \in B$, $J$ 为 $B$ 的理想, 并且对 $B$ 的任意极大理想 $m$, 在局部化 $B_m$

中均有 $f \in JB_m$, 则在 $B$ 中有 $f \in J$.

注: 也可以考虑商环 $B/J$, 利用商与局部化交换, 将问题转化为*1*.

*3.* 设 $A$ 为 Dedekind 整环, $I, J$ 为 $A$ 的非零理想, 并且 $div(I) = div(J)$, 则 $I = J$.

*4.* (Dedekind 整环中理想的唯一分解) 设 $I$ 为 $A$ 的非零理想, 并且 $div(I) = n_1P_1 + \cdots + n_kP_k$, 则 $I = P_1^{n_1} \cdots P_k^{n_k}$.=

*5.* 设 $I$ 为 $A$ 的非零理想, 并且存在 $f \in Frac(A)^*$, 使得 $div(I) = (f)$ 为主除子, 则 $f \in A$, 并且 $I = (f)$ 为主理想.

*6.* $Cl(A) = 0$ 即 $Cl(A)$ 为平凡 Abel 群 $\Leftrightarrow A$ 为主理想整环.

对于一个 Abel 半群 $S$, 我们记 $\langle S \rangle$ 为 $S$ 生成的 Abel 群 (用万有性质刻画就是: 对于 Abel 半群 $S$ 到群 $G$ 的半群同态 $\psi$, 存在唯一的群同态 $\bar{\psi}$: $\langle S \rangle \to G$, 使得 $\bar{\psi}|_S = \psi$). 对于 Dedekind 整环 $A$, 令 $\mathcal{I}$ 为 $A$ 中所有非零理想在理想乘积下形成的 Abel 半群, $\mathcal{P}$ 为 $A$ 的所有非零主理想在理想乘积下形成的子半群, 则上面的讨论说明 $\langle \mathcal{I} \rangle$ 同构于除子群 $Div(A)$, $\langle \mathcal{P} \rangle$ 同构于所有主除子形成的 $Div(A)$ 的子群, 从而商群 $\langle \mathcal{I} \rangle / \langle \mathcal{P} \rangle$ 同构于除子类群 (理想类群)$Cl(A)$.

将 $Frac(A)$ 看作 $A$-模, 则 $Frac(A)$ 的一个非零的有限生成 $A$-子模称为 $A$ 的一个分式理想, 可以证明 $\langle \mathcal{I} \rangle$ 与 $A$ 的所有分式理想在自然定义的乘积下形成的 Abel 群同构. 而对于 $f \in Frac(A)^*$, $f$ 生成 $Frac(A)$ 的一个 (自由) 子模 $Af$, 这样得到的分式理想称为主分式理想, 可以验证 $\langle \mathcal{P} \rangle$ 同构于主分式理想形成的 Abel 群. 这样我们得到 $Cl(A)$ 同构于分式理想所形成的群商去主分式理想所形成的子群. 这是 $Cl(A)$ 的另一种看法 (可以参考第二轮口试题目的选题 2: 模的局部化).

# 2022-03-19,03-20 第一轮口试题目-交换环

习题 **1.** 设 $R$ 为交换环. $A$ 称为 $R$-代数, 如果 $A$ 为 $R$-模, 且 $A$ 为环, 满足: 对任意 $r \in R$, $a, b \in A$, 有

$$r(a \cdot b) = (ra) \cdot b = a \cdot (rb)$$

习题 **2.** 设 $A$ 为有限交换环, 且 $A$ 为整环, 证明 $A$ 为域.

习题 **3.** 设 $A$ 为交换 $k$-代数, $k$ 为域, 且 $dim_k A < +\infty$.

*1.* 如果 $A$ 为整环, 证明 $A$ 为域.

*2.*$A$ 中素理想均为极大理想.

*3.*$A$ 中只有有限个素理想, 记为 $P_1, \cdots, P_n$.

*4.* 存在 $m \geq 1$, 使得 $(\cap_{i=1}^n P_i)^m = (0)$.

*5.* $A \simeq \prod\limits_{i=1}^n A/P_i^m$, 并且 $A/P_i^m$ 为局部环.

*6.* $A \simeq \prod\limits_{i=1}^n A_{P_i}$.

*7.* 如果 $A$ 为既约环, 即 $A$ 中没有非零的幂零元, 则 $A$ 同构于有限个域的乘积.

习题 **4.** 分析环 $\mathbb{Z}[\sqrt{3}]$ 中的素理想: 对于素数 $p$, 其上方的素理想个数, 生成元等.

习题 **5.** 设 $S$ 为交换环 $A$ 的乘法集, 则典范同态 $i\colon A \to A_S$ 诱导下面两个集合的双射:

$$\mathrm{Spec} A_S \xrightarrow{\sim} \{P \in \mathrm{Spec} A \mid P \cap S = \varnothing\}$$

$$q \mapsto i^{-1}(q)$$

习题 **6.** 设 $A$ 为交换环, $S$ 为 $A$ 的乘法子集, 并设 $A$ 为 Noether 环, 记 $A_S$ 为 $A$ 在 $S$ 处的局部化, $\varphi$: $A \to A_S$ 为自然同态.

*1.* 证明:$A_S$ 为 Noether 环.

*2.* 设 $J$ 为 $A_S$ 的理想, 且存在 $0 \neq y \in A_S$, 使得

$$J = Ann(y) := \{\alpha \in A_S \mid \alpha \cdot y = 0\}$$

证明: 存在 $0 \neq x \in A$, 使

$$\varphi^{-1}(J) = Ann(x) := \{\alpha \in A \mid \alpha \cdot x = 0\}$$

习题 **7.** 设 $A \xrightarrow{\varphi} B$ 为单同态且 $A, B$ 均为整环, 以及 $\varphi$ 为整扩张, 则 $A$ 为域 $\Leftrightarrow B$ 为域.

习题 **8.** 设 $m$ 为 $\mathbb{Z}[x]$ 的一个极大理想. 证明:

*1.* 存在次数大于零的不可约多项式 $f(x) \in m$.

*2.* 记 $n \neq 0$ 为 $f(x)$ 的首项系数, 记 $\mathbb{Z}_n$ 为 $\mathbb{Z}$ 在 $\{n^k | k \geq 0\}$ 处的局部化. 则 $\mathbb{Z}_n \to \mathbb{Z}_n[x]/(f(x))$ 为整环之间的单同态, 且为整扩张.

*3.*$m \cap \mathbb{Z} \neq (0)$. 从而存在素数 $p$, 使得 $m \cap \mathbb{Z}$=(p). ♢

*4.* 存在 $g(x) \in \mathbb{Z}[x]$, 使得 $\overline{g(x)}$ 在 $\mathbb{F}_p[x]$ 中为不可约多项式, 而且 $m = (p, g(x))$.

习题 **9.** 举出一个 UFD 但不是 PID 的例子.

以下为整闭整环的定义.

**定义** 1. 设 $A$ 为整环, $K$ 为 $A$ 的分式域, 如果 $A$ 在 $K$ 中的整闭包等于 $A$(或者说 $A$ 在 $K$ 中整闭), 则称 $A$ 为整闭整环 (integrally closed domain normal  domain).

习题 **10.** 证明 UFD 为整闭整环.

以下为一个关于整闭整环的判断方法.

习题 **11.** 设 $A$ 为整环, $K$ 为 $A$ 的分式域.

*1.* $A = \cap_{P\in \mathrm{Spec}A} A_P$. 这里将 $A$ 和 $A_P$ 均看作 $K$ 的子环.

*2.* 如果 $\forall P \in \mathrm{Spec}A$, $A_P$ 为整闭整环, 则 $A$ 为整闭整环.

习题 **12.** 设 $p$ 为素数

*1.* 证明:$\Phi_p(x) := \dfrac{x^p-1}{x-1}$ 为 $\mathbb{Q}[x]$ 中不可约多项式.

*2.* 设 $p^m$ 为素数幂次, 证明:$\Phi_{p^m}(x) := \dfrac{x^{p^m}-1}{x^{p^{m-1}}-1}$ 为 $\mathbb{Q}[x]$ 中不可约多项式.

习题 **13.** 证明 $f := x^n+x_{n-1}x^{n-1} = \cdots + x_1x+x_0$ 为 $n+1$ 元多项式环 $\mathbb{Z}[x_0,\cdots,x_{n-1},x]$ 中的不可约多项式.

**定义** 2. 设 $(A, m$ 为局部环, 并且 $A$ 为 Noether 整环, $m$ 为非 0 主理想, 则称 $A$ 为离散赋值环 (DVR).

习题 **14.** 证明 $\mathbb{Z}_p, \mathbb{C}[[x]]$, 以及 $\mathbb{Z}_{(p)} := \{\dfrac{a}{b} \mid a \in \mathbb{Z}, p \nmid b\}$(即 $\mathbb{Z}_{(p)}$ 为 $\mathbb{Z}$ 在素理想 $(p)$ 处的局部化) 均为离散赋值环.

习题 **15.** 设 $(A, m)$ 为离散赋值环, $m = (\pi)$, 则:

1. $A^* = A \backslash m$.

2. $\forall 0 \neq a \in A$, 存在 $k \geq 0$ 为非负整数, 以及 $u \in A^*$, 使得 $a = u \cdot \pi^k$.

3. $A$ 为 PID 从而为 UFD, 为整闭整环.

# 2022-03-21 代数不变量理论

设 $G$ 为群, $\rho\colon G \to GL(V)$ 为 $G$ 的有限维复表示. 记 $\mathbb{C}[V]$ 为 $V$ 上的复值多项式函数形成的环, $G$ 作用于 $\mathbb{C}[V]: \forall g \in G, \forall f \in \mathbb{C}[V], (g \cdot f)(v) = f(g^{-1}v)$, 对于 $v \in V$, 记 $\mathbb{C}[V]^G = \{f \in V | gf = f, \forall g \in G\}$ 为 $G$-不变多项式函数构成的子环. 代数不变量理论研究 $\mathbb{C}$-代数 $\mathbb{C}[V]^G$ 的结构.

习题 **1.** 设 $G$ 为有限群, $V$ 为有限维复线性空间, $\rho\colon G \to GL(V)$ 为 $G$ 在 $V$ 上的表示. 通过以下步骤证明 $\mathbb{C}[V]^G$ 为有限生成 $\mathbb{C}$-代数.

*1.* 取对偶空间 $V^*$ 的一组基, 则有 $\mathbb{C}[V] \simeq \mathbb{C}[x_1, \ldots, x_n]$, 从而 $G$ 作用于 $\mathbb{C}[x_1, \ldots, x_n]$, 并且该作用保持次数.

*2.* 记 $I$ 为 $\mathbb{C}[x_1, \ldots, x_n]^G$ 中的正次数齐次多项式在 $\mathbb{C}[x_1, \ldots, x_n]$ 中生成的理想. 证明: 存在正次数齐次多项式 $f_1, \ldots, f_k \in \mathbb{C}[x_1, \ldots, x_n]^G$, 使得 $I = (f_1, \ldots, f_k)$.

*3.* 证明: 任取正次数齐次多项式 $f \in \mathbb{C}[x_1, \ldots, x_n]^G$, 存在齐次多项式 $g_1, \ldots, g_k \in \mathbb{C}[x_1, \ldots, x_n]$, 使得:$f = g_1 f_1 + \cdots + g_k f_k$.

*4.* 证明: 任取正次数齐次多项式 $f \in \mathbb{C}[x_1, \ldots, x_n]^G$, 存在齐次多项式 $g_1, \ldots, g_k \in \mathbb{C}[x_1, \ldots, x_n]^G$, 使得:$f = g_1 f_1 + \cdots + g_k f_k$.

*5.* 证明:$\mathbb{C}[x_1, \ldots, x_n]^G$ 为有限生成 $\mathbb{C}$-代数, 从而 $\mathbb{C}[V]^G$ 为有限生成 $\mathbb{C}$-代数.

习题 **2.** 设 $V = \mathbb{C}e_1 \bigoplus \cdots \bigoplus \mathbb{C}e_n$ 为 $n$ 维线性空间, 置换群 $\mathfrak{S}_n$ 作用于 $V: \forall \sigma \in \mathfrak{S}_n$, $\forall i$, $\sigma e_i = e_{\sigma(i)}$. 证明:$\mathbb{C}[V]^{\mathfrak{S}_n} \simeq \mathbb{C}[\sigma_1, \ldots, \sigma_n] \subset \mathbb{C}[x_1, \ldots, x_n]$, 其中 $\sigma_i$ 为 $x_1, \ldots, x_n$ 的 $i$ 次初等对称多项式.

习题 **3.** $GL_n(\mathbb{C})$ 通过相似作用于 $n$ 阶方阵形成的线性空间 $M_n(\mathbb{C}) : \forall g \in GL_n(\mathbb{C}), \forall A \in M_n(\mathbb{C}), g \cdot A := gAg^{-1}$. 证明:$\mathbb{C}[M_n(\mathbb{C})]^{GL_n(\mathbb{C})} = \mathbb{C}[\sigma_1, \ldots, \sigma_n]$, 其中对于 $A \in M_n(\mathbb{C})$, 有 $\det(\lambda I_n - A) = \lambda^n - \sigma_1(A)\lambda^{n-1} + \cdots + (-1)^n \sigma_n(A)$.

习题 **4.** $SL_n(\mathbb{C})$ 通过矩阵的左乘作用于 $M_n(\mathbb{C})$. 证明:$\mathbb{C}[M_n(\mathbb{C})]^{SL_n(\mathbb{C})} = \mathbb{C}[\det]$, 其中 $\det$ 为 $M_n(\mathbb{C})$ 上的行列式函数.

习题 **5.** $SL_2(\mathbb{C})$ 通过矩阵的左乘作用于 $2 \times 4$ 阶复矩阵空间 $M_{2\times 4}(\mathbb{C})$, 确定该作用下的不变量 $\mathbb{C}[M_{2\times 4}(\mathbb{C})]^{SL_2(\mathbb{C})}$.

习题 **6.** 记 $Pol_{2,2} = \{ax_1^2 + bx_1x_2 + cx_2^2 | a, b, c \in \mathbb{C}\}$ 为两个变元的二次齐次复系数多项式形成的线性空间. $SL_2(\mathbb{C})$ 通过换元作用于 $Pol_{2,2} : \forall A \in SL_2(\mathbb{C}), \forall f(x_1, x_2) \in Pol_{2,2}, (A \cdot f)(x_1, x_2) := f(y_1, y_2)$, 其中 $(y_1, y_2) = (x_1, x_2)A$. 证明:$\mathbb{C}[Pol_{2,2}]^{SL_2(\mathbb{C})} = \mathbb{C}[\Delta]$, 其中 $\Delta$ 为判别式函数 : $\forall f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$, $\Delta(f) = b^2 - 4ac$.

# 2022-03-23 Eisenstein 判别法, 结式与判别式

- Eisenstein 判别法.

习题 **1.** 设 $p$ 为素数, $\zeta_{p^n} := e^{\frac{2\pi i}{p^n}} \in \mathbb{C}$ 为一个 $p^n$ 次本原单位根.

*1.* $\Phi_p(x) := \dfrac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1}$ 为 $\mathbb{Z}[x]$ 中不可约多项式.

*2.* $\Phi_{p^n}(x) := \dfrac{x^{p^n} - 1}{x^{p^{n-1}} - 1}$ 为 $\mathbb{Z}[x]$ 中不可约多项式.

事实: 对于正整数 $N$, 分圆多项式 (cyclotomic polynomial) $\Phi_N(x) := \prod\limits_{\substack{1\le i\le N\\(i,N)=1}} (x-\zeta_N^i)$ 为不可约的整系数多项式.

习题 **2.** 证明一个多项式的不可约性.

*1.* 证明 $f := x^n + tx^{n-1} + \cdots + tx + t$ 为二元多项式环 $\mathbb{Z}[t, x]$ 中的不可约元.

*2.* 证明 $f := x^n + x_{n-1}x^{n-1} + \cdots + x_1x + x_0$ 为 $n+1$ 元多项式环 $\mathbb{Z}[x_0, \cdots, x_{n-1}, x]$ 中的不可约元.

- 结式与判别式

设 $A$ 为 UFD, $f(x) = a_nx^n + \cdots + a_0, g(x) = b_mx^m + \cdots + b_0 \in A[x]$, 且 $a_mb_m \neq 0$.

习题 **3.** $f, g$ 在 $A[x]$ 中存在次数大于零的公因子 $\Leftrightarrow$ 存在 $f_1, g_1 \in A[x]$, 满足:$\deg f_1 \leq n - 1, \deg g_1 \leq m - 1$, 并且 $fg_1 = gf_1$.

设 $f_1(x) = a'_{n-1}x^{n-1} + \cdots + a_0,\ g_1(x) = b'_{m-1}x^{m-1} + \cdots + b'_0 \in A[x]$, 则有

$$f(x)g_1(x) - g(x)f_1(x) = (1, x, \cdots, x^{m+n-1})M \begin{pmatrix} b'_0 \\ b'_1 \\ \vdots \\ b'_{m-1} \\ -a'_0 \\ -a'_1 \\ \vdots \\ a'_{n-1} \end{pmatrix}$$

其中 $M = M(a_0, \ldots, a_n, b_0, \ldots, b_m)$ 为如下 $m+n$ 阶方阵:

$$M = \begin{pmatrix} a_0 & & & b_0 & & \\ & \ddots & & \vdots & \ddots & \\ \vdots & & a_0 & & & b_0 \\ a_n & & & b_m & & \\ & \ddots & & & \ddots & \\ & & a_n & & & b_m \end{pmatrix}$$

定义 $f$ 和 $g$ 的结式 (resultant) 为 $\operatorname{Res}(f, g) := \det M$.

习题 **4.** $f, g$ 在 $A[x]$ 中存在次数大于零的公因子 $\Leftrightarrow \operatorname{Res}(f, g) = 0$.

习题 **5.** *1.* 设 $R$ 为交换环, $Q \in M_n(R)$, 则存在 $x_1, \ldots, x_n \in R$, 使得

$$Q \cdot (x_1, \cdots, x_n)^t = (\det Q, 0 \cdots, 0)^t$$

*2.* 存在 $f_1, g_1 \in A[x]$, 满足: $\deg f_1 \geq n-1, \deg g_1 \geq m-1$, 并且 $fg_1 - gf_1 = \operatorname{Res}(f,g)$.

