代数 IV 习题课讲义

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

1958
University of Science and Technology of China

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。2022-06-08 Galois 下降法应用中，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
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 $\varphi(X)=\sqrt{2}$.

♣ 考虑映射 $\psi\colon \mathbb{Z}[X]\to R,\ X\mapsto\sqrt{2}$. 考虑如下图表:

$$\begin{array}{ccc}\mathbb{Q}[X] & \xrightarrow{\bar{\psi}} & \mathbb{Q}[\sqrt{2}] \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle j} \\ \mathbb{Z}[X] & \xrightarrow{\psi} & R\end{array}$$

其中 i 和 j 为自然嵌入. 由于两条路径均将 $\mathbb{Z}[X]$ 中的 X 映至 $\sqrt{2}$, 故该图表交换. 易见 ψ 为满同态, 由于 j 为单射, 有 $\ker(\psi)=\ker(j\circ\psi)=\ker(\bar{\psi}\circ i)=i^{-1}(\ker(\bar{\psi}))$. 而 $\mathbb{Q}[\sqrt{2}]$ 是域, 且 $\bar{\psi}$ 满, 故 $\ker(\bar{\psi})$ 为 $\mathbb{Q}[X]$ 的极大理想, 由一个不可约多项式生成. 易见 $X^2-2\in\ker(\bar{\psi})$, 故 $\ker(\bar{(}\psi))=(X^2-2)$. 而 $i^{-1}(\ker(\bar{\psi}))$ 即 $(X^2-2)\cap\mathbb{Z}[X]$, 由 Gauss 引理, 这是 $\mathbb{Z}[X]$ 的主理想, 且由 X^2-2 生成. 故 $\ker(\psi)=(X^2-2)$(在 $\mathbb{Z}[X]$ 中生成). 这诱导同构 $\mathbb{Z}[X]/(X^2-2)\simeq R$. ♢

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.

♣ 对 $f\in\mathrm{Hom}(R,A)$, 考虑映射 $\pi\colon \mathbb{Z}[X]\to A$, 使得 $\pi=f\circ\psi$, 设 $f(\sqrt{2})=a\in A$, 那么 $a^2-2=f(\psi(X^2-2))=0$. 另一方面, 每给出一个 $a\in A$, 使得 $a^2-2=0$, 令 $\pi:\mathbb{Z}[X]\to A,\ X\mapsto a$, 则由于 $X^2-2\in\ker\pi$, 这会诱导 $f:\mathbb{Z}[X]/(X^2-2)\to A$, 于是给出了对应的 $f\in\mathrm{Hom}(R,A)$, 且可验证这是一对互逆映射. ♢

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

♣ 考虑 $\sigma(\sqrt{2})^2-2=\sigma((\sqrt{2})^2-2)=0$. ♢

4. 以下映射保持乘法

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

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

♣ 直接计算即可. ♢

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

♣ $\Rightarrow$: $N(x)N(x^{-1})=N(1)=1$, 又 $N(x)\in\mathbb{Z}$, 知 $N(x)=\pm1$.

$\Leftarrow$: 若 $N(x)=1$, 即 $a^2-2b=1$, 其中 $x=a+b\sqrt{2}$. 取 $x^{-1}=a-b\sqrt{2}$ 即可; 若 $N(x)=-1$, 则取 $x^{-1}=b\sqrt{2}-a$ 即可. ♢

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

♣ 利用*4*,*5*. ♢

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

♣$(1+\sqrt{2})(-1+\sqrt{2})=1$. ♢

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

♣ 设 $x=a+b\sqrt{2}$. 显然 $a=1,b=0$ 满足要求. 若否, 则一定有 $a>0,b\le0$ 或 $a<0,b\ge0$. 若 $a>0,b\le0$, 则 $N(x)=a^2-2b^2=1$ (因为 $a-b\sqrt{2}>0$) , $a^2-2b^2\ge(1-b\sqrt{2})^2-2b^2=1-2b\sqrt{2}\ge1$, 故 $b=0$. 若 $a<0,b\ge0$, 则 $N(x)=a^2-2b^2=-1$ (因为 $a-b\sqrt{2}<0$), 故 $-1=(a+b\sqrt{2})(a-b\sqrt{2})\le(a-b\sqrt{2})<1+\sqrt{2}-2b\sqrt{2}$, 得到 $b<\frac{1+\sqrt{2}}{2}$, 则 $b=1$, 故 $a^2=-1+2b^2=1\Rightarrow a=\pm1$, 但都不满足 $1\le x=a+b\sqrt{2}<1+\sqrt{2}$. ♢

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

♣ 考虑 $x, -x, x^{-1}, -x^{-1}$ 中不小于 1 的那个, 并仍记为 x. 则存在唯一的正整数 n, 使得 $(1+\sqrt{2})^n \leq x < (1+\sqrt{2})^{n+1}$, 即 $1 \leq x(1+\sqrt{2})^{-n} < 1+\sqrt{2}$. 注意 $(1+\sqrt{2})^n \in R^*$, 利用 *8*, 知 $x(1+\sqrt{2})^{-n} = 1$, 即 $x = (1+\sqrt{2})^n$. 故 $R^* = \{(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$. ♢

注: 本例事实上给出了 $\mathbb{Z}[\sqrt{2}]$ 中的单位, 这是解 *Pell* 方程 $a^2 - 2b^2 = \pm 1$ 的一种方法.

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 $\varphi(X) = i\sqrt{5}$.