习题 **6.** 设 $R$ 为整环, $a_0(t), \ldots, a_n(t), b_0(t), \ldots, b_m(t) \in R[t]$, 且有 $\deg a_i(t) \leq n-i$, $\deg b_j(t) \leq m-j, \forall 0 \leq i \leq n, 0 \leq j \leq m$. 证明:

$$\deg \det M(a_0(t), \ldots, a_n(t), b_0(t), \cdots, b_m(t)) \leq mn.$$

也即

$$M = \begin{pmatrix} a_0 & & & b_0 & & \\ & \ddots & & \vdots & \ddots & \\ \vdots & & a_0 & & & b_0 \\ a_n & & & b_m & & \\ & \ddots & & & \ddots & \\ & & a_n & & & b_m \end{pmatrix}$$

习题 **7.** 令 $B = \mathbb{Z}[a_n, b_m, x_1, \ldots, x_n, y_1, \ldots, y_m]$ 为 $m+n+2$ 个变元的多项式环. $f(x) = a_n \prod_{i=1}^{n}(x - x_i), g(x) = b_m \prod_{j=1}^{m}(x - y_j) \in B[x]$.

*1.* 存在 $h \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$, 以及 $m_{ij} \geq 1$ 使得

$$\operatorname{Res}(f,g) = h a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (y_j - x_i)^{m_{ij}}$$

*2.* 在 $B[t]$ 中令 $f_t(x) = a_n \prod_{i=1}^{n}(x - tx_i), g_t(x) = b_m \prod_{j=1}^{m}(x - ty_j) \in B[t][x]$. 证明 $\operatorname{Res}(f_t, g_t)$ 作为 $t$ 的多项式的次数 $\deg \operatorname{Res}(f_t, g_t) \leq mn$.

*3.* 在 *1* 中, $h \in \mathbb{Z}, m_{ij} = 1, \forall i, j$.

*4.* 在 *1* 中, $h = \pm 1$.

*5.*$\mathrm{Res}(f,g)=a_n^m b_m^n\prod_{i=1}^{n}\prod_{j=1}^{m}(y_j-x_i)$.

*6.* $\mathrm{Res}(f,f')=(-1)^{\frac{n(n-1)}{2}}a_n^{2n-1}\prod_{1\le i<j\le n}(x_i-x_j)^2$

*7.* 设 $f(x)=a_n\prod_{i=1}^{n}(x-x_i)=a_nx^n+\ldots+a_0$，定义 $f$ 的判别式 (discriminant) 为 $\Delta(f):=a_n^{2n-2}\prod_{1\le i<j\le n}(x_i-x_j)^2$. 证明:$\mathrm{Res}(f,f')=(-1)^{\frac{n(n-1)}{2}}a_n\Delta(f)$，并由此证明 $\Delta(f)$ 为变量 $a_0,\ldots,a_n$ 的 $2n-2$ 次齐次多项式.

*8.* 设 $f(x)=a_2x^2+a_1x+a_0$, 验证 $\Delta(f)=a_1^2-4a_0a_2$. 设 $f(x)=a_3x^3+a_2x^2+a_1x+a_0$, 求 $\Delta(f)$.

注: 可以证明, 对于 $f(x)=a_nx^n+\ldots+a_0, g(x)=b_mx^m+\ldots+b_0, \mathrm{Res}(f,g)$ 作为 $a_i,b_j$ 的多项式为不可约多项式, $\Delta(f)$ 作为 $a_i$ 的多项式为不可约多项式.

- 一些应用

习题 **8.** 设 $f(x,y),g(x,y)\in\mathbb{C}[x,y]$ 为互素的非零多项式, 记 $V(f,g):=\{(a,b)\in\mathbb{C}^2\mid f(a,b)=g(a,b)=0\}$ 为 $f$ 和 $g$ 的公共零点. 证明:

*1.* $V(f,g)$ 为有限集.

*2.*$|V(f,g)|\le\deg f\cdot\deg g$.

习题 **9.** 应用结式证明整性.

*1.* 令 $R=\mathbb{Z}[a_0,\ldots,a_{n-1},b_0,\ldots,b_{m-1},\alpha,\beta]$ 为 $n+m+2$ 个变元的多项式环. 令 $f(x)=x^n+a_{n-1}x^{n-1}=\ldots+a_0$, $g(x)=x^m+b_{m-1}x^{m-1}+\ldots+b_0\in R[x]$ 为 $\alpha$ 和 $\beta$ 的零化不可约多项式. 记 $\gamma=\alpha+\beta\in R$. 证明: 存在系数在 $\mathbb{Z}[a_0,\ldots,a_{n-1},b_0,\ldots,b_{m-1}]$

中的首一多项式 $h(x)$, 使得:

$$\mathrm{Res}(f(\gamma - x), g(x)) = h(\gamma)$$

*2.* 设 $\varphi\colon A \to B$ 为环同态, 设 $\alpha, \beta \in B$ 均在 $A$ 上整, 证明: $\alpha + \beta$ 在 $A$ 上整.

*3.* 设 $\varphi\colon A \to B$ 为环同态, 设 $\alpha, \beta \in B$ 均在 $A$ 上整, 证明:$\alpha\beta$ 在 $A$ 上整.

注: 事实上有如下等价命题:

(1) $b \in B$ 在 $A$ 上整;

(2) $A[b]$ 为有限生成 $A$-模;

(3) 存在 $B$ 的子环 $C$, 且 $\varphi(A) \subset C$, 使得 $C$ 作为 $A$-模是有限生成的, 且 $b \in C$.

# 2022-03-28 伴随方阵技巧, 模的正合列

为方便理解, 以下环均值交换环.

- 伴随方阵技巧.

习题 **1.** (Cayley-Hamilton) 设 $M$ 为有限生成 $A$-模, $\varphi \in End_A(M)$, 证明: 存在首一多项式 $f(x) \in A[x]$, 使得 $f(\varphi) = 0 \in End_A(M)$.

习题 **2.** 设 $A \to B$ 为环同态.

*1.* 设 $a \in B$, 则 $a$ 在 $B$ 上整 $\Leftrightarrow A[a]$ 为有限生成 $A$-模.

*2.* 设 $a \in B$, 则 $a$ 在 $B$ 上整 $\Leftrightarrow$ 存在 $B$ 的子环 $C$, 使得 $a \in C$, 并且 $C$ 为 $B$ 的有限生成 $A$-子模.

*3.* 设 $a, b \in B$ 均在 $A$ 上整, 则 $a + b, ab$ 也在 $A$ 上整.

习题 **3.** 设 $M$ 为有限生成 $A$-模, $\varphi \in End_A(M)$, 并设 $\varphi$ 为满同态. 证明:$\varphi$ 为单同态, 从而为同构.

- 正合列.

习题 **4.** 研究 $\mathrm{Hom}_A(N, -)$ 函子的正合性.

*1.* 设 $0 \to M' \xrightarrow{u} M \xrightarrow{v} M''$ 为 $A$-模正合列. 设 $N$ 为 $A$-模, 证明以下为 $A$-模正合列:

$$0 \to \mathrm{Hom}_A(N, M') \xrightarrow{u\circ} \mathrm{Hom}_A(N, M) \xrightarrow{v\circ} \mathrm{Hom}_A(N, M'')$$

*2.* 设 $0 \to M' \xrightarrow{u} M \xrightarrow{v} M''$ 为 $A$-模复形 (即 $v \circ u = 0$), 并设对任意 $A$-模 $N$, 以下

为 $A$-模正合列:

$$0 \to \mathrm{Hom}_A(N, M') \xrightarrow{u\circ} \mathrm{Hom}_A(N, M) \xrightarrow{v\circ} \mathrm{Hom}_A(N, M'')$$

证明: 为 $A$-模正合列.

习题 **5.** 研究 $\mathrm{Hom}_A(-, N)$ 函子和 $-\otimes_A N$ 函子的正合性.

*1.* 设 $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ 为 $A$-模正合列, 设 $N$ 为 $A$-模, 证明: 以下为 $A$-模正合列:

$$0 \to \mathrm{Hom}_A(M'', N) \xrightarrow{\circ v} \mathrm{Hom}_A(M, N) \xrightarrow{\circ u} \mathrm{Hom}_A(M', N)$$

*2.* 设 $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ 为 $A$-模复形 (即 $v \circ u = 0$), 并设对任意 $A$-模 $N$, 以下为正合列:

$$0 \to \mathrm{Hom}_A(M'', N) \xrightarrow{\circ v} \mathrm{Hom}_A(M, N) \xrightarrow{\circ u} \mathrm{Hom}_A(M', N)$$

证明: $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ 为 $A$-模正合列.

*3.* 设 $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3 \to 0$ 为 $A$-模复形. 则其为正合列 $\Leftrightarrow$ 对任意 $A$-模 $N$,

$$M_1 \otimes_A N \xrightarrow{\varphi\otimes id} M_2 \otimes_A N \xrightarrow{\psi\otimes id} M_3 \otimes_A N \to 0$$

为正合列.

习题 **6.** (蛇引理) 设以下为 $A$-模的交换图表, 并且上下两行均为 (短) 正合列:

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r] \arrow[d, "f"] & M \arrow[r] \arrow[d, "g"] & N \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & L' \arrow[r] & M' \arrow[r] & N' \arrow[r] & 0
\end{tikzcd}$$

证明: 有以下 $A$-模的 (长) 正合列:

$$0 \to \ker f \to \ker g \to \ker h \to \mathrm{coker} f \to \mathrm{coker} g \to \mathrm{coker} h \to 0.$$

也即:

$$\begin{tikzcd}
0 \arrow[r] & \ker f \arrow[r] \arrow[d] & \ker g \arrow[r] \arrow[d] & \ker h \arrow[d] \arrow[dddll, rounded corners] & \\
0 \arrow[r] & L \arrow[r, "\varphi"] \arrow[d, "f"] & M \arrow[r, "\psi"] \arrow[d, "g"] & N \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & L' \arrow[r, "\varphi'"] \arrow[d] & M' \arrow[r, "\psi'"] \arrow[d] & N' \arrow[r] \arrow[d] & 0 \\
 & \mathrm{coker} f \arrow[r] & \mathrm{coker} g \arrow[r] & \mathrm{coker} h \arrow[r] & 0
\end{tikzcd}$$

注: 特别地, $f, g, h$ 中任意两个为同构蕴含第三个也为同构 (短五引理).

# 2022-04-02 复形与上同调，单形的同调群

● 复形与上同调

设 $A$ 为交换环.

**定义** 1. 一个 $A$-模复形 (complex)$(C^\bullet, d^\bullet)$ 是指对每个 $i \in \mathbb{Z}$, 给定一个 $A$-模 $C^i$, 以及一个 $A$-模同态 $d^i \colon C^i \to C^{i+1}$, 并且满足 $\forall i \in \mathbb{Z}, d^{i+1} \circ d^i = 0$. 称 $H^i(C^\bullet) := \ker d^i / \mathrm{Im} d^{i-1}$ 为复形 $(C^\bullet, d^\bullet)$ 的第 $i$ 阶上同调群 (cohomology group).

**注** 1. 复形 $(C^\bullet, d^\bullet)$ 为正合列当且仅当 $H^i(C^\bullet) = 0, \forall i \in \mathbb{Z}$.

**定义** 2. $A$-模复形 $(C^\bullet, d^\bullet)$,$(C'^\bullet, d'^\bullet)$ 之间的一个同态 $\varphi^\bullet$ 是指对任意 $i \in \mathbb{Z}$, 给定一个 $A$-模同态 $\varphi^i \colon C^i \to C'^i$, 并且满足 $\forall i \in \mathbb{Z}, \varphi^{i+1} \circ d^i = d'^i \circ \varphi^i$. 即有以下交换图表:

$$\begin{tikzcd}
{} \arrow[r] & C^i \arrow[r, "d^i"] \arrow[d, "\varphi^i"] & C^{i+1} \arrow[r, "d^{i+1}"] \arrow[d, "\varphi^{i+1}"] & C^{i+2} \arrow[r] \arrow[d, "\varphi^{i+2}"] & {} \\
{} \arrow[r] & C'^i \arrow[r, "d'^i"] & C'^{i+1} \arrow[r, "d'^{i+1}"] & C'^{i+2} \arrow[r] & {}
\end{tikzcd}$$

习题 **1.** $(C'^\bullet, d'^\bullet) \xrightarrow{\varphi^\bullet} (C^\bullet, d^\bullet)$ 为 $A$-模复形同态, 则对任意 $i \in \mathbb{Z}$, $\varphi^\bullet$ 自然诱导了上同调群之间的一个 $A$-模同态 $H^i(\varphi^\bullet) : H^i(C'^\bullet) \to H^i(C^\bullet)$.

**定义** 3. 称 $0 \to (C'^\bullet, d'^\bullet) \xrightarrow{\varphi^\bullet} (C^\bullet, d^\bullet) \xrightarrow{\psi^\bullet} (C''^\bullet, d''^\bullet) \to 0$ 为 $A$-模复形的一个短正合列, 如果 $\varphi^\bullet, \psi^\bullet$ 为复形同态, 并且对任意 $i \in \mathbb{Z}$, $0 \to C'^i \xrightarrow{\varphi^i} C^i \xrightarrow{\psi^i} C''^i \to 0$ 为 $A$-模的短正合列.

习题 **2.** (复形的短正合列诱导上同调的长正合列) 设 $0 \to (C'^{\bullet}, d'^{\bullet}) \xrightarrow{\varphi^{\bullet}} (C^{\bullet}, d^{\bullet}) \xrightarrow{\psi^{\bullet}} (C''^{\bullet}, d''^{\bullet}) \to 0$ 为 $A$-模复形的一个短正合列, 则有上同调群的长正合列:

$$\to H^i(C'^{\bullet}) \xrightarrow{H^i(\varphi^{\bullet})} H^i(C^{\bullet}) \xrightarrow{H^i(\psi^{\bullet})} H^i(C''^{\bullet}) \xrightarrow{\delta^i} H^{i+1}(C'^{\bullet}) \xrightarrow{H^{i+1}(\varphi^{\bullet})}$$

- 单形的同调群

设 $n$ 为正整数. 对 $0 \leq m \leq n$, 定义 $C_m(\Delta_n)$ 为符号集合 $\{\langle e_{i_0} e_{i_1} \cdots e_{i_m} \rangle \mid 0 \leq i_0 \leq i_1 \leq \ldots \leq i_m \leq n\}$ 中的元素作为基生成的自由 $\mathbb{Z}$-模. 对于 $1 \leq m \leq n$, 定义同态 $\partial_m \colon C_m(\Delta_n) \to C_{m-1}(\Delta_n)$ 在基上的作用为:

$$\partial_m(\langle e_{i_0} e_{i_1} \cdots e_{i_m} \rangle) = \sum_{j=0}^{m} (-1)^j \langle e_{i_0} \cdots \hat{e}_{i_j} \cdots e_{i_m} \rangle.$$

其中 $\langle e_{i_0} \cdots \hat{e}_{i_j} \cdots e_{i_m} \rangle$ 表示删去 $e_{i_j}$, 即 $\langle e_{i_0} \cdots \hat{e}_{i_j} \cdots e_{i_m} \rangle := \langle e_{i_0} \cdots e_{i_{j-1}} e_{i_{j+1}} \cdots e_{i_m} \rangle$.

习题 **3.** 证明:$\forall 1 \leq i \leq n-1, \partial_i \circ \partial_{i+1} = 0$.

记 $(C_{\bullet}(\Delta_n), \partial_n)$ 为如下复形:

$$\cdots \xrightarrow{\partial_{n+2}} 0 \xrightarrow{\partial_{n+1}} C_n(\Delta_n) \xrightarrow{\partial_n} C_{n-1}(\Delta_n) \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_2} C_1(\Delta_n) \xrightarrow{\partial_1} C_0(\Delta_n) \xrightarrow{\partial_0} 0 \xrightarrow{\partial_{-1}} \cdots$$

记 $H_i(\Delta_n) := \ker\ \partial_i / \mathrm{Im}\ \partial_{i+1}$, 称为 $n$-单形 $\Delta_n$ 的第 $i$ 阶同调群 (Homology group).

习题 **4.** 证明:

$$H_i(\Delta_n) = \begin{cases} \mathbb{Z}, i = 0; \\ 0, i \neq 0. \end{cases}$$

一般地, 对于一个集合 $S$, 指定其上的一个全序 "$<$", 定义 $C_m(\langle S\rangle)$ 为 $\{\langle e_0\cdots e_m\rangle \mid e_j\in S, e_0<e_1<\cdots<e_m\}$ 为基生成的自由 $\mathbb{Z}$-模, 定义边缘同态 $\partial_m\colon C_m(\langle S\rangle)\to C_{m-1}(\langle S\rangle)$ 为

$$\partial_m(\langle e_0\cdots e_m\rangle)=\sum_{j=0}^{m}(-1)^j\langle e_0\cdots\hat{e}_j\cdots e_m\rangle$$

这样得到复形 $(C_\bullet(\langle S\rangle),\partial_\bullet,\partial_\bullet)$, 同样的方法可以验证:

$$H_i(C_\bullet(\langle S\rangle))=\begin{cases}\mathbb{Z}, i=0;\\ 0, i\neq 0.\end{cases}$$

为方便计算或其它应用, 我们还经常使用复形 $(C'_\bullet(\langle S\rangle),\partial'_\bullet)$ 和 $(C''_\bullet(\langle S\rangle),\partial''_\bullet)$. 其定义为: $C'_m(\langle S\rangle)$ 为 $\{\langle e_0\cdots e_m\rangle \mid e_j\in S, \forall 0\le j\le m\}$ 为基生成的自由 $\mathbb{Z}$-模, $C''_m(\langle S\rangle)$ 为 $C'_m(\langle S\rangle)$ 商去 $\{\langle e_0\cdots e_m\rangle+(-1)^{\epsilon(\sigma)}\langle e_{\sigma(0)}\cdots e_\sigma(m)\rangle \mid e_0,\ldots,e_m\in S,\sigma\in\mathfrak{S}\}$ 生成的 $\mathbb{Z}$-子模得到的商模. $\partial'_\bullet$ 和 $\partial''_\bullet$ 的定义与前面类似. 可以验证, 对任意 $i\in\mathbb{Z}$, 有 $H_i(C_\bullet(\langle S\rangle))\simeq H_i(C'_\bullet(\langle S\rangle))\simeq H_i(C''_\bullet(\langle S\rangle))$.

## 阅读材料: 从单形构造一般的上同调

- 群的上同调

设 $G$ 为群, $V$ 为 $\mathbb{Z}[G]$-模. 注意到对于复形 $(C'_\bullet(\langle G\rangle),\partial'_\bullet)$, $C'_m(\langle G\rangle)$ 为 $\mathbb{Z}[G]$-模: $g\cdot\langle g_0g_1\cdots g_m\rangle=\langle(gg_0)(gg_1)\cdots(gg_m)\rangle$, 并且 $\partial'_m$ 为 $\mathbb{Z}[G]$-模同态. 将函子 $\mathrm{Hom}_{\mathbb{Z}[G]}(-,V)$ 作用到 $\mathbb{Z}[G]$-模复形 $(C'_\bullet(\langle G\rangle),\partial'_\bullet)$ 上, 即得到复形 $(C^\bullet(G,V),d^\bullet)$. 即对于 $m\ge 0$, 定义 $C^m(G,V):=\mathrm{Hom}_{\mathbb{Z}[G]}(C'_m(\langle G\rangle),V)$, 而对于 $f\in C^m(G,V)$, $d^m(f):=f\circ\partial'_{m+1}\in C^{m+1}(G,V)$. 上同调群 $H^m(G,V)$ 定义为 $H^m(C^\bullet(G,V))$.

我们将按此方式定义的复形与课上定义的群上同调的复形进行比较:

设 $G$ 为群, $V$ 为 $\mathbb{Z}[G]$-模, 对 $n \geq 1$, 记 $C^n(G,V) := \{f \colon G^n \to V\}$. 定义 $d \colon C^n(G,V) \to C^{n+1}(G,V)$, 使得对于 $f \in C^n(G,V)$,

$$df(g_1,\dots,g_{n+1}) = g_1 f(g_1^{-1}g_2,\dots,g_1^{-1}g_{n+1}) + \sum_{i=1}^{n+1}(-1)^i f(g_1,\dots,g_{i-1},\hat{g}_i,g_{i+1},\dots,g_{n+1}).$$

事实上, 两处定义的 $C^n(G,v)$ 可自然对应起来, 即 $C'_n(\langle G\rangle)$ 到 $V$ 的 $\mathbb{Z}[G]$-模同态和 $G^n$ 到 $V$ 的映射是一回事, 这是因为 $C'_n(\langle G\rangle)$ 为自由 $\mathbb{Z}[G]$-模, 且其定义给出的一组 $\mathbb{Z}$-基恰对应到 $G^{n+1}$, 由上面乘法的定义, 我们取其中 $g_0 = 1$ 的元素将给出 $\mathbb{Z}[G]$-模的生成元, 且可验证成为一组基.

但此时给出的微分 $d$ 与课上给的并不一致, 事实上二者相差一个自同构:

对任意 $n \geq 1$, 定义双射 $\alpha_n \colon G^n \to G^n$ 为 $\alpha_n(x_1,x_2,\dots,x_n) = (g_1,\dots,g_n)$, 其中

$$\begin{cases} g_1 = x_1 \\ g_2 = x_1x_2 \\ \vdots \\ g_n = x_1\cdots x_n \end{cases}$$

$\alpha_n$ 诱导双射 $\beta_n \colon C^n(G,V) \to C^n(G,V)$, 使得对 $f \in C^n(G,V), \beta_n(f) = \alpha_n \circ f$. 验证有如下交换图表:

$$\begin{tikzcd} C^n(G,V) \arrow[r, "d"] \arrow[d, "\beta_n"] & C^{n+1}(G,V) \arrow[d, "\beta_{n+1}"] \\ C^n(G,V) \arrow[r, "\tilde{d}"] & C^{n+1}(G,V) \end{tikzcd}$$

其中同态 $\tilde{d}\colon C^n(G,V)\to C^{n+1}(G,V)$ 满足对于 $f\in C^n(G,V)$, $\tilde{d}f(g_1,\ldots,g_{n+1})=$

$$g_1f(g_2,\ldots,g_{n+1})+\sum_{i=1}^{n}(-1)^i f(g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_{n+1})+(-1)^{n+1}f(g_1,\ldots,g_n).$$

可以验证 $\beta$ 诱导了上同调之间的同构, 于是采取两种定义的结果一致.

- Čech 上同调

设 $X$ 为拓扑空间, $\mathcal{U}=U_i|i\in I$ 为 $X$ 中的一族开集, 其中 $I$ 为指标集 (固定其上的一个全序 "$<$"). 设 $X=\cup_{i\in I}U_i$(我们称 $\mathcal{U}$ 为 $X$ 的一个开覆盖). 对于 $i_0,\ldots,i_m\in I$, 记 $U_{i_0\cdots i_m}:=U_{i_0}\cap\cdots\cap U_{i_m}$. 对于 $X$ 的一个非空开集 $U$, 称函数 $f\colon U\to\mathbb{Z}$ 为局部常值的, 如果 $f$ 在 $U$ 的每个连通分支上都是常值映射. 记 $\mathbb{Z}(U)$ 为所有局部常值函数 $f\colon U\to\mathbb{Z}$ 在函数的加法下形成的 Abel 群. 约定 $\mathbb{Z}(\varnothing)=0$ 为零 Abel 群. 不严格地看, 将 "函子" $\mathbb{Z}(U_\bullet)$ 作用到复形 $(C_\bullet(<I>),\partial_\bullet)$ 上, 即得到 Čech 复形 $((\mathcal{U},X),\delta^\bullet)$. 严格而言, 对于 $m\geq 0$

$$\check{C}^m(\mathcal{U},X):=\prod_{i_0<i_1<\cdots<i_m,i_j\in I}\mathbb{Z}(U_{i_0\cdots i_m})$$

对于 $f=(f_{i_0\cdots i_m})\in\check{C}^m(\mathcal{U},X)$, 以及 $i_0<\cdots<i_{m+1}$,

$$\delta^m(f)_{i_0\cdots i_{m+1}}:=\sum_{j=0}^{m+1}(-1)^j f_{i_0\cdots\hat{i}_j\cdots i_{m+1}}.$$

开覆盖 $\mathcal{U}$ 下的第 $i$ 阶 Čech 上同调群定义为 $\check{H}^i(\mathcal{U},X):=H^i(\check{C}^\bullet(\mathcal{U},X))$. 可以证明当 $X$ 为比较好的拓扑空间 (如微分流形), $\mathcal{U}$ 充分细时, $\check{H}^i(\mathcal{U},X)$ 不依赖 $\mathcal{U}$, 从而我们将 $\check{H}^i(\mathcal{U},X)$ 记为 $\check{H}^i(\mathcal{U})$, 称为 $X$ 的第 $i$ 阶 Čech 上同调群.

## 2022-04-11 自由模, 模同态的行列式

设 $A$ 为交换环.

习题 **1.** 设 $P, Q \in M_n(A)$, 则 $\det(PQ) = \det P \cdot \det Q$.

习题 **2.** 设 $P \in M_{m\times n}(A), Q \in M_{n\times m}(A)$, 且 $m > n$, 则 $\det(PQ) = 0$.

习题 **3.** 设 $\varphi\colon A^n \to A^m$ 为 $A$-模之间的满同态, 则 $n \geq m$.

习题 **4.** 本题考虑习题 3 的对偶命题.

*1.* 设 $P \in M_n(A)$ 且 $\det P = 0$, 则存在非零列向量 $x \in A^n$, 使得 $Px = 0$.

*2.* 设 $P \in M_{n\times m}(A)$ 且 $m \geq n$. 则存在非零列向量 $x \in A^m$, 使得 $Px = 0$.

*3.* 设 $\varphi\colon A^n \to A^m$ 为 $A$-模之间的单同态, 则 $n \leq m$.

习题 **5.** 设 $f_1, \dots, f_m$ 为自由模 $A^n$ 的一组生成元, 则

*1.* $m \geq n$.

*2.* 如果 $A$ 为局部环, 则存在 $f_1, \dots, f_m$ 中的 $n$ 个元素成为 $A^n$ 的一组基.

## 阅读材料: 向量丛

向量丛是非常重要的对象, 其截面 (section) 是模的例子的重要来源.

**定义** 1. 设 $n$ 为正整数, 设 $\pi\colon E \to X$ 为拓扑空间 (微分流形, 复流形, 代数簇,$\cdots$) 之间的连续 (光滑, 全纯, 正则,$\cdots$) 映射, 并且对任意 $x \in X$, 纤维 $E_x := \pi^{-1}(x)$ 为一个 $n$ 维 $\mathbb{C}$-线性空间. 如果对任意 $x \in X$, 存在 $x$ 的开邻域 $U_x$, 以及同胚 (微分同胚, 全纯

同构, 代数簇同构,$\cdots$) $\varphi_x\colon \pi^{-1}(U_x) \xrightarrow{\sim} U_x \times \mathbb{C}^n$), 满足:

- $\pi|_{\pi^{-1}(U_x)} = p_1 \circ \varphi_x$, 其中 $p_1\colon U_x \times \mathbb{C}^n \to U_x$ 为到第一个因子的投影映射.
- $\forall y \in U_x$, $\varphi$ 限制在 $E_y$ 上为 $\mathbb{C}$-线性空间同构 $E_y \xrightarrow{\sim} y \times \mathbb{C}^n$.

则我们称 $E$ 为 $X$ 上的一个秩为 $n$ 的复向量丛 (vector bundle). 如果上面将 $\mathbb{C}$ 全换为 $\mathbb{R}$, 就得到实向量丛的概念. 秩为 1 的向量丛也被称为线丛 (line bundle).

例 **1.** $E = X \times \mathbb{C}^n$, $\pi$ 为到 $X$ 的投影. 这样得到的向量丛 $E$ 称为平凡向量丛.

例 **2.** (无限长 Möbius 带) 令 $\tilde{E} = [0,1] \times \mathbb{R}$. 将 $\tilde{E}$ 中的点 $(0,y)$ 与 $(1,-y)$ 粘合 $(\forall y \in \mathbb{R})$ 得到商空间 $E$. 令 $\pi^{-1}\colon E \to S^1$, $[(x,y)] \mapsto e^{2\pi i x}$, 则得到 $S^1$ 上的实线丛.

例 **3.** (射影空间上的 tautological bundle) 回忆复射影空间 $\mathbb{CP}^n = \mathbb{C}^{n+1}\backslash 0/\sim$ 中的每个点 $[L]$ 代表了 $\mathbb{C}^{n+1}$ 中的一条过原点的直线 $L$. 考虑乘积空间 $\mathbb{CP}^n \times \mathbb{C}^{n+1}$ 中如下定义的子空间

$$\mathcal{O}(-1) := \{([L], x) \in \mathbb{CP}^n \times C^{n+1} \mid x \in L\}$$

令 $\pi\colon \mathcal{O}(-1) \to \mathbb{CP}^n$ 为到第一个因子的投影映射. 则 $\mathcal{O}(-1)$ 为 $\mathbb{CP}^n$ 上的复线丛.

同样的构造可以得到实射影空间 $\mathbb{RP}^n$ 上的实线丛, 并且这样得到的 $\mathbb{RP}^1 \simeq S^1$ 上的实线丛同构于上面例子的无限长 Möbius 带.

例 **4.** 设 $M$ 为微分流形, $TM(T^*M)$ 为其所有点处的切空间 (余切空间) 形成的微分流形, 则带上到 $M$ 的自然映射后, $TM(T^*M)$ 为 $M$ 上的向量丛, 称为 $M$ 的切丛 (余切丛).

设 $\pi\colon E \to X$ 为拓扑空间 (微分流形, 复流形, 代数簇,$\cdots$) 上的复向量丛, 一个连续

(光滑, 全纯, 正则,$\cdots$) 映射 $s\colon X \to E$ 称为 $E$ 的一个截面 (section), 如果 $\pi \circ s = id$. 记 $E$ 的所有截面形成的集合为 $\Gamma(X, E)$. 设 $R$ 为 $X$ 上的所有复值连续 (光滑, 全纯, 正则,...) 函数形成的交换环, 则 $\Gamma(X, E)$ 为 $R$-模: $\forall f \in R, s \in \Gamma(X, E)$, $(f \cdot s)(x) := f(x) \cdot s(x)$. 其中 $f(x) \cdot s(x)$ 为线性空间 $E_x$ 中的数乘.(加法类似定义)

习题 **6.** 如果 $E$ 为秩 $n$ 的平凡向量丛, 则 $\Gamma(X, E)$ 为秩 $n$ 的自由 $R$-模.

# 2022-04-16,04-17 第二轮口试题目

注: 本轮口试为学生自主准备内容, 提前两周准备, 讲授 40 分钟. 许金兴老师提供了四个选题, 我们将其整理如下. 当然, 我们鼓励同学们自主准备其他选题.

**选题 1. PID 上有限生成模的结构**

叙述并证明主理想整环 (PID) 上有限生成模的结构定理, 并利用该定理来看方阵的 Jordan 标准形与线性变换的循环子空间分解.

**选题 2. 模的局部化**

设 $A$ 为交换环, $M$ 为 $A$-模. 设 $S \subset A$ 为一个乘法子集 ($1 \in S$, 且 $\forall s_1,\ s_2 \in S,\ s_1s_2 \in S$). 定义 $M \times S$ 上的一个关系 $\sim$ 如下:

$$(m_1, s_1) \sim (m_2, s_2) \Leftrightarrow \exists s \in S, s(s_2m_1 - s_1m_2) = 0$$

验证这是一个等价关系. 将等价类 $[(m, s)]$ 记作 $\dfrac{m}{s}$. 将等价类集合 $M \times S/\sim$ 记作 $M_S$ 或 $S^{-1}M$. 与环的局部化类似, 如果 $S$ 为 $A$ 的素理想 $P$ 的补集, 则通常将 $M_S$ 记作 $M_P$, 称为 $M$ 在素理想 $P$ 处的局部化.

定义 $M_S$ 上的加法运算为 $\dfrac{m_1}{s_1} + \dfrac{m_2}{s_2} := \dfrac{s_2m_1 + s_1m_2}{s_1s_2}$, 数乘作用为 : $\dfrac{a}{s_1}\dfrac{m}{s_2} := \dfrac{am}{s_1s_2}$. 验证这两个定义都是良好的, 并且 $M_S$ 由此成为一个 $A_S$-模.

命题 **1.** 有如下的 $A_S$-模同构:

$$\varphi\colon M\otimes_A A_S \xrightarrow{\sim} M_S$$
$$m\otimes\frac{a}{s}\mapsto\frac{am}{s}$$

命题 **2.** $-\otimes_A A_S\colon M\mapsto M_S$ 为一正合函子, 即对任意 $A$-模的短正合列 $0\to M_1\to M_2\to M_3\to 0$, 有 $A_S$-模的短正合列 : $0\to M_{1S}\to M_{2S}\to M_{3S}\to 0$.

命题 **3.** 设 $m\in M$, 且对任意极大理想 $P\subset A$, $m$ 在自然同态 $M\to M_P$ 下的像为 0, 则在 $M$ 中 $m=0$.

下面讨论 Dedekind 整环上的分式理想与理想类群的关系. 可以先阅读 2022−03−16 习题课讲义的阅读材料: Dedekind 整环的理想类群. 设 $A$ 为 Dedekind 整环, $K$ 为其分式域, 从而也为 $A$-模. 我们称 $K$ 的一个非零的有限生成 $A$-子模为 $A$ 的分式理想. 设 $M$ 为 $A$ 的一个分式理想. 由定义, $M\subset K$.

命题 **4.** 设 $M$ 为 $A$ 的一个分式理想.

*1.* 对 $A$ 的每个非零素理想 $P$, $M_p$ 为 $K$ 的 $A_P$-子模, 并且存在 $n_P\in\mathbb{Z}$, 使得 $M_P=A_P\cdot\pi_P^{n_P}$. 其中 $\pi_P$ 为 DVR $A_P$ 的极大理想的生成元.

*2.* 只有有限个非零素理想 $P$ 使得 $n_P\neq 0$. 从而

$$Div(M):=\sum_{P\in SpecA,P\neq(0)} n_P\cdot P\in Div(A)$$

为良好定义的一个除子.

*3.* 设 $N$ 为 $A$ 的一个分式理想. 则有:

$$Div(M) = Div(N) \Rightarrow M = N$$

对 $A$ 的两个分式理想 $M$, $N$, 定义 $MN$ 为 $\{mn \mid m \in M,\ n \in N\}$ 生成的 $K$ 的 $A$-子模. 容易验证, 在这个运算下, 所有 $A$ 的分式理想形成一个 Abel 群. 对于 $f \in K^*$, $Af$ 为分式理想, 称为一个主分式理想. 显然主分式理想形成一个子群. 上面的命题实际上证明了 $A$ 的除子类群 (理想类群)$Cl(A)$ 同构于 $A$ 的分式理想形成的群商去主分式理想形成的子群.

## 选题 3. Nakayama 引理

**命题 5.** (Nakayama 引理, 第一形式) 设 $(A, m)$ 为局部环, $M$ 为有限生成 $A$-模. 如果 $M = mM$, 则 $M = 0$.

**命题 6.** (Nakayama 引理, 第二形式) 设 $(A, m)$ 为局部环, $M$ 为有限生成 $A$-模, $N$ 为 $M$ 的子模. 如果 $M = N + mM$, 则 $M = N$.

**命题 7.** (Nakayama 引理, 第三形式) 设 $(A, m)$ 局部环, $M$ 有限生成 $A$-模, $x_1, \ldots, x_n \in M$. 设 $\bar{x}_1, \ldots, \bar{x}_n$ 为 $A/m$-线性空间 $M/mM$ 的生成元, 则 $x_1, \ldots, x_n$ 为 $M$ 作为 $A$-模的一组生成元.

**推论 1.** *1.* 设 $(A, m)$ 为 Noether 局部环, 并且存在 $k \geq 1$, 使得 $m^k = m^{k+1}$, 则 $m^k = (0)$.

*2.* 设 $A$ 为 Noether 整环, $P$ 为 $A$ 的非零素理想, 则理想 $P^k, k \geq 1$ 互不相同.

**推论 2.** 设 $(A,m)$ 为局部环, $M$ 为有限生成 $A$-模. 设 $M$ 为投射 (projective)$A$-模.

*1.* 存在满同态 $A^n \xrightarrow{\varphi} M$, 使得 $\bar{\varphi}\colon A^n \otimes_A A/m \to M \otimes_A A/m$ 为同构.

*2.* $M$ 为自由 $A$-模.

## 选题 4.Artin-Rees 引理

**命题 8.** (Artin-Rees 引理) 设 $A$ 为 Noether 环, $I$ 为 $A$ 的理想. $M$ 为有限生成 $A$-模. $N$ 为 $M$ 的子模, 则存在整数 $c > 0$, 使得对任意 $n \geq c$, 都有 $I^nM \cap N = I^{n-c}(I^cM \cap N)$.