♣ 仿照例 1即可. ♢

2. 有以下环同构:

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

♣$R/(p) \simeq (\mathbb{Z}[X]/(X^2+5))/(q) \simeq \mathbb{Z}[X]/(X^2+5, q) \simeq (\mathbb{Z}[X]/(q))/(X^2+5) \simeq \mathbb{F}_p[X]/(X^2+5)$. (注意各 (X^2+5) 所在的环不尽相同.) ♢

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

♣ 注意到 $\mathbb{F}_p[X]$ 是主理想整环, 如果 $X^2+5=0$ 在 $\mathbb{F}_p$ 上无解, 说明 (X^2+5) 是 $\mathbb{F}_p[X]$ 中的极大理想, 故 $\mathbb{F}_p[X]/(X^2+5)$ 是域. 由*2*中所给同构, 知 $R/(p)$ 是域, 故 (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, β_i 为 R 中极大理想.

♣ 设 $X^2+5=0$ 在 $\mathbb{F}_p$ 中两根为 $x_1 \neq x_2$, 则有

$$R/(p) \simeq \mathbb{F}_p[X]/(X^2+5) \simeq \mathbb{F}_p[X]/(X-x_1, X-x_2).$$

由中国剩余定理, 这同构于 $\mathbb{F}_p[X]/(X-x_1) \times \mathbb{F}_p[X]/(X-x_2) \simeq \mathbb{F}_p \times \mathbb{F}_p$. 由于 R 中包含 (p) 的素理想一一对应到 $R/(p)$ 中的素理想, 由此同构知其对应到 $\mathbb{F}_p \times \mathbb{F}_p$ 中的素理想. 而形如域的乘积的环的素理想容易确定 (见 03-16习题 3), $\mathbb{F}_p \times \mathbb{F}_p$ 的素理想即为 $0 \times \mathbb{F}_p$ 和 $\mathbb{F}_p \times 0$, 那么

$$R/\mathfrak{P}_i \simeq (\mathbb{F}_p \times \mathbb{F}_p)/(\mathbb{F}_p \times 0) \simeq \mathbb{F}_p,$$

故 R 恰有两个包含 p 的素理想 $\mathfrak{P}_1, \mathfrak{P}_2$, 且为极大理想. ♢

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 $(p) \subsetneqq \mathfrak{P}$. 特别地, $\mathfrak{P}$ 为 R 中极大理想.

♣ 设 $X^2+5=0$ 在 $\mathbb{F}_p$ 中的重根为 x_0, 则有 $R/(p) \simeq \mathbb{F}_p[X]/(X^2+5) \simeq \mathbb{F}_p[X]/(X-x_0)^2$. 同*4*中论述, R 中真包含 (p) 的素理想 $\mathfrak{P}$ 对应到 $\mathbb{F}_p[X]/(X-x_0)^2$ 中的非零素理想, 进一步对应到 $\mathbb{F}_p[X]$ 中真包含 $(X-x_0)^2$ 的唯一素理想 $(X-x_0)$. 注意到此时有 $R/\mathfrak{P} \simeq \mathbb{F}_p[X]/(X-x_0) \simeq \mathbb{F}_p$, 故 $\mathfrak{P}$ 为 R 中极大理想. ♢

6. 3 不是 R 中素元, 即 (3) 不是 R 中素理想.

♣ 考虑 $(1+\sqrt{5}i)(1-\sqrt{5}i)=6 \in (3)$. ♢

7. 以下映射保持乘法

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

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

♣ 验证即可. ♢

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

♣ 类似上*5*验证, 注意此处 N 取值在 $\mathbb{N}$ 中. ♢

9. 3 是 R 中不可约元.

♣ 因为 $3 = xy \Rightarrow 9 = N(3) = N(x)(y)$. 若 $x, y \notin R^*$, 则 $N(x) = N(y) = 3$, 但 $a^2 + 5b^2 = 3$ 无整数解. ♢

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*)

♣ 任取 $0 \neq x \in \mathfrak{P}$, 有 $N(x) \in \mathfrak{P}$, 故 $\mathfrak{P} \cap \mathbb{Z} \neq (0)$. 考虑以下交换图:

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}[X] \\ \downarrow{\scriptstyle i} & \swarrow & \\ \dfrac{\mathbb{Z}[X]}{(X^2+5)} & & \end{array}$$

那么 $\mathfrak{P} \cap \mathbb{Z} = i^{-1}(\mathfrak{P})$, 为素理想的原像, 是 $\mathbb{Z}$ 中一非零素理想 (p). 再利用*4*,*5*, 可知 $\mathfrak{P}$ 为 R 中一包含 (p) 的极大理想. ♢

注: 本例事实上研究了 $\mathbb{Z}$ 中素理想 (p) 在 $\mathbb{Q}[\sqrt{-5}]$ 的代数整数环 $\mathbb{Z}[\sqrt{-5}]$ 上的分歧行为. *3*对应的是 $(\dfrac{-5}{p}) = -1$ 的情况, *4*对应的是 $(\dfrac{-5}{p}) = 1$ 的情况, *5*对应的是 $p = 2$ 或 $p = 5$ 的情况.

又注: 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 $f(X) \in A[X]^*$.

♣ 取 N 充分大, 使得 $(a_1X + \cdots + a_nX^n)^N = 0$. 则

$$f = a_0 + (a_1X + \cdots + a_nX^n) \mid a_0^{2N+1} + (a_1X + \cdots + a_nX^n)^{2N+1},$$

而后者是 $a_0^{2N+1} \in A[X]^*$. 故 $f(X) \in A[X]^*$. ♢

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

♣ 设 $f^{-1}(X) = g(X) = b_0 + b_1X + \cdots + b_nX^n$, 比较式 $fg = 1$ 两侧常数项系数知 $a_0b_0 = 1$, 故 $a_0 \in A*$. ♢

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.

♣ 考虑 $mod\ \mathfrak{P}$ 环同态:

$$A[X] \to A/\mathfrak{P}[X]$$

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \mapsto \bar{f}(X) = \