**习题 1.** 设 $M$ 的一组生成元为 $x_1, \ldots, x_m$. 设 $y_1, \ldots, y_k$ 为理想 $I$ 的一组生成元. 通过以下步骤证明 Artin-Rees 引理.

*1.* 记 $R = A[T_1, \ldots, T_k]$ 为多项式环. 对 $n \geq 1$, 定义 $S_n := \{(f_1, \ldots, f_m) \in R^m \mid$ 每个 $f_i$ 均为 $n$ 次齐次多项式, 且 $\sum\limits_{i=1}^{m} f_i(y_1, \ldots, y_k)x_i \in N\}$. 证明: $I^nM \cap N = \{\sum\limits_{i=1}^{m} f_i(y_1, \ldots, y_k)x_i \mid (f_1, \cdots, f_m) \in S_n\}$.

*2.* 令 $L$ 为 $\cup_{n=1}^{\infty} S_n$ 生成的 $R^m$ 子 $R$-模. 证明: 存在有限子集 $S \subset \cup_{n=1}^{\infty} S_n$, 使得 $S$ 为 $R$-模 $L$ 的生成元.

*3.* 证明 Artin-Rees 引理.

**推论 3.** *1.* 设 $A$ 为 Noether 环, $I$ 为 $A$ 的理想, 令 $J = \cap_{n=1}^{\infty} I^n$, 则 $IJ = J$. ◊

*2.* 设 $(A,m)$ 为 Noether 局部环, 则 $\cap_{n=1}^{\infty} m^n = (0)$.

*3.* 设 $A$ 为 Noether 整环, $P$ 为 $A$ 的素理想, 则 $\cap_{n=1}^{\infty} P^n = (0)$.

以下设 $A$ 为 Noether 环, $I$ 为 $A$ 的一个理想. 对于一个 $A$-模 $M$, 对 $n \geq 1$, 有自然的 $A$-模同态 $\pi_n : M/I^{n+1}M \to M/I^nM$, 使得对于 $x \in M, \pi_n(x \bmod I^{n+1}M) =$

$x \bmod I^n M$. 令 $\hat{M}$ 为如下的 $\prod_{n=1}^{\infty} M/I^n M$ 的子模:

$$\hat{M} := \{(x_n) \in \prod_{n=1}^{\infty} M/I^n M \mid \forall n \geq 1,\ \pi_n(x_{n+1}) = x_n\}$$

我们称 $\hat{M}$ 为 $M$ 的 $I-adic$ 完备化.

推论 **4.** 对于 Noether 环上的有限生成模, $I-adic$ 完备化函子是正合的. 即设 $A$ 为 Noether 环, $I$ 为 $A$ 的一个理想, 设

$$0 \to M_1 \to M \to M_2 \to 0$$

为有限生成 $A$-模的一个短正合列, 则

$$0 \to \hat{M}_1 \to \hat{M} \to \hat{M}_2 \to 0$$

也为短正合列.

# 2022-04-18 Noether 性质

以下环均指交换环.

**例 1.** 设 $G$ 为有限群, $|G| = m$, 设 $\rho\colon G \to GL(V)$ 为 $G$ 的复线性表示. 记 $\mathbb{C}[V]$ 为 $V$ 上 $\mathbb{C}$-值多项式函数形成的环.$\rho$ 诱导了 $G$ 在 $\mathbb{C}[V]$ 上的作用:$(g \cdot f)(v) = f(g^{-1} \cdot v), \forall g \in G, f \in \mathbb{C}[V], v \in V$. 通过以下步骤证明 $G$-不变多项式函数环 $\mathbb{C}[V]^G$ 为有限生成 $\mathbb{C}$-代数.

*1.* 设 $V \simeq \mathbb{C}^n$, 则 $\mathbb{C}[V]^G \simeq \mathbb{C}[x_1, \ldots, x_n]^G$.

*2.* 对 $i = 1, \ldots, n$, 令 $f_i(x) = \prod_{g \in G}(x - gx_i) = x^m + c_{m-1}^{(i)} x^{m-1} + \ldots + c_0^{(i)} \in \mathbb{C}[x_1, \ldots, x_n, x]$. 则关于 $x$ 的多项式 $f_i(x)$ 的各个系数 $c_j^{(i)} \in \mathbb{C}[x_1, \ldots, x_n]^G$.

*3.* 令 $A = \mathbb{C}[c_j^{(i)} | 1 \le i \le n, 0 \le j \le m-1]$ 为 $\mathbb{C}[x_1, \ldots, x_n]^G$ 的子环, 则 $A$ 为 Noether 环, 并且通过自然嵌入 $A \to \mathbb{C}[x_1, \ldots, x_n], \mathbb{C}[x_1, \ldots, x_n]$ 为有限生成 $A$-模, 从而为 Noether $A$-模.

*4.* $\mathbb{C}[x_1, \ldots, x_n]^G$ 为有限生成 $A$-模.

*5.* $\mathbb{C}[x_1, \ldots, x_n]^G$ 为有限生成 $\mathbb{C}$-代数.

**习题 1.** 设 $A$ 为 Noether 环, 则 $A$ 的极小素理想个数有限.

## 阅读材料: 模的伴随素理想

以下设 $A$ 为 Noether 环. 设 $M$ 为 $A$-模. 对 $x \in M$, 令 $Ann(x) := \{a \in A | ax = 0\}$ 为 $A$ 的理想, 称为 $x$ 的零化理想. 称 $A$ 的一个素理想 $P$ 为 $M$ 的伴随素理想 (associate prime ideal), 如果存在 $x \in M$, $x \neq 0$, 使得 $P = Ann(x)$. 记 $M$ 的伴随素理

想全体为 $Ass(M)$.

习题 **2.** *1.* 设 $I$ 为 $A$ 的理想. 则存在 $x \in M$, 使得 $I = Ann(x) \Leftrightarrow$ 存在模的单同态 $A/I \hookrightarrow M$.

*2.* 设 $I$ 为集合 $\{Ann(x) | x \in M, x \neq 0\}$ 的极大元 (存在性由 $A$ 是 Noether 环保证), 则 $I$ 为 $A$ 的素理想, 从而 $I \in Ass(M)$.

*3.* 设 $M$ 为非零 $A$-模, 则 $Ass(M) \neq \varnothing$.

习题 **3.** 设 $S$ 为 $A$ 的乘法子集, $M$ 为有限生成 $A$-模. 则 $Ass(M_S)$ 与 $\{P \in Ass(M) | P \cap S = \varnothing\}$ 一一对应. 这里局部化 $M_S$ 为 $A_S$-模, 从而 $Ass(M_S)$ 为 $\mathrm{Spec}(A_S)$ 的子集, 而 $\mathrm{Spec}(A_S)$ 可以等同于 $A$ 中与 $S$ 不相交的素理想全体.

习题 **4.** $A$ 的极小素理想均为伴随素理想.

习题 **5.** *1.* 设 $0 \to M_1 \xrightarrow{i} M \xrightarrow{x} M_2 \to 0$ 为 $A$-模的短正合, 则

$$Ass(M) \subset Ass(M_1) \cup Ass(M_2).$$

*2.* 设 $M$ 为有限生成 $A$-模, 则 $Ass(M)$ 为有限集. 作为推论, Noether 环 $A$ 的极小素理想个数有限.

# 2022-04-29 期中考试

**1** 设 $A = \mathbb{Z}[i\sqrt{3}]$, 并记 $K$ 为它的分式域.

*1.1* 证明 $P = X^2 - X + 1$ 是 $A[X]$ 中的不可约多项式.

*1.2* 证明 $P$ 视作 $K[x]$ 中的多项式时是可约的.

*1.3* 得出结论: $A$ 不是唯一分解整环.

**2** 设 $A$ 为一个环. 我们称 $A$-模 $I$ 为内射的, 如果 $A$ 满足以下两个等价条件之一:

(i) 若有 $A$-模同态 $f\colon M' \to I$ 和 $A$-模单同态 $g\colon M' \to M$, 则存在 $A$-模同态 $h\colon M \to I$, 使得以下图表交换:

$$\begin{tikzcd} & I & \\ 0 \arrow[r] & M' \arrow[u, "f"] \arrow[r, "g"] & M \arrow[ul, "h"'] \end{tikzcd}$$

(ii) 形如

$$0 \longrightarrow I \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

的 $A$-模正合列均可裂.

以下假设 $I$ 和 $I'$ 为内射 $A$-模, 且有如下两个正合列:

$$0 \longrightarrow M \xrightarrow{i} I \xrightarrow{p} Q \longrightarrow 0$$

$$0 \longrightarrow M \xrightarrow{i'} I' \xrightarrow{p'} Q' \longrightarrow 0$$

*2.1* 证明: 存在 $A$-模同态 $h\colon I \to I'$, $k\colon Q \to Q'$, 使得以下图表交换:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "i"] \arrow[d, "Id_M"] & I \arrow[r, "p"] \arrow[d, "h"] & Q \arrow[r] \arrow[d, "k"] & 0 \\
0 \arrow[r] & M \arrow[r, "i'"] & I' \arrow[r, "p'"] & Q' \arrow[r] & 0
\end{tikzcd}$$

*2.2* 定义态射 $r\colon I \to Q \oplus I'$, $x \mapsto (p(x), h(x))$, $s : Q \oplus I' \to Q'$, $(q, x') \mapsto k(q) - p'(x')$. 证明有以下短正合列:

$$0 \longrightarrow I \xrightarrow{r} Q \oplus I' \xrightarrow{s} Q' \longrightarrow 0$$

*2.3* 证明 $Q \oplus I$ 与 $Q' \oplus I'$ 作为 $A$-模同构.

**3** 设 $A$ 为交换环, $I_1, \ldots, I_r$ 为 $A$ 中理想. 乘积理想 $I_1 I_2 \cdots I_r$ 定义为由形如 $x_1 x_2 \cdots x_r$ 的元素生成的理想, 其中 $x_i \in I_i$.

*3.1* 设 $\mathfrak{M}_1$, $\mathfrak{M}_2 \ldots, \ldots, \mathfrak{M}_s$ 为 $A$ 中互异的极大理想, 其中 $s \geq 2$. 证明: 对 $i = 1, \ldots, s-1$, 存在 $a_i \in \mathfrak{M}_i \backslash \mathfrak{M}_s$, 使得

$$\prod_{i=1}^{s_1} a_i \in \mathfrak{M}_1 \mathfrak{M}_2 \cdots \mathfrak{M}_{s-1} \backslash \mathfrak{M}_1 \mathfrak{M}_2 \cdots \mathfrak{M}_s$$

*3.2* 若 $A$ 作为 $A$-模是 Artin 的, 那么 $A$ 中只有有限多个极大理想.

下面我们总假设 $A$ 作为 $A$-模是 Artin 的. 记 $\mathfrak{M}_1, \ldots, \mathfrak{M}_t$ 为 $A$ 中所有极大素理想, 并令 $\mathfrak{r} = \cap_{i=1}^{t} \mathfrak{M}_i$.

*3.3* 证明存在正整数 $N$, 使得对任意不小于 $N$ 的正整数 $n$, 都有 $\mathfrak{r}^n = \mathfrak{r}^N$.

记 $\mathfrak{a} = \mathfrak{r}^N$. 以下我们用反证法证明 $\mathfrak{a} = \{0\}$. 假设 $\mathfrak{a} \neq 0$, 并记 $\mathfrak{b} = \{b \in A \mid b\mathfrak{a} = 0\}$.

*3.4* 验证 $\mathfrak{b}$ 为 $A$ 的一个理想. 假设 $\mathfrak{b} \neq A$. 证明 $B = A/\mathfrak{b}$ 有一个形如 $\mathfrak{c}/\mathfrak{b}$ 的非零的

极小 $A$-子模 (在包含关系下), 其中 $\mathfrak{c}$ 为 $A$ 的一个理想, 并证明这个子模为单模. 进一步地, 证明这个单模的零化子是 $A$ 的一个极大理想, 并得出结论: $\mathfrak{r}\mathfrak{c} \subset \mathfrak{b}$, 进而有 $\mathfrak{c} \subset \mathfrak{b}$, 得到 $\mathfrak{b} = A$ 且 $\mathfrak{a} = \{0\}$.

**4** 设 $A$ 为有限维含幺 $\mathbb{C}$-代数, 乘法单位元记为 $1_A$, 并记 $A^\times$ 为 $A$ 中所有可逆元的集合. 对 $a \in A$, 定义

$$Spec(a) = \{\lambda \in \mathbb{C} \mid a - \lambda 1_A \notin A^\times\}$$

为 $a$ 的谱. 任取 $a \in A$. 本题前四小问的目标是证明对 $\forall a \in A$, $Spec(a) \neq \varnothing$. 由于 $a = 0$ 时显然有 $Spec(0) = \{0\}$, 我们假设 $a \neq 0$.

*4.1* 假设存在无穷多个 $\lambda \in C$, 使得 $a - \lambda 1_A$ 可逆, 证明存在 $r \geq 2$ 和互异的复数 $\lambda_1, \ldots, \lambda_r$, 及非零的复数 $\mu_1, \ldots, \mu_r$, 使得对 $i = 1, \ldots, r$, 总有 $a - \lambda_i 1_A$ 可逆, 且

$$\sum_{i=1}^{r} \mu_i (a - \lambda_i 1_A)^{-1} = 0$$

.

*4.2* 证明存在正次数的多项式 $P \in \mathbb{C}[X]$, 使得 $P(a) = 0$.

*4.3* 证明 $P$ 的零点集与 $Spec(a)$ 的交非空.

*4.4* 证明 $Spec(a) \neq \varnothing$.(注意这里我们不再保留 *4.1* 中关于 $a$ 的假设)

*4.5* 若 $A$ 为可除 $C$-代数 (即 $A \backslash 0 = A^\times$), 则 $A = \mathbb{C}$.

*4.6* 假设 $a$ 为 $A$ 中一幂零元 (即存在 $N \in \mathbb{N}$ 使得 $a^N = 0$), 证明 $Spec(a) = \{0\}$

*4.7* 若 $Spec(a) = \{0\}$, 证明 $a$ 为幂零的.

*4.8* 该问的目标是证明: 在有限维代数中, 左逆、右逆、双边逆总相同.(这只需证明

左逆总是双边逆. 假设 $a \in A$ 有左逆, 也即是说存在 $b \in A$, 使得 $ba = 1_A$, 通过考虑线性映射 $R_a\colon A \to A,\ c \mapsto ac$, 证明 $ab = 1_A$.)

*4.9* 设 $a \in A$ 不为幂零元. 由前可知 $Spec(a)$ 中包含一个非零元 $\lambda$. 以下两问的目标是证明存在 $A$-单模 $S$ 使得 $a \cdot S \neq 0$.

*4.10* 证明 $A$-模 $N = A/A \cdot (a - \lambda 1_A)$ 为非零的有限生成 $A$-模.

*4.11* 我们在课堂上证明了: 所有有限生成模都有单的商模. 以此证明存在 $A$-单模 $S$, 使得 $a \cdot S \neq 0$.

# 2022-04-27 域扩张的次数 (1)

习题 **1.** 设 $L/K, K/k$ 均为域的有限扩张, 则 $[L:k]=[L:K][K:k]$.

习题 **2.** *1.* 证明:$[\mathbb{Q}(\sqrt[5]{2}):\mathbb{Q}]=5$.

*2.* 证明:$[\mathbb{Q}(\sqrt[5]{2},\sqrt{5}):\mathbb{Q}]=10$.

*3.* 证明:$[\mathbb{Q}(\sqrt[4]{2},\sqrt{5}):\mathbb{Q}]=8$.

习题 **3.** 设 $K$ 为域, $K(x)$ 为有理函数域 (即 $K[x]$ 的分式域).

*1.* $\forall\ 0\neq h\in K(x), \forall\ 0\neq f(x)\in K[x]$, 均有 $f(h)\neq 0$. 从而 $K(h)\simeq K(x)$.

*2.* $\forall\ 0\neq f(x)\in K[x]$, 且 $\deg f>0$, 有 $[K(x):K(f(x))]=\deg f$

*3.* 设 $0\neq h(x)=\dfrac{f(x)}{g(x)}\in K(x)$, 其中 $f(x),g(x)\in K[x]$ 为正次数互素多项式, 则 $[K(x):K(h(x))]=max\{\deg f,\deg g\}$.

# 2022-05-09 域扩张的次数 (2)

习题 **1.** 设 $L/K, K/k$ 均为域的有限扩张, 则 $[L:k]=[L:K][K:k]$.

例 **1.** 证明:$[\mathbb{Q}(\sqrt[5]{2},\sqrt{5}):\mathbb{Q}]=10$.

习题 **2.** 设 $E/F$ 为域的有限扩张, 且 $E=F(\alpha)$. 如果 $f(x)\in F[x]$ 为非零不可约多项式且 $f(\alpha)=0$, 则 $[E:F]=\deg f$.

方法点 **1.** 由以上习题, 为了求出域扩张次数 $[F(\alpha):F]$, 只需找到一个不可约多项式 $f(x)\in F[x]$, 使得 $f(\alpha)=0$. 在实际例子中我们通常可以先写出一个次数尽可能小的 $f(x)$ 使得 $f(\alpha)=0$, 然后想办法证明 $f$ 不可约. 为此, 可以构造一个 $F$ 的子环 $A$, 使得 $A$ 为 UFD, $f(x)\in A[x]$ 且 $A$ 的分式域为 $F$. 如果可以证明 $f(x)$ 在 $A[x]$ 中不可约, 由 Gauss 引理就可以知道 $f(x)$(差一个 $A$ 中因子的意义下) 在 $F[x]$ 中不可约. 为了证明 $f(x)$ 在 $A[x]$ 中不可约, 我们可以想办法利用 Eisenstein 判别法, 为此就需要找到 $A$ 中合适的素元 $p$.

习题 **3.** 设 $K$ 为域, $K(x)$ 为有理函数域 (即 $K[x]$ 的分式域).

*1.* $\forall\ 0\neq h\in K(x), \forall\ 0\neq f(x)\in K[x], \deg f>0$, 均有 $f(h)\neq 0$. 从而 $K(h)\simeq K(x)$.

*2.* $\forall\ 0\neq f(x)\in K[x], \deg f>0, [K(x):K(f(x))]=\deg f$.

*3.* 设 $0\neq h(x)=\dfrac{f(x)}{g(x)}\in K(x)$, 其中 $f(x),g(x)\in K[x]$ 为正次数互素多项式, 则 $[K(x):K(h(x))]=max\{\deg f,\deg g\}$.

下面的习题经常用来构造离散赋值环 (DVR). 回忆 DVR 是 UFD.

习题 **4.** 我们给出一种 DVR 的构造方法.

*1.* 设 $R=K_1\times\cdots\times K_n$ 为 $n$ 个域的乘积, 则 $R$ 中恰有 $n$ 个素理想 $P_1,\ldots,P_n$, 其中 $P_i=\{(x_1,\cdots,x_n)\in R|x_i=0\}$. 并且有 $R_{P_i}\simeq K_i$, $P_iR_{P_i}=0,\forall i=1,\ldots,n$.

*2.* 设 $F$ 为域, $f(x)\in F[x]$ 且 $(f(x),f'(x))=1$(即 $f$ 无重根), 则 $F[x]/(f(x))$ 同构于有限个域的乘积.

*3.* 设 $A\to B$ 为环同态, 主理想 $(p)$ 为 $A$ 中极大理想, 并且 $B/pB\simeq K_1\times\cdots\times K_n$ 同构于 $n$ 个域的乘积, 则 $B$ 中素理想 $P_1,\ldots,P_n$ 位于 $(p)$ 上方 (即 $P_i\cap A=(p)$), 并且局部环 $B_{P_i}$ 为 DVR, 而极大理想 $P_iB_{P_i}=pB_{P_i}$ 由 $p$ 的像生成, $p$ 为 DVR $B_{P_i}$ 中相伴意义下的唯一素元.

例 **2.** 设 $p$ 为素数, $\zeta_p=e^{\frac{2\pi i}{p}}$ 为本原 $p$ 次单位根. 考虑环同态 $\mathbb{Z}\to\mathbb{Z}[\zeta_p]$. 如果 $q\in\mathbb{Z}$ 为素数, 且 $q\neq p$, 则 $\mathbb{Z}[\zeta_p]/(q)$ 为一些域的乘积. 这是因为: 令 $B=\mathbb{Z}[x]/(x^p-1)$, 则商环 $\mathbb{Z}[\zeta_p]/(q)$ 自然为 $B/(q)$ 的商环, 而 $B/(q)\simeq\mathbb{F}_q[x]/(\bar{x}^p-1)$ 为有限个域的乘积 (无重根), 从而其商环 $\mathbb{Z}[\zeta_p]/(q)$ 也为有限个域的乘积. 任取 $\mathbb{Z}[\zeta_p]$ 中位于 $q$ 上方的素理想 $P$, 则 $\mathbb{Z}[\zeta_p]_P$ 为 DVR, 且 $q$ 为其素元.

对于正整数 $N$, 符号 $\zeta_N=e^{\frac{2\pi i}{N}}\in\mathbb{C}^*$ 代表一个本原 $N$ 次单位根.$\varphi(N)=|(\mathbb{Z}/N\mathbb{Z})^*|$ 为 *Euler* 函数.

习题 **5.** 设 $p,q$ 为不同的素数, 记 $K=\mathbb{Q}(\zeta_{pq}),F=\mathbb{Q}(\zeta_p)$. 证明:

*1.* $K=F(\zeta_q)$.

*2.* $[K:F]=\varphi(q)=q-1$.

*3.* $[K:\mathbb{Q}]=\varphi(pq)=(p-1)(q-1)$.

**习题 6.** 设 $N$ 为正整数, $N = p^m N_1$, 其中 $p$ 为素数, $(p, N_1) = 1$. 证明:

1. $[\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}] = \varphi(p^m) = p^m - p^{m-1}$.
2. 记 $K = \mathbb{Q}(\zeta_{N_1})$, 则 $[K(\zeta_{p^m}) : K] = \varphi(p^m) = p^m - p^{m-1}$.
3. $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\zeta_{N_1})(\zeta_{p^m})$.
4. $[\mathbb{Q}(\zeta_N) : \mathbb{Q}] = \varphi(N)$.

**习题 7.** 证明:$[\mathbb{Q}(\sqrt[4]{2}, \sqrt{5}) : \mathbb{Q}] = 8$.

**习题 8.** $[\mathbb{Q}(\sqrt{2+\sqrt{2}}) : \mathbb{Q}] = 4$.

**习题 9.** $[\mathbb{Q}(\sqrt[3]{2+\sqrt{3}}) : \mathbb{Q}] = 6$.

# 2022-05-14,05-15 第三轮口试题目-域扩张

习题 **1.1** 设 $K/\mathbb{Q}$ 为二次扩张 ($K$ 称为二次域). 记 $\mathcal{O}_K=\{\alpha\in K\mid 存在非零的首一多项式\ f(x)\in\mathbb{Z}[x],使得f(\alpha)=0\}$ 为 $K$ 的代数整数环.

*1.* 证明: 存在无平方因子整数 $n$, 使得 $K\simeq\mathbb{Q}(\sqrt{n})$.

*2.* 证明:$\mathcal{O}_K=\begin{cases}\mathbb{Z}\left[\dfrac{1+\sqrt{n}}{2}\right], & n\equiv 1 \mod 4;\\ \\ \mathbb{Z}[\sqrt{n}], & n\equiv 2,3 \mod 4.\end{cases}$

*3.* 对于素数 $p$, 分析 $\mathcal{O}_K$ 中位于 $(p)$ 上方的素理想个数, 并证明 $\mathcal{O}_K$ 为 *Dedeking* 整环.

习题 **1.2** 设 $N$ 为正整数, 证明有环同构 $\mathbb{Z}[\zeta_N]\simeq\mathbb{Z}[x]/(\Phi_N(x))$, 并且 $\mathbb{Z}[\zeta_N]$ 为 Dedekind 整环.

习题 **1.3** 设 $A$ 为整环, $K$ 为其分式域. 称 $A$ 为整闭整环, 如果 $A$ 在 $K$ 中的整闭包 $\{a\in K\mid a在A上整\}=A$. 证明:

*1.* UFD 为整闭整环.

*2.* 如果对 $A$ 中任意极大理想 $m$, 局部化 $A_m$ 均为整闭整环, 则 $A$ 为整闭整环.

注 **1.1** 由以上练习, 对于二次域或分圆域 $K$, 其代数整数环 $\mathcal{O}_K$ 为整闭整环.

对于域扩张 $K\xrightarrow{i}L$, 我们记 $\mathrm{Gal}(L/K):=\{\sigma\mid\sigma\colon L\xrightarrow{\sim}L为域同构, 且\sigma\circ i=i\}$, 称为域扩张 $L/K$ 的 Galois 群.

习题 **1.4** 计算下面域扩张的 Galois 群:

注: 我们本题会用到如下结论: 若 $L/K$ 为代数扩张, 而 $a\in L$ 且在 $K$ 上的极小

多项式为 $f$, 则 $\forall\sigma\in\mathrm{Gal}(L/K)$, $\sigma(a)$ 也为 $f$ 的根; 若任给一个 $f$ 在 $K(a)$ 中的根 $b$, $a\mapsto b$ 会唯一决定一个 $\tau\in\mathrm{Gal}(K(a)/K)$. 证明直接考虑 $\sigma(f(a))=f(\sigma(a))$, 以及 $K(a)$ 和 $K(b)$ 有包含关系且均与 $K[x]/(f(x))$ 同构, 即可.

*1.* $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$.

*2.* $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$, 其中 $\omega=e^{\frac{2\pi i}{3}}$ 为一个三次本原单位根.

*3.* $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$.

*4.* $\mathbb{Q}(\zeta_N)/\mathbb{Q}$.

*5.* $K/\mathbb{F}_p(t)$, 其中 $K=\mathbb{F}_p(t)[x]/(x^p-t)$, $p$ 为素数.

*6.* $K/\mathbb{F}_p(t)$, 其中 $K=\mathbb{F}_p(t)[x]/(x^p-x-1)$, $p$ 为素数.

*7.* $\mathbb{C}(t^{\frac{1}{n}})/\mathbb{C}(t)$.

*8.* $K(t)/K$, 其中 $K$ 为域.

# 2022-05-16 代数扩张与代数闭包

**定义 1.** 称域扩张 $E/F$ 为代数扩张, 如果这是环的整扩张, 即 $\forall \alpha \in E$, 存在非零的 $f(x) \in F[x]$, 使得 $f(\alpha)=0$. 如果 $f(x)$ 为首一的次数最小的零化 $\alpha$ 的 $F[x]$ 中的多项式, 则称 $f(\alpha)$ 为 $\alpha$ 在 $F$ 上的极小多项式.

**习题 1.** 设域扩张 $E/F$ 为代数扩张, $\alpha \in E$, 其在 $F$ 上的极小多项式为 $f(x)$. 如果 $g(x) \in F[x]$ 且 $g(\alpha)=0$, 则 $f(x)|g(x)$. $\diamondsuit$

**习题 2.**

*1.* 域的有限扩张为代数扩张.

*2.* 设 $E/F$, $K/E$ 均为代数扩张, 则 $K/F$ 为代数扩张.

设 $F \xrightarrow{i_1} E_1$, $F \xrightarrow{i_2} E_2$ 为代数扩张, 记 $\mathrm{Hom}_F(E_1,E_2)=\{\varphi \mid \varphi\colon E_1 \to E_2$ 为域同态 (嵌入), 且 $i_2=\varphi\circ i_1\}$.

Galois 理论中的主要问题: 研究 $\mathrm{Hom}_F(E_1,E_2)$ !

**定理 1.** 设 $F(\alpha)/F$ 为单代数扩张, 设 $f(x)\in F[x]$ 为 $\alpha$ 在 $F$ 上的极小多项式, 设 $E/F$ 为域扩张, 则

$$|\mathrm{Hom}_F(F(\alpha),E)| \le [F(\alpha):F]=\deg f$$

并且等号成立当且仅当 $f$ 在 $E$ 上恰有 $\deg f$ 个互不相同的根.

**定理 2.** 设 $E_1/F$ 为有限扩张, $E_2/F$ 为域扩张, 则

$$|\mathrm{Hom}_F(E_1,E_2)| \le [E_1:F],$$

并且等号成立

$\Leftrightarrow$ 对任意 $\alpha \in E_1$, $\alpha$ 在 $F$ 上的极小多项式 $f(x) \in F[x]$ 在 $E_2$ 上恰有 $\deg f$ 个互不相同的根

$\Leftrightarrow E_1 = F(\alpha_1. \cdots, \alpha_n)$, 并且对每个 $i = 1, \cdots, n$, $\alpha_i$ 在 $F$ 上的极小多项式 $f_i(x) \in F[x]$ 在 $E_2$ 上恰有 $\deg f_i$ 个互不相同的根.

(提示: 将 $E_1/F$ 分解为有限个单扩张的复合)

**定义 2.** 称域 $F$ 为代数封闭域, 如果对任意 $f(x) \in F[x]$, 均存在 $\alpha \in F$, 使得 $f(\alpha) = 0$.

注: 此时容易归纳得到 $f(x)$ 的所有根都在 $F$ 中.

**习题 3.** 设 $F$ 为代数封闭域, 如果 $E/F$ 为代数扩张, 则 $E = F$(严格而言, 为同构).

事实: 设 $F$ 为域, 则存在域扩张 $E/F$, 使得 $E$ 为代数封闭域.

**定义 3.** 设 $\bar{F}/F$ 为域扩张, 称 $\bar{F}$ 为 $F$ 的一个代数闭包, 如果 $\bar{F}/F$ 为代数扩张, 且 $\bar{F}$ 为代数封闭域.

**习题 4(代数闭包存在).** 设 $F$ 为域, 取域扩张 $E/F$, 使得 $E$ 为代数封闭域. 定义 $\bar{F} := \{\alpha \in E \mid \alpha\text{在}F\text{上整}\}$, 则 $\bar{F}$ 为 $E$ 的子域, 且为 $F$ 的代数闭包.

**习题 5(代数闭包的唯一性).**

*1.* 设 $E_2/F$ 为域扩张, 且 $E_2$ 为代数封闭域, 设 $E_1/F$ 为代数扩张, 则 $\mathrm{Hom}_F(E_1, E_2) \neq \varnothing$.

*2.* 设 $\bar{F}_1/F$, $\bar{F}_2/F$ 均为 $F$ 的代数闭包, 则存在 $F$-同构 $\bar{F}_1 \simeq \bar{F}_2$.

习题 **6.** 设 $E/F$ 为代数扩张, 设 $\bar{E}/E$ 为 $E$ 的代数闭包, 则 $\bar{E}/F$ 为 $F$ 的代数闭包.

习题 **7.** 设 $E/F$ 为代数扩张,$\bar{F}$ 为 $F$ 的一个代数闭包. 那么所有的域同态 $\sigma\colon F \hookrightarrow \bar{F}$ 都可以延拓到 $E$ 上, 即 $\tilde{\sigma}\colon E \hookrightarrow \bar{F}, \tilde{\sigma}|_F = \sigma$.

# 2022-05-18 可分扩张

**习题 1.** 设 $E/F$ 为域的有限扩张, $\bar{F}$ 为 $F$ 的代数闭包, 则以下三条互相等价:

*1.* $|\mathrm{Hom}_F(E,\bar{F})|=[E:F]$.

*2.* $\forall\alpha\in E$, $\alpha$ 在 $F$ 上的极小多项式 $f(x)$ 无重根, 即 $(f(x),f'(x))=1$.

*3.* $E=F(\alpha_1,\cdots,\alpha_n)$, 并且对任意 $1\le i\le n$, $\alpha_i$ 在 $F$ 上的极小多项式 $f_i(x)$ 无重根, 即 $(f_i(x),f_i'(x))$.

**定义 1.** 设 $E/F$ 为有限扩张, 如果其满足上面习题中的三个等价条件之一, 则称其为(有限) 可分扩张.

**习题 2.** 设 $E/F$, $K/E$ 均为有限扩张.

*1.* 若 $E/F$, $K/E$ 均为可分扩张, 则 $K/F$ 为可分扩张.

*2.* 若 $K/F$ 为可分扩张, 则 $E/F$, $K/E$ 均为可分扩张.

注: 对于有限扩张 $K/E,E/F$, 我们总有以下的等式成立:

$$|\mathrm{Hom}_F(K,\bar{F})|=|\mathrm{Hom}_E(K,\bar{F})|\cdot|\mathrm{Hom}_F(E,\bar{F})|$$

这不依赖于扩张的可分性.

**习题 3.** 设 $f(x)$ 为域 $F$ 上的首一不可约多项式, 则 $f$ 有重根 $\Leftrightarrow$ 域 $F$ 的特征为素数 $p$, 并且存在 $g(x)\in F[x]$, 使得 $f(x)=g(x^p)$.

**习题 4.** 设域 $F$ 的特征为 0, 则任意有限扩张 $E/F$ 均为可分扩张.

**习题 5.** 有限域 $\mathbb{F}_p$ 的任意有限扩张均为可分扩张.

- 问题: 设 $E/F$ 为有限扩张, 设 $\alpha \in E$, 如何判断 $E \overset{?}{=} F(\alpha)$?

**例 1.** 设 $a_1, \cdots, a_n$ 为无平方因子的正整数, 则 $\mathbb{Q}(\sqrt{a_1}, \cdots, \sqrt{a_n}) = \mathbb{Q}(\sqrt{a_1}+\cdots+\sqrt{a_n})$.

记 $K = \mathbb{Q}(\sqrt{a_1}, \cdots, \sqrt{a_n})$, 记自然的包含映射 $K \subset \mathbb{C}$ 为 $i$. 记 $\alpha = \sqrt{a_1} + \cdots + \sqrt{a_n}$.

*1.* 如果 $[K : \mathbb{Q}(\alpha)] = m$, 则 $|\mathrm{Hom}_{\mathbb{Q}(\alpha)}(K, \mathbb{C})| = m$, 特别地, $\forall \varphi \in \mathrm{Hom}_{\mathbb{Q}(\alpha)}(K, \mathbb{C})$, $\varphi(\alpha) = \alpha$.

*2.* $m = 1$, 进而 $K = \mathbb{Q}(\alpha)$.

这个例子启发我们可以提出以下引理:

**引理 1.** 设 $F \subset E \subset \bar{F}$ 为域扩张, 并且 $E/F$ 为有限可分扩张, $\bar{F}$ 为 $F$ 的代数闭包. 对于 $\alpha \in E$, 有 $E = F(\alpha) \Leftrightarrow \varphi \in \mathrm{Hom}_F(E, \bar{F})$, 只要 $\varphi$ 不等于包含同态 $i$, 就有 $\varphi(\alpha) \neq \alpha$.

**定理 1.** (单扩张定理) 设 $E/F$ 为有限可分扩张, 则存在 $\alpha \in E$, 使得 $E = F(\alpha)$.

## 阅读材料: Krasner 引理

设 $E$ 为域, 称一个函数 $|\cdot| : E \to \mathbb{R}_{\geq 0}$ 为域范数, 如果其满足:

- 对 $x \in E$, $|x| = 0 \Leftrightarrow x = 0$;
- 对任意 $x, y \in E$, $|x + y| \leq |x| + |y|$(三角不等式);
- 对任意 $x, y \in E$, $|x \cdot y| = |x| \cdot |y|$.

**习题 6.** 设 $|\cdot|$ 为 $E$ 上的域范数, 证明: $|1| = |-1| = 1$.

**习题 7.** $\mathbb{Q}_p$ 上的 $p$-进范数 $|\cdot|_p$ 为完备的域范数. 其中完备是指在该范数下的 Cauchy 列均在 $\mathbb{Q}_p$ 上有极限.

$\mathbb{Q}_p$ 上的 $p$-进范数 $|\cdot|_p$ 还满足如下强三角不等式:

$$|x+y|_p \leq \max\{|x|_p, |y|_p\}, \quad \forall x, y \in \mathbb{Q}_p.$$

事实: 存在代数闭包 $\bar{\mathbb{Q}}_p$ 上唯一的域范数 $|\cdot|$, 使得 $\forall x \in \mathbb{Q}_p$, 有 $|x| = |x|_p$. 而且 $|\cdot|$ 也满足强三角不等式.

**习题 8.** 设 $x, y \in \bar{\mathbb{Q}}_p$ 且 $|x| < |y|$, 则 $|x+y| = |y|$.

**定理 2.** 设 $V$ 为 $\mathbb{Q}_p$ 上的有限维线性空间, 并且 $V$ 上的两个范数 $|\cdot|_1$ 和 $|\cdot|_2$ 均使 $V$ 成为赋范 $\mathbb{Q}_p$-线性空间 (即 $|\cdot|: V \to \mathbb{R}_+$ 正定, 有三角不等式, 与 $\mathbb{Q}_p$-数乘相容), 则这两个范数等价, 即存在正实数 $C_1, C_2$, 使得对任意 $x \in V$, 均有 $C_1|x|_2 \leq |x|_1 \leq C_2|x|_2$.

**习题 9.** 设 $|\cdot|_1, |\cdot|_2$ 均为域 $E$ 上的域范数, 并且这两个范数等价, 即存在正实数 $C_1, C_2$, 使得对任意 $x \in E$, 均有 $C_1|x|_2 \leq |x|_1 \leq C_2|x|_2$, 那么 $|\cdot|_1 = |\cdot|_2$

**习题 10.** 设 $E/\mathbb{Q}_p$ 为有限扩张, 记 $|\cdot|$ 为 $\bar{\mathbb{Q}}_p$ 上范数 $|\cdot|$ 在 $E$ 上的限制. 则对任意 $\sigma \in \mathrm{Hom}_{\mathbb{Q}_p}(E, \bar{\mathbb{Q}}_p)$, 对任意 $x \in E$, 有 $|\sigma(x)| = |x|$.

**习题 11.** (Krasner 引理) 设 $\alpha \in \bar{\mathbb{Q}}_p$, 设 $f(x) \in \mathbb{Q}_p[x]$ 为 $\alpha$ 在 $\mathbb{Q}_p$ 上的极小多项式, 并设 $f(x)$ 在 $\mathbb{Q}_p$ 上的所有根 (两两互异) 为 $\{\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n\}$. 设 $\beta \in \bar{\mathbb{Q}}_p$ 满足 $|\alpha - \beta| < |\alpha_i - \beta|$, $\forall i = 2, \cdots, n$. 证明:$\mathbb{Q}_p(\alpha) \subset \mathbb{Q}_p(\beta)$.

# 2022-05-23 域扩张的超越次数, 对称多项式基本定理

• 域扩张的超越次数

回忆: 域之间代数扩张的复合还是代数扩张.

**习题 1.** 设 $K$ 为域, $f_1, f_2 \in K(x)$. 证明: 存在非零的二元多项式 $F(x, y) \in K[x, y]$, 使得 $F(f_1, f_2) = 0$.

**习题 2.** 设 $K$ 为域, $E/K(x_1, \cdots, x_n)$ 为代数扩张, $f_1, \cdots, f_{n+1} \in E$. 证明: 存在非零的 $n+1$ 元多项式 $F(x_1, \cdots, x_{n+1}) \in K[x_1, \cdots, x_{n+1}]$, 使得 $F(f_1, \cdots, f_{n+1}) = 0$.

**定义 1.** 设 $E/K$ 为域扩张, 称其为有限生成扩张, 如果存在有限个元 $a_1, \cdots, a_n \in E$, 使得 $E = K(a_1, \cdots, a_n)$.

**定义 2.** 设 $E/K$ 为域扩张, $a_1, \cdots, a_n \in E$, 若有非零的 $F(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$, 使得 $F(a_1, \cdots, a_n) = 0$, 则称 $a_1, \cdots, a_n$ 在 $K$ 上代数相关, 否则称为在 $K$ 上代数无关. 对于集合 $S \subset E$, 如果存在有限个 $a_1, \ldots, a_n \in S$ 在 $K$ 上代数相关, 则称 $S$ 中的元素在 $K$ 上代数相关, 否则称 $S$ 中的元素在 $K$ 上代数无关.

**习题 3.** 设 $E/K$ 为域的有限生成扩张.

*1.* 存在有限个元 $a_1, \cdots, a_n \in E$ 为 $K$ 上的极大代数无关组 (即 $a_1, \cdots, a_n \in E$ 在 $K$ 上代数无关, 并且 $\forall a \in E$, $a, a_1, \cdots, a_n$ 在 $K$ 上代数相关).

*2.* 设 $a_1, \cdots, a_n \in E$ 和 $b_1, \cdots, b_m \in E$ 均为 $E$ 在 $K$ 上的极大代数无关组, 则有 $n = m$.

**定义 3.** 设 $E/K$ 为域的有限生成扩张. 设 $a_1, \cdots, a_n \in E$ 为 $E$ 在 $K$ 上的极大代数无关组. 我们称 $n$ 为 $E$ 在 $K$ 上的超越次数, 记作 $\mathrm{tr.deg}\, E/K$. 由上面的习题, 超越次数不依赖于极大代数无关组的选取. 如果 $E/K$ 为代数扩张, 则极大代数无关组为空集, 此时我们约定超越次数 $\mathrm{tr.deg}\, E/K = 0$.

**习题 4.** 设 $E/F$, $F/K$ 均为域的有限生成扩张, 则有

$$\mathrm{tr.deg}\, E/K = \mathrm{tr.deg}\, E/F + \mathrm{tr.deg}\, F/K.$$

- 一个应用:对称多项式基本定理

设 $K \xrightarrow{i} E$ 为域扩张, 我们记 $\mathrm{Gal}(E/K) := \{\sigma \mid \sigma\colon E \xrightarrow{\sim} E\text{为域同构, 且}\sigma \circ i = i\}$. 这是 $E$ 的自同构群的子群, 称为 $E/K$ 的 Galois 群.

**习题 5.** 设 $E/K$ 为域的有限扩张, 则 $|\mathrm{Gal}(E/K)| \leq [E : K]$.

置换群 $\mathfrak{S}_n$ 通过置换角标作用于多项式环 $\mathbb{Q}[x_1, \cdots, x_n]$: 对 $\sigma \in \mathfrak{S}_n$, $1 \leq i \leq n$, $\sigma x_i = x_{\sigma^{-1}(i)}$. 记 $\mathbb{Z}[x_1, \cdots, x_n]^{\mathfrak{S}_n} = \{f \in \mathbb{Z}[x_1, \cdots, x_n] \mid \sigma f = f,\ \forall \sigma \in \mathfrak{S}_n\}$ 为对称多项式形成的子环. 记 $\mathbb{Q}(x_1, \cdots, x_n)^{\mathfrak{S}_n} = \{f \in \mathbb{Q}(x_1, \cdots, x_n) \mid \sigma f = f, \forall \sigma \in \mathfrak{S}_n\}$, 这是 $\mathbb{Q}(x_1, \cdots, x_n)$ 的子域. 对 $1 \leq m \leq n$, 定义初等对称多项式

$$\sigma_m := \sum_{1 \leq i_1 < i_2 < \cdots < i_m \leq n} x_{i_1} x_{i_2} \cdots x_{i_m}.$$

**习题 6.** 按以下步骤证明对称多项式基本定理: $\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}=\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$, 并且 $\sigma_1,\cdots,\sigma_n$ 在 $\mathbb{Q}$ 上代数无关.

*1.* 记 $K=\mathbb{Q}(\sigma_1,\cdots,\sigma_n)$, $F=\mathbb{Q}(x_1,\cdots,x_n)^{\mathfrak{S}_n}$, $E=\mathbb{Q}(x_1,\cdots,x_n)$. 则 $K\subset F\subset E$, 并且 $[E:K]\leq n!$, 从而为代数扩张.

*2.* $\operatorname{tr.deg} E/\mathbb{Q}=n$.

*3.* $\sigma_1,\cdots,\sigma_n$ 在 $\mathbb{Q}$ 上代数无关.

*4.* $\mathbb{Z}[\sigma_1,\cdots,\sigma_n]\hookrightarrow\mathbb{Z}[x_1,\cdots,x_n]$ 为环的整扩张, 故 $\mathbb{Z}[\sigma_1,\cdots,\sigma_n]\subseteq\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}$ 为环的整扩张.

*5.* $\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$ 的分式域为 $K$, $\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}$ 的分式域为 $F$.

*6.* $\mathfrak{S}_n\subseteq\operatorname{Gal}(E/F)$, 从而 $[E:F]\geq n!$.

*7.* $F=K,[E:K]=n!$, 且 $\operatorname{Gal}(E/K)=\mathfrak{S}_n$.

*8.* $R:=\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$ 为整闭整环, 即对任意 $x\in Frac(R)$, 如果 $x$ 在 $R$ 上整, 则 $x\in R$.

*9.* $\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}=\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$.

**习题 7.** 设 $R$ 为交换环, 则 $R[x_1,\cdots,x_n]^{\mathfrak{S}_n}=R[\sigma_1,\cdots,\sigma_n]$.

# 2022-05-25 正规扩张

设 $E/F$ 为域的有限扩张. 取定一个代数闭包 $\bar{F}$, 并设 $F \subset E \subset \bar{F}$, 记自然包含映射为 $i$.

**定义 1.** 称 $E/F$ 为正规扩张 (normal extension), 如果对任意 $\sigma \in \mathrm{Hom}_F(E, \bar{F})$, 均有 $\sigma(E) \subseteq E$.

**习题 1.** 设 $F \subseteq E \subseteq \bar{F}$ 同上, 证明以下几条等价:

*1.* $E/F$ 为正规扩张.

*2.* $\mathrm{Gal}(E/F) \to \mathrm{Hom}_F(E, \bar{F})$, $\sigma \mapsto i \circ \sigma$ 为双射.

*3.* 对任意 $\alpha \in E$, $\alpha$ 在 $F$ 上的极小多项式 $f(x)$ 的所有根均在 $E$ 中.

*4.* 对任意 $\alpha \in E$, $\alpha$ 在 $F$ 上的极小多项式 $f(x)$ 在 $E[x]$ 中分解为一些一次多项式的乘积.

*5.* $E = F(\alpha_1, \cdots, \alpha_n)$, 并且 $\forall 1 \leq j \leq n$, $\alpha_j$ 在 $F$ 上的极小多项式 $f_j(x)$ 的所有根均在 $E$ 中.

*6.* $E = F(\alpha_1, \cdots, \alpha_n)$, 并且 $\forall 1 \leq j \leq n$, $\alpha_j$ 在 $F$ 上的极小多项式 $f_j(x)$ 在 $E[x]$ 中分解为一些一次多项式的乘积.

注 1. 由上面习题, 可以看到 $E/F$ 是否为正规扩张不依赖于 $\bar{F}$ 的选取.

**习题 2.** 判断以下域扩张是否为正规扩张:

*1.* $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

*2.* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

*3.* $\mathbb{Q}(\zeta_N)/\mathbb{Q}$, 其中 $\zeta_N$ 为一个本原 $N$ 次单位根.

*4.* $E/F$, 其中 $F=\mathbb{F}_p(t)$, $E=F(t^{\frac{1}{p}})=F[x]/(x^p-t)$.

习题 **3.** 设 $E/F$, $K/E$ 为域的有限扩张.

*1.* 设 $K/F$ 为正规扩张, 则 $K/E$ 为正规扩张, 并举例说明此时 $E/F$ 不一定为正规扩张.

*2.* 举例说明如果 $E/F$, $K/E$ 均为正规扩张, 那么 $K/F$ 也不一定为正规扩张.

设 $E=F(\alpha_1,\ldots,\alpha_n)$ 为域 $F$ 的有限扩张. 取一个代数闭包 $E\subset\bar{F}$. 记 $f_j(x)\in F[x]$ 为 $\alpha_j$ 在 $F$ 上的极小多项式. 设 $f_j(x)$ 在 $\bar{F}$ 中的所有根为 $\alpha_{j1},\ldots,\alpha_{jk_j}$. 令 $\tilde{E}:=F(\alpha_{ji},\ 1\le j\le n,\ 1\le i\le k_j)$. 则 $E\subset\tilde{E}$, 并且 $\tilde{E}/F$ 为正规扩张. 我们称 $\tilde{E}$ 为 $E/F$ 的正规闭包 (normal closure). 容易验证, $\tilde{E}$ 为最小的既在 $F$ 上正规又包含 $E$ 的域.

如果 $E=F[x]/(f(x))$ 为 $F$ 上的单扩张, 则称 $\tilde{E}$ 为多项式 $f(x)\in F[x]$ 在 $F$ 上的分裂域. 具体而言, $\tilde{E}$ 为 $F$ 添加 $f(x)$ 的所有根得到.

习题 **4.** 设 $f(x)\in F[x]$ 为没有重根的首一不可约多项式, 设 $E$ 为 $f$ 在 $F$ 上的分裂域. 证明 $E/F$ 为正规且可分的扩张.

# 2022-05-30 Galois 理论基本定理

- Galois 扩张

习题 **1.** 设 $E/F$ 为有限扩张.

*1.* $|\mathrm{Gal}(E/F)| \le |\mathrm{Hom}_F(E,\bar{F})|$, 并且等号成立 $\Leftrightarrow E/F$ 为正规扩张.

*2.* $|\mathrm{Hom}_F(E,\bar{F})| \le [E:F]$, 并且等号成立 $\Leftrightarrow E/F$ 为可分扩张.

*3.* $|\mathrm{Gal}(E/F)| \le [E:F]$, 并且等号成立 $\Leftrightarrow E/F$ 为既正规又可分的扩张.

定义 **1.** 设 $E/F$ 为有限扩张. 称其为 Galois 扩张, 如果 $|\mathrm{Gal}(E/F)| = [E:F]$.

习题 **2.** 设 $E/F$ 为有限扩张, 则以下几条互相等价:

*1.* $E/F$ 为 Galois 扩张.

*2.* $E/F$ 为既正规又可分的扩张.

*3.* $E$ 为一个无重根的不可约多项式 $f(x) \in F[x]$ 在 $F$ 上的分裂域.

习题 **3.** (Artin 引理) 设 $E$ 为域, $G \subset Aut(E)$ 为 $E$ 的自同构群的有限子群. 令 $F = E^G := \{x \in E \mid gx = x,\ \forall g \in G\}$. 令 $n = |G|$. 依次证明如下命题:

*1.* $\forall \alpha \in E$, 存在 $f(x) \in F[x]$, 使得 $f(\alpha) = 0,\ \deg f \le n$, 并且 $f$ 无重根.

*2.* $E/F$ 为代数扩张, 并且对任意中间域 $F \subset E_1 \subset E$, 如果 $[E_1 : F] < +\infty$, 则 $E_1/F$ 为可分扩张, 并且 $[E_1 : F] \le n$.

*3.* $E/F$ 为有限扩张, 且 $[E:F] \le n$.

*4.* $E/F$ 为 Galois 扩张, 且 $\mathrm{Gal}(E/F) = G$.

习题 **4.** 设 $E/F$ 为有限扩张, 则以下几条互相等价:

*1.* $E/F$ 为 Galois 扩张.

*2.* 记 $G = \mathrm{Gal}(E/F)$, 则 $E^G = F$.

*3.* 存在有限子群 $G \leq Aut(E)$, 使得 $F = E^G$.

• Galois 扩张的重要例子

以下为需要熟悉的 Galois 扩张的几个典型例子.

例 **1.** (有限域的扩张) 设 $p$ 为素数, $q$ 为 $p$ 的正整数次幂. 设 $F$ 为 $q$ 元有限域, $E$ 为 $q^n$ 元有限域. 则 $E/F$ 为 Galois 扩张, 其 Galois 群为循环群 $\mathrm{Gal}(E/F) = \langle Fr \rangle \simeq \mathbb{Z}/n\mathbb{Z}$. 其中 $Fr\colon E \to E,\ x \mapsto x^q$ 为 Frobenius 自同态.

例 **2.** (一般系数的 $n$ 次首一多项式) 记 $F = \mathbb{Q}(t_1, \cdots, t_n)$ 为 $\mathbb{Q}$ 上的 $n$ 元有理函数域. 令 $f(x) = x^n + t_1 x^{n-1} + t_2 x^{n-2} + \cdots + t_n \in F[x]$. 设 $E$ 为 $f$ 在 $F$ 上的分裂域. 则 $E/F$ 为 Galois 扩张, 且 $\mathrm{Gal}(E/F) \simeq \mathfrak{S}_n$.

例 **3.** (分圆扩张) 设 $\zeta_N \in \mathbb{C}$ 为一个 $N$ 次本原单位根, 则 $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ 为 Galois 扩张. 并且

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) = \{\sigma \mid \sigma(\zeta_N) = \zeta_N^i,\ 1 \leq i \leq N,\ (i, N) = 1\} \simeq (\mathbb{Z}/N\mathbb{Z})^*.$$

例 **4.** (循环扩张) 设 $F$ 为域, $n$ 为正整数, $\mathrm{char}.F = 0$ 或 $\mathrm{char}.F = p$ 且 $(n, p) = 1$. 设 $x^n - 1 = 0$ 的所有根 $\zeta_n^i$ $(1 \leq i \leq n)$ 均在 $F$ 中. 设 $a \in F$ 使得 $f(x) = x^n - a$ 为 $F$ 上的不可约多项式. 记 $E = F(\sqrt[n]{a})$ 为 $f$ 在 $F$ 上的分裂域. 则 $E/F$ 为 Galois 扩张, 并且

$$\mathrm{Gal}(E/F) = \{\sigma \mid \sigma(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n^i,\ 1 \leq i \leq n\} \simeq \mathbb{Z}/n\mathbb{Z}.$$

例 **5.** (Artin−Schreier 扩张) 设 $F$ 为特征 $p$ 的域, 设 $a \in F$, 使得 $f(x) = x^p - x - a$ 在 $F$ 上没有根. 作为练习可以证明 $f$ 在 $F$ 上不可约. 令 $E$ 为 $f$ 在 $F$ 上的分裂域. 取 $\alpha \in E$ 为 $f$ 的一个根. 则 $E = F(\alpha)$, 并且 $E/F$ 为 Galois 扩张. 其 Galois 群为:

$$\mathrm{Gal}(E/F) = \{\sigma \mid \sigma(\alpha) = \alpha + \beta,\ \beta \in \mathbb{F}_p\} \simeq \mathbb{Z}/p\mathbb{Z}.$$

• Galois 基本定理

设 $E/F$ 为有限扩张, 且为 Galois 扩张. 记 $G = \mathrm{Gal}(E/F)$. 定义 $G$ 的所有子群集合与 $E/F$ 的所有中间域的集合:

$$S := \{H \mid H\text{为}G\text{的子群}\}.$$

$$M := \{K \mid K\text{为}E\text{的包含}F\text{的子域}\}.$$

定义映射:

$$\varphi\colon S \to M$$

$$H \mapsto E^H$$

以及

$$\psi\colon M \to S$$

$$K \mapsto \mathrm{Gal}(E/K)$$

习题 **5.** (Galois 理论基本定理)

*1.* 上述 $\varphi, \psi$ 为互逆映射.

*2.* 若 $H_1, H_2 \in S$, 则 $H_1 \subseteq H_2 \Leftrightarrow E^{H_2} \subset E^{H_1}$.

*3.* 对于 $H \in S$, 其对应的中间域 $E^H$ 为 $F$ 的 Galois 扩张 $\Leftrightarrow$ $H$ 为 $G$ 的正规子群, 并且此时以下为群的正合列:

$$1 \to H \to G \to \mathrm{Gal}(E^H/F) \to 1.$$

其中 $G \to \mathrm{Gal}(E^H/F)$ 为限制映射: $\sigma \mapsto \sigma|_{E^H}$.

# 2022-06-01 迹与范数, 纯不可分扩张

设 $E/F$ 为域的有限扩张. 对于 $\alpha \in E$, 考虑 $F$-线性映射 $\varphi_\alpha \colon E \to E,\ x \mapsto \alpha x$. 定义 $\alpha$ 的迹 (trace) 为 $Tr_{E/F}(\alpha) := \mathrm{tr}\varphi_\alpha$, 定义 $\alpha$ 的范数 (norm) 为 $N_{E/F}(\alpha) := \det \varphi_\alpha$. 这样我们得到映射 $Tr_{E/F} : E \to F$ 和 $N_{E/F} : E \to F$. 我们主要从线性代数的观点来考察这两个映射的性质.

习题 **1.** 设 $E/F$ 为域的有限扩张.

*1.* $Tr_{E/F} \colon E \to F$ 为加法群同态, $N_{E/F} \colon E^* \to F^*$ 为乘法群同态.

*2.* $\forall \alpha \in F,\ Tr_{E/F}(\alpha) = [E:F]\alpha,\ N_{E/F}(\alpha) = \alpha^{[E:F]}$.

习题 **2.** 设 $E/F$ 为域的有限扩张, 且 $E = F(\alpha)$ 为单扩张. 设 $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in F[x]$ 为 $\alpha$ 在 $F$ 上的极小多项式. 证明: $F$-线性变换 $\varphi_\alpha \colon E \to E$ 的特征多项式和极小多项式均等于 $f(x)$.

习题 **3.** 设 $E/F$ 为域的有限扩张, $\alpha \in E$. 设 $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in F[x]$ 为 $\alpha$ 在 $F$ 上的极小多项式. 证明: $Tr_{E/F}(\alpha) = -[E:F(\alpha)]a_{n-1}, N_{E/F}(\alpha) = ((-1)^n a_0)^{[E:F(\alpha)]}$.

习题 **4.** 设 $E/F$ 为域的有限可分扩张, $x \in E$. 设 $\mathrm{Hom}_F(E, \bar{F}) = \{\sigma_1, \ldots, \sigma_n\}$. 证明: $Tr_{E/F}(x) = \sum\limits_{i=1}^{n} \sigma_i(x),\ N_{E/F}(x) = \prod\limits_{i=1}^{n} \sigma_i(x)$.

习题 **5.** 设 $p$ 为素数, $q$ 为 $p$ 的正整数次幂. 设 $F$ 为 $q$ 元有限域, $E$ 为 $q^n$ 元有限域. 证明: 对于 $\alpha \in E,\ Tr_{E/F}(\alpha) = \sum\limits_{i=0}^{n-1} \alpha^{q^i},\ N_{E/F}(\alpha) = \alpha^{\sum_{i=0}^{n-1} q^i}$.

习题 **6.** (迹与范数的复合) 设 $E/F, K/E$ 均为域的有限扩张. 本题的目标是证明 $N_{E/F}\circ N_{K/E} = N_{K/F}$ 和 $Tr_{E/F}\circ Tr_{K/E} = Tr_{K/F}$. 对于 $K$ 上的一个 $E$-线性变换 $\psi \in End_E(K)$, 将其看作 $K$ 上的 $F$-线性变换时记作 $\psi_F \in End_F(K)$.

*1.* 对于 $\psi_1, \psi_2 \in End_E(K)$, 有

$$N_{E/F}(\det(\psi_1 \circ \psi_2)) = N_{E/F}(\det \psi_1) \cdot N_{E/F}(\det \psi_2).$$

*2.* 设 $\psi \in End_E(K)$ 为可对角化的, 证明: $N_{E/F}(\det \psi) = \det \psi_F$.

*3.* 设 $\psi \in End_E(K)$ 为可上三角化的, 证明:$N_{E/F}(\det \psi) = \det \psi_F$.

*4.* 对任意 $\psi \in End_E(K)$, 证明: $N_{E/F}(\det \psi) = \det \psi_F$.

*5.* 证明:$N_{E/F} \circ N_{K/E} = N_{K/F}$.

*6.* 利用同样的思路, 证明对任意 $\psi \in End_E(K)$, $Tr_{E/F}(tr\psi) = tr\psi_F$. 并由此证明 $Tr_{E/F} \circ Tr_{K/E} = Tr_{K/F}$.

下面讨论迹与域扩张的可分性之间的关系. 设 $F$ 为特征 $p$ 的域, 我们称域扩张 $E/F$ 为纯不可分扩张 (purely inseparable), 如果对任意 $a \in E$, 均存在正整数 $n$, 使得 $a^{p^n} \in F$. 下面的这个扩张是纯不可分扩张的最典型的例子.

习题 **7.** $F = \mathbb{F}_p(t),\ E = F[t^{\frac{1}{p}}] = F[x]/(x^p - t)$. 则 $E/F$ 为纯不可分扩张.

习题 **8.** 设 $E/F$ 为纯不可分有限扩张, $char\ F = p$, 则

*1.* $|\mathrm{Hom}_F(E, \bar{F})| = 1$.

*2.* $[E : F]$ 为 $p$ 的幂次.

*3.* $\forall a \in E,\ Tr_{E/F}(a) = 0$.

习题 **9.** (有限扩张分解为可分扩张和纯不可分扩张的复合) 设 $E/F$ 为有限扩张, 令 $E_s := \{a \in E \mid a$ 在 $F$ 上的极小多项式无重根 (即 $a$ 在 $F$ 上可分)$\}$. 证明:

*1.* $E_s$ 为 $E$ 的子域, 称为 $F$ 在 $E$ 中的可分闭包.

*2.* $E_s/F$ 为可分扩张, $E/E_s$ 为纯不可分扩张.

*3.* 如果 $E/F$ 不是可分扩张, 则 $Tr_{E/F}\colon E \to F$ 为零映射.

注: 关于纯不可分扩张的内容可以参考 [?] 的 V.6 节.

设 $E/F$ 为有限扩张, 定义 $E$ 上的对称 $F$-双线性型如下:

$$\varphi\colon E \times E \to F$$

$$(x, y) \mapsto Tr_{E/F}(xy)$$

如果 $E/F$ 为可分扩张, 设 $E = F(\alpha)$, $\mathrm{Hom}_F(E, \bar{F}) = \{\sigma_1, \ldots, \sigma_n\}$. 则 $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ 为 $E$ 的一组 $F$-线性基. $\varphi$ 在这组基下对应得方阵记为 $M$, 则 $M(i,j) = Tr_{E/F}(\alpha^{i+j-2}) = \sum\limits_{k=1}^{n} \sigma_k(\alpha^{i+j-2})$.

习题 **10.** 证明: $\det M = \prod\limits_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$. 从而对于可分扩张 $E/F$, 二次型 $\varphi$ 为非退化的.

习题 **11.** 设 $K$ 为代数数域 (即 $K/\mathbb{Q}$ 为有限扩张), 记 $\mathcal{O}_K$ 为相应的代数整数环 (即 $\mathcal{O}_K$ 为 $K$ 中在 $\mathbb{Z}$ 上整的所有元素形成的子环). 本题的目标是证明 $\mathcal{O}_K$ 为 Noether 环. 依次证明:

*1.* 存在 $e_1, \ldots, e_n \in \mathcal{O}_K$ 为 $K$ 的一组 $\mathbb{Q}$-线性基.

2. $Tr_{K/\mathbb{Q}}(\mathcal{O}_K) \subset \mathbb{Z}$.

3. 二次型 $\varphi$ 对应的方阵 $M = (Tr_{K/\mathbb{Q}}(e_i e_j))$ 为整系数方阵, 并且其行列式非零.

4. $\det M \cdot \mathcal{O}_K \subset \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$.

5. $\mathcal{O}_K$ 为有限生成 $\mathbb{Z}$-模, 从而为 Noether 环.

习题 **12.** (习题 10. 的另一种证法) 设 $E/F$ 为有限可分扩张, 双线性型 $\varphi$ 同上.

1. 证明有 $F$-代数同构 $E \otimes_F \bar{F} \simeq \prod_{i=1}^{n} \bar{F}$.

2. 证明系数扩张到 $\bar{F}$ 后, $\varphi$ 为 $E \otimes_F \bar{F}$ 上的非退化对称 $\bar{F}$-双线性型.

3. $\varphi$ 为 $E$ 上的非退化对称 $F$-双线性型.

习题 **13.** (选做) 设 $F$ 为域, $A$ 为有限维交换 $F$-代数. 对 $a \in A$, 记 $Tr(a) \in F$ 为 $A$ 上 $F$-线性变换 $x \mapsto ax$ 的迹. 令 $\varphi\colon A \times A \to F$, $(x, y) \mapsto Tr(xy)$ 为 $A$ 上的对称 $F$-双线性型. 证明以下命题等价:

1. 对任意 $F$ 的扩域 $K$, $A \otimes_F K$ 没有非平凡幂零元 (即只有 0 为幂零元).

2. $A \otimes_F \bar{F}$ 没有非平凡幂零元.

3. 存在 $\bar{F}$-代数同构 $A \otimes_F \bar{F} \simeq \prod_{i=1}^{n} \bar{F}$.

4. $\varphi$ 为非退化双线性型.

# 2022-06-06 Galois 群的计算

设 $E/F$ 为有限 Galois 扩张, $G = \mathrm{Gal}(E/F)$. 为了计算 $G$, 一方面可以通过计算 $[E:F]$ 得到 $|G|$, 另一方面可以找到尽可能少的容易计算的共轭根的生成元, 使得 $E = F(\alpha_1, \ldots, \alpha_m)$, 这样每个 $\sigma \in G$ 均置换 $\alpha_i$ 的共轭根, 从而得到 $|G|$ 的上界. 如果该上界恰好等于 $|G|$, 则 $G$ 就是所有上面形式的置换.

例 **1.** 设 $K$ 为 $x^8 - 5$ 在 $\mathbb{Q}$ 上的分裂域, 求 $\mathrm{Gal}(K/\mathbb{Q})$.

习题 **1.** 设 $K$ 为 $x^4 - 2$ 在 $\mathbb{Q}$ 上的分裂域, 证明 $\mathrm{Gal}(K/\mathbb{Q})$ 同构于正四边形对应的二面体群 $D_4$.

习题 **2.** 设 $K$ 为 $x^4 - x^2 - 1$ 在 $\mathbb{Q}$ 上的分裂域, 求 $\mathrm{Gal}(K/\mathbb{Q})$.

习题 **3.** 设 $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$. 证明 $K/\mathbb{Q}$ 为 Galois 扩张, 并求 $\mathrm{Gal}(K/\mathbb{Q})$.

习题 **4.** 设 $p$ 为素数,$K = \mathbb{F}_p(T)$. 考虑如下 $K[x]$ 中的多项式:

$$f(x) = x^p - Tx - T,\ g(x) = x^{p-1} - T.$$

*1.* 证明 $f, g$ 均为 $K[x]$ 中不可约多项式, 并且均没有重根.

*2.* 令 $M$ 为 $g$ 在 $K$ 上的分裂域, 证明 $\mathrm{Gal}(M/K) \simeq \mathbb{F}_p^*$.

*3.* 令 $L$ 为 $f$ 在 $K$ 上的分裂域, 证明 $g$ 在 $L[x]$ 中分裂为一次多项式的乘积, 并且 $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{F}_p \rtimes \mathbb{F}_p^*$, 其中 $\mathbb{F}_p^*$ 通过数乘作用到加法群 $\mathbb{F}_p$ 上.

为了得到 Galois 群中的一些非平凡元素, 下面的性质经常用到.

习题 **5.** 设 $F$ 为域, $f(x) \in F[x]$ 为首一的无重根多项式. 设 $f(x)$ 在 $\bar{F}$ 中的所有根为 $\{\alpha_1, \ldots, \alpha_n\}$. 令 $K = F(\alpha_1, \cdots, \alpha_n)$ 为 $f$ 在 $F$ 上的分裂域. 令 $G = \mathrm{Gal}(K/F)$. 证明:$f$ 在 $F$ 上不可约 $\Leftrightarrow G$ 在 $\{\alpha_1, \ldots, \alpha_n\}$ 上的置换作用是传递的. 特别地, 当 $f$ 在 $F$ 上不可约时, $|G|$ 为 $n$ 的倍数.

习题 **6.** 设 $f(x) \in \mathbb{Q}[x]$ 为首一不可约多项式, 并且 $\deg f = p$ 为素数. 设 $f$ 恰有 $p-2$ 个实根. 令 $K$ 为 $f$ 在 $\mathbb{Q}$ 上的分裂域, $G = \mathrm{Gal}(K/\mathbb{Q})$. 证明:

*1.* 通过 $G$ 在 $f$ 的 $p$ 个根上的置换作用, $G$ 可以看作 $\mathfrak{S}_p$ 的子群.

*2.* $G$ 包含一个对换.(提示: 考虑 $\mathbb{C}$ 上的共轭)

*3.* $G$ 包含一个长度为 $p$ 的圈 (循环).(提示: $G$ 中包含 $p$ 阶元).

*4.* $G = \mathfrak{S}_p$

习题 **7.** 设 $f(x) = x^5 - 6x + 3$. 令 $K$ 为 $f$ 在 $\mathbb{Q}$ 上的分裂域. 证明 $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathfrak{S}_5$.

习题 **8.** 设 $f(x) = x^3 - 3x + 1$, $K$ 为 $f$ 在 $\mathbb{Q}$ 上的分裂域.

*1.* 设 $f$ 的判别式为 $\Delta(f) \in \mathbb{Q}$. 证明 $\sqrt{\Delta(f)} \notin \mathbb{Q}$. 进而证明 $2|[K:\mathbb{Q}]$.

*2.* 证明 $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathfrak{S}_3$.

# 2022-06-08 Galois 下降法应用

设 $K \subset \bar{K}$, $\bar{K}$ 为域 $K$ 的一个代数闭包. 设 $K \subset L \subset \bar{K}$, $L/K$ 为有限 Galois 扩张, 记 $L$ 到 $\bar{K}$ 的包含同态为 $i$.

习题 **1.** *1.* 映射 $\mathrm{Gal}(L/K) \to \mathrm{Hom}_K(L, \bar{K})$, $\sigma \mapsto i \circ \sigma$ 为双射. 通过该双射, 对 $\sigma \in \mathrm{Gal}(L/K)$, 我们将 $K$-嵌入 $i \circ \sigma \colon L \to \bar{K}$, 直接记为 $\sigma \colon L \to \bar{K}$.

*2.* $\forall \sigma \in \mathrm{Gal}(L/K)$, 映射 $\varphi_\sigma \colon \bar{K} \otimes_K L \to \bar{K}$, $x \otimes y \mapsto x \cdot \sigma(y)$ 为 $K$-线性映射 (实际为 $\bar{K}$-代数同态).

*3.* 乘积映射 $\prod\limits_{\sigma \in \mathrm{Gal}(L/K)} \varphi_\sigma \colon \bar{K} \otimes_K L \to \prod\limits_{\sigma \in \mathrm{Gal}(L/K)} \bar{K}$ 为 $\bar{K}$-线性同构 (实际上为 $\bar{K}$-代数同构).

*4.* $\forall \sigma \in \mathrm{Gal}(L/K)$, 记 $e_\sigma$ 为 $\prod\limits_{\sigma \in \mathrm{Gal}(L/K)} \bar{K}$ 中 $\sigma$ 分量为 1, 其它分量为 0 的元素, 则 $\{e_\sigma \mid \sigma \in \mathrm{Gal}(L/K)\}$ 为 $\prod\limits_{\sigma \in \mathrm{Gal}(L/K)} \bar{K}$ 的一组 $\bar{K}$-线性空间基.

*5.* 对 $\tau \in \mathrm{Gal}(L/K)$, 记 $1 \otimes \tau$ 为如下 $\bar{K}$-线性映射:

$$\bar{K} \otimes_K L \to \bar{K} \otimes_K L$$

$$x \otimes y \mapsto x \otimes \tau(y)$$

记 $\tilde{\tau}$ 为 $\prod\limits_{\sigma \in \mathrm{Gal}(L/K)} \bar{K}$ 上满足 $\tilde{\tau}(e_\sigma) = e_{\sigma \cdot \tau^{-1}} (\forall \sigma \in \mathrm{Gal}(L/K))$ 的 $\bar{K}$-线性变换. 证明: 有如下交换图表:

$$\begin{tikzcd}
\bar{K}\otimes_K L \arrow[r, "\prod\limits_{\sigma\in\mathrm{Gal}(L/K)}\varphi_\sigma"] \arrow[d, "1\otimes\tau"] & \prod\limits_{\sigma\in\mathrm{Gal}(L/K)}\bar{K} \arrow[d, "\tilde{\tau}"] \\
\bar{K}\otimes_K L \arrow[r, "\prod\limits_{\sigma\in\mathrm{Gal}(L/K)}\varphi_\sigma"] & \prod\limits_{\sigma\in\mathrm{Gal}(L/K)}\bar{K}
\end{tikzcd}$$

*6.* 记 $G=\mathrm{Gal}(L/K)$, 记 $\bar{K}[G]$ 为群代数, 则映射

$$\prod_{\sigma\in\mathrm{Gal}(L/K)}\bar{K}\xrightarrow{\sim}\bar{K}[G]$$

$$e_\sigma\mapsto\sigma^{-1}$$

为 $\bar{K}$-线性空间同构, 且通过该同构, $\tilde{\tau}$ 等同于 $\bar{K}[G]$ 上左乘 $\tau$ 的 $\bar{K}$-线性变换.

*7.* 总结上面的讨论, $\forall\tau\in G=\mathrm{Gal}(L/K)$, 我们得到如下 $\bar{K}$-线性映射的交换图表:

$$\begin{tikzcd}
\bar{K}\otimes_K L \arrow[r, "\sim"] \arrow[d, "1\otimes\tau"] & \bar{K}[G] \arrow[d, "\tau\cdot"] \\
\bar{K}\otimes_K L \arrow[r, "\sim"] & \bar{K}[G]
\end{tikzcd}$$

注意在上面的 $\bar{K}$-线性同构 $\bar{K}\otimes_K L\simeq\bar{K}[G]$ 下, 1 对应到 $\sum\limits_{\tau\in G}\tau$.

下面几个定理均有相似的证明思路: 基于上面的交换图表, 将跟 $\mathrm{Gal}(L/K)$ 中元素有关的线性代数问题系数扩张到 $\bar{K}$ 上, 进而利用群代数 $\bar{K}[G]$ 将问题转化为几乎显然的线性代数问题.

### 应用一: **Artin** 引理

定理一 (Artin 引理) 设 $L/K$ 为有限 Galois 扩张, $\mathrm{Gal}(L/K)=\{\sigma_1,\ldots,\sigma_n\}$. 那么 $\sigma_1,\ldots,\sigma_n$ 作为 $L$ 上的 $L$-值函数, 是 $L$-线性无关的, 即若 $\lambda_1,\ldots,\lambda_n\in L$, 使得 $\lambda_1\sigma_1(x)+$

$\ldots + \lambda_n \sigma_n(x) = 0,\ \forall x \in L$, 则 $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$.

**应用二: Kummer 扩张**

定理 **2** (Kummer 扩张) 设 $L/K$ 为有限 Galois 扩张, $G = \mathrm{Gal}(L/K) \simeq \mathbb{Z}/n\mathbb{Z}$ 为 $n$ 阶循环群. 设 $char\ K = 0$, 或者 $char\ K = p$ 及 $p \nmid n$, 并设 $\zeta_n \in K$, 其中 $\zeta_n$ 为本原 $n$ 次单位根, 则存在 $a \in K$, 使得 $L = K(\sqrt[n]{a})$.

**应用三: Artin-Schreier 扩张**

定理 **3** (Artin-Schreier 扩张) 设 $p$ 为素数, $L/K$ 为有限 Galois 扩张, $char\ K = p$, 且 $[L:K] = p$(等价地, $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}$), 则存在 $\alpha \in L,\ a \in K$, 使得 $L = K(\alpha)$, 且 $\alpha$ 为 $K$ 上多项式 $f(x) = x^p - x - a$ 的根.

**应用四: 正规基定理**

设 $L/K$ 为有限 Galois 扩张, 则存在 $\alpha \in L$, 使得 $\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(L/K)\}$ 为 $L$ 的一组 $K$-线性空间基.

**应用五: Hilbert 90**

习题 **2.** 设 $L/K$ 为有限 Galois 扩张, $G = \mathrm{Gal}(L/K)$. 对 $\alpha \in L$, 令 $\varphi_\alpha \colon L \to L,\ x \mapsto \alpha \cdot x$ 为左乘 $\alpha$ 的 $K$-线性变换. 验证在习题 1.7 的同构下, 有如下交换图表:

$$\begin{array}{ccccc} \bar{K} \otimes_K L & \xrightarrow{\sim} & \bar{K}[G] & & \sigma \\ \downarrow{\scriptstyle 1\otimes\varphi_\alpha} & & \downarrow & & \downarrow \\ \bar{K} \otimes_K L & \xrightarrow{\sim} & \bar{K}[G] & & \sigma^{-1}(\alpha)\cdot\sigma \end{array}$$

**定理 5** (Hilbert 90, 循环群乘法情形) 设 $L/K$ 为有限 Galois 扩张, $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$ 为循环群, $\beta \in L^*$. 则 $N_{L/K}(\beta) = 1 \Leftrightarrow \exists\alpha \in L^*,\ s.t.\ \beta = \dfrac{\sigma\alpha}{\alpha}$.

**定理 6** (Hilbert 90, 循环群加法情形) 设 $L/K$ 为有限 Galois 扩张, $G = \mathrm{Gal}(L/K)$, $\langle\sigma\rangle$ 为循环群, $\beta \in L$. 则 $Tr_{L/K}(\beta) = 0 \Leftrightarrow \exists\alpha \in L,\ s.t.\ \beta = \sigma(\alpha) - \alpha$.

更一般地, 设 $L/K$ 为有限 Galois 扩张, $G = \mathrm{Gal}(L/K)$, $f\colon G \to L^*$ 为映射.

**习题 3.** 对 $\sigma \in G$, 考虑如下 $\bar{K}$-线性映射:

$$\begin{aligned} \varphi_\sigma\colon \bar{K}[G] &\to \bar{K}[G] \\ \tau &\mapsto \tau^{-1}(f(\sigma)) \cdot \tau \end{aligned}$$

设 $a = \sum\limits_{h \in G} c_h \cdot h \in \bar{K}[G] \backslash \{0\}$, 其中 $c_h \in \bar{K}$.

证明: 以下两条等价:

*1.* $\forall\sigma \in G,\ \varphi_\sigma(a) = \sigma \cdot a$, 等式右边为群代数中乘法.

*2.* $c_h = c_1 \cdot f(h^{-1}),\ \forall h \in G$, 并且 $f(\sigma_1\sigma_2) = f(\sigma_1) \cdot \sigma_1(f(\sigma_2)),\ \forall\sigma_1, \sigma_2 \in G$.

**定理 7** (Hilbert90, 乘法情形) 设 $L/K$ 为有限 Galois 扩张, $G = \mathrm{Gal}(L/K)$, $f\colon G \to L^*$ 为映射, 则 $f(\sigma_1\sigma_2) = f(\sigma_1) \cdot \sigma_1(f(\sigma_2)),\ \forall\sigma_1, \sigma_2 \in G \Leftrightarrow \exists a \in L^*,\ s.t.\ f(\sigma) = \dfrac{\sigma(a)}{a},\ \forall\sigma \in G$. 这等价于说 $H^1(G, L^*) = \{1\}$.

利用同样的思路, 可以得到下面定理的证明.

**定理 8** (Hilbert90, 加法情形) 设 $L/K$ 为有限 Galois 扩张, $G = \mathrm{Gal}(L/K)$, $f\colon G \to L$ 为映射, 则 $f(\sigma_1\sigma_2) = f(\sigma_1) + \sigma_1(f(\sigma_2)),\ \forall\sigma_1, \sigma_2 \in G \Leftrightarrow \exists a \in L,\ s.t.\ f(\sigma) = \sigma(a) -$

$a$, $\forall\sigma \in G$. 这等价于说 $H^1(G, L) = \{0\}$.

## 2022-06-23 期末考试

**1** 设 $\iota\colon K\hookrightarrow L$ 为域扩张, $x$ 和 $y$ 为 $L$ 的两个元素; 假定 $x$ 在 $K$ 上代数, 且 $K(x)=K(y)$. 证明 $y$ 在 $K$ 上也是代数的, 并比较 $x$ 和 $y$ 各自的极小多项式的次数.

**2** 域的二次扩张 (即 $\iota\colon K\hookrightarrow L$, $[L:K]=2$) 一定是正规扩张吗?

**3** 设 $\iota\colon K\hookrightarrow L$ 为域扩张, $\Lambda\subset L$ 为 $L$ 的子集, 其中的元素均在 $K$ 上代数; 考虑 $K[\Lambda]$ 为 $\Lambda$ 在 $K$ 上生成的 $L$ 的子环, 它是否一定等于 $\Lambda$ 在 $K$ 上生成的子域 $K(\Lambda)$?

**4** 令 $n\in\mathbb{N}^*$, 且 $K$ 为 $\mathbb{R}$ 的子域, 令 $K=K_0\subset K_1\subset K_2\subset\cdots\subset K_n$ 为一列二次扩张塔 (即每个 $K_i/K_{i-1}$ 都是二次扩张). 刻画 $\mathbb{R}$ 的所有子域 $K$, 满足 $K_n$ 在 $K$ 上是可建造的.

(回忆: 我们称一个 $\mathbb{R}^2$ 的子集 $\tilde{\Sigma}$ 在另一个子集 $\tilde{\Sigma}_0$ 上是可建造的 (constructible), 是指存在正整数 $N$ 和一列递增子集 $\tilde{\Sigma}_0\subset\tilde{\Sigma}_1\subset\cdots\subset\tilde{\Sigma}_N=\tilde{\Sigma}$, 使得 $\tilde{\Sigma}_i\backslash\tilde{\Sigma}_{i-1}$ 为一个点, 这个点要么是 $\tilde{\Sigma}_{i-1}$ 上可定义的两条直线的交点, 要么是 $\tilde{\Sigma}_{i-1}$ 上一个可定义的圆和一条可定义直线的其中一个交点, 要么是两个可定义圆的其中一个交点. 这里称一个 $\mathbb{R}$ 的子集 $\Sigma$ 是在 $K$ 上可建造的是指存在一个 $\mathbb{R}^2$ 的在 $K\times\{0\}$ 上可建造的子集 $\tilde{\Sigma}$, 使得 $\tilde{\Sigma}$ 向第一个分量的正交投影正好是 $\Sigma$.)

**5** 设 $K$ 为域, $P$ 和 $Q$ 是 $K$ 上两个互素的多项式. 仅使用课上所学的东西, 且不允许引入 $P$ 和 $Q$ 的根, 证明结式 $Res(P,Q)\neq 0$. 该结论的逆命题是否成立?

**6** 设 $K$ 为域, $K(X)$ 为 $K$ 上的有理分式域. 证明 $[K(X):K]$ 是可数的, 当且仅当 $K$ 为有限域或可数域.

**7** 所有 Liouville 数构成 $\mathbb{R}$ 的一个子集, 它是否稠密?

回忆:Liouville 数是指以下集合

$$\mathcal{L} := \left\{x \in \mathbb{R} \mid \forall n \in \mathbb{N},\ \left|\{(a,b) \in \mathbb{Z} \times \mathbb{Z}\backslash\{0\} \colon 0 < |x - \frac{a}{b}| < \frac{1}{b^n}\}\right| = \infty\right\}$$

**8** 设 $p \in \mathcal{P}$ 为素数, 我们介绍计数函数: $f \colon \mathbb{N} \to \mathbb{N},\ n \mapsto f(n)$, 其中

$$f(n) = \left|\{P \in \mathbb{F}_p[X] \mid P\text{是}n\text{次首一不可约的多项式}\}\right|$$

*8.1* 在 $T$ 为变量的形式幂级数环 $\mathbb{Z}[[T]]$ 中证明如下恒等式

$$\sum_{n\in\mathbb{N}} p^n T^n \prod_{n\in\mathbb{N}^*} (1 - T^n)^{f(n)} = 1;$$

*8.2* 由此导出 $nf(n)$ 的一个表达式: $\sum\limits_{k\in F} \varepsilon(k) p^k$, 其中 $F$ 为 $\mathbb{N}$ 的有限子集, $\varepsilon(k) \in \{\pm 1\}$ 为可显式写出的符号函数.

*8.3* 由上一题给的 $f$ 的表达式推出, 对任意 $n \in \mathbb{N}^*$, 存在 $p^n$ 元域.

*8.4* 引入 $X^{p^n} - X$ 在 $\mathbb{F}_p$ 上的分裂域重新证明上一题的结论.

**9** 设 $n \in \mathbb{N}^*$ 为正整数, $P_n = X^n - 1 \in \mathbb{Q}[X]$ 为多项式.

*9.1* 证明对所有的 $n$, 存在一个 $P_n$ 的根生成 $P_n$ 在 $\mathbb{Q}$ 上的分裂域, 记为 $K_n$; 记 $\zeta_n$ 为这个根, 即需要给出 $K_n = \mathbb{Q}(\zeta_n)$.

*9.2* 当 $n$ 为素数的时候, 求 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$.

*9.3* 回忆对扩张 $K/\mathbb{Q}$, 我们记 $\mu_n(K)$ 为 $P_n$ 在 $K$ 中的根的集合, 而 $\tilde{\mu}_n(K)$ 为 $K$

中 $n$ 次本原单位根的集合. 定义 $\phi_n(X)=\prod\limits_{\zeta\in\tilde{\mu}_n(K_n)}(X-\zeta)$;

*9.4* 证明对所有正整数 $n\in\mathbb{N}^*$ 有恒等式 $P_n(X)=\prod\limits_{d|n}\phi_d$, 并由此证明等式 $n=\prod\limits_{d|n}\varphi(d)$, 其中 $\varphi$ 为欧拉函数.

*9.5* 对 $n\in\mathbb{N}^*$, 证明 $\phi_n$ 为整系数多项式, 即 $\phi_n\in\mathbb{Z}[X]$,

*9.6* 在什么条件下我们有 $X^n-1\in K[X]$ 是可分的?

*9.7* 设 $p\in\mathcal{P}$ 为素数, 且 $p\nmid n, \zeta\in\tilde{\mu}_n(K_n)$ 为一个 $n$ 次本原单位根, $Q\in\mathbb{Z}[X]$ 为 $\phi_n$ 的一个不可约因子. 证明若 $\zeta$ 是 $Q$ 的根, 那么 $\zeta^p$ 也是.

*9.8* 由此导出 $\phi_n$ 在 $\mathbb{Q}[X]$ 中是不可约的.

*9.9* 对正整数 $n\in\mathbb{N}^*$, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 的扩张次数是多少?

*9.10* 设 $L/\mathbb{Q}$ 为一个有限扩张, 集合

$$\bigcup_{n\in\mathbb{N}^*}\mu_n(L):=\{l\in L\mid \exists n\in\mathbb{N}^*,\ l^n=1\}$$

是否总是有限的?

*9.11* 设 $n$ 和 $m$ 为两个互素的正整数, $p$ 为奇素数, $L/\mathbb{Q}$ 为有限域扩张, 且扩张次数 $[L:\mathbb{Q}]=p^n$. 此时对上一问的集合可以给出什么结论?

*9.12* 在 $p=2$ 的情形结论是否是不同的?

*9.13* 设 $n$ 为奇数, 且 $n\geq 3$. $\phi_n$ 和 $\phi_{2n}$ 有什么关系?

**10** (前面习题给出的结论可以使用)

*10.1* 设 $P$ 为非常值的整系数多项式, 证明集合

$$\{p\in\mathcal{P}\mid \exists n\in N^*,\ p|P(n)\}$$

为无限集.

*10.2* 设 $n$ 为正整数, $p$ 为奇素数且不整除 $n$, $\alpha$ 为一个整数, 且满足 $p|\phi_n(\alpha)$, 其中 $\phi_n$ 为前一题中定义的多项式 (即分圆多项式). 证明 $p\nmid\alpha$, 且 $\alpha$ 模 $p$ 的剩余在 $(\mathbb{Z}/p\mathbb{Z})^*$ 中的阶恰好是 $n$.

*10.3* 利用前面的结论, 证明存在无穷多个模 $n$ 余 1 的素数 $p$.

*10.4* 这个结论让你想到了什么?

**11** 设 $m$ 和 $n$ 为两个互素的正整数, $p$ 为素数. 多项式 $X^{p^m}-X$ 在 $\mathbb{F}_{p^n}$ 里有多少个根? 证明你的结论.

**12** 设 $p$ 为素数, $\bar{\mathbb{F}}_p$ 为 $\mathbb{F}_p$ 一个取定的代数闭包. 令 $G=\mathrm{Gal}(\bar{F}_p/\mathbb{F}_p)$ 为 Galois 群.

*12.1* a- 证明 Frobenius 自同态 $Fr$ 为 $\bar{\mathbb{F}}_p$ 的一个自同构

b- 设 $n$ 为正整数. 证明扩张 $\mathbb{F}_{p^n}/\mathbb{F}_p$ 的 Galois 群是循环群, 且生成元恰为 $Fr$.

c- 多项式 $X^{p^n}-X$ 在 $\mathbb{F}_p$ 中的因子是什么? 它们的重数分别是多少?

*12.2* 设 $H$ 是 $G$ 由 $Fr$ 生成的子群, 将 $\bar{\mathbb{F}}_p$ 的子域 $\bar{\mathbb{F}}_p^G$ 和 $\bar{\mathbb{F}}_p^G$ 与 $\mathbb{F}_p$ 作比较.

*12.3* a- 证明对所有的正整数 $n$, $\bar{\mathbb{F}}_p$ 有唯一的阶为 $p^n$ 的子域.

b- 将它记作 $\mathbb{F}_{p^n}$, 证明它与以前的记号是一致的.

c- 刻画 $\bar{\mathbb{F}}_p\setminus\cup_{n\in\mathbb{N}^*}\mathbb{F}_{p^n}$.

*12.4* a- 设 $p_1$ 和 $p_2$ 为两个素数, $m_1$ 和 $m_2$ 是两个正整数描述所有的四元对 $(p_1,p_2,m_1,m_2)\in\mathcal{P}^2\times\mathbb{N}^{*2}$ 使得 $\mathbb{F}_{p_1^{m_1}}$ 是 $\mathbb{F}_{p_2^{m_2}}$ 的子域.

b- 证明

$$K=\bigcup_{n\in\mathbb{N}^*}\mathbb{F}_{p^{2^n}}$$

是 $\bar{\mathbb{F}}_p$ 的真子域.

*12.5* 由上述结论导出, 不存在 $\bar{\mathbb{F}}_p$ 的子域 $L$ 使得相应的 Galois 群 $\mathrm{Gal}(\bar{\mathbb{F}}_p/L)=H$. 也就是说, 有限 Galois 对应的结论不能直接推广到任意的 Galois 扩张, 无限 Galois 扩张中存在 Galois 群的子群无法对应到中间扩张.

**13** 设 $L$ 为域, $L_1$ 和 $L_2$ 为 $L$ 的两个子域, $K$ 是 $L_1$ 和 $L_2$ 的公共子域. 假定 $L/L_1$ 和 $L/L_2$ 均为代数扩张.

*13.1* 证明如果 $L_1/K$ 或 $L_2/K$ 为代数扩张, 则 $L/L_1\cap L_2$ 也是代数扩张.

*13.2* 若上一问没有前面的假设, 结论是否还正确?

*13.3* 假定 $L/L_1\cap L_2$ 是代数扩张, $L/L_1$ 和 $L/L_2$ 为正规扩张, 证明 $L/L_1\cap L_2$ 也是正规扩张.

**14** 设有域 $K_1, K_2, L_1, L_2$, 其中 $L_1\subseteq L_2$ 为子域, $\iota_1\colon K_1\hookrightarrow L_1$ 和 $\iota_2\colon K_2\hookrightarrow L_2$ 为两个域扩张, 有域同态 $\sigma\colon K_1\hookrightarrow K_2$ 以及它的一个关于 $\iota_1,\iota_2$ 的延拓 $\tilde{\sigma}\colon L_1\to L_2$ (即 $\tilde{\sigma}\circ\iota_1=\iota_2\circ\sigma$). 我们假定 $\sigma$ 和 $\tilde{\sigma}$ 均为同构.

*14.1* 我们再假定有 $\iota_2\circ\sigma(x)=\iota_1(x)\ \forall x\in K_1$, 且 $\iota_1$ 给出有限扩张. 证明此时有 $L_1=L_2$.

*14.2* 在上一问中去掉 $\iota_1$ 为有限扩张的条件, 此时结论是否仍正确?

*14.3* 与前一问相反, 我们保留 $\iota_1$ 有限的条件, 但去掉 $\iota_2\circ\sigma=\iota_1$, 此时结论是否仍正确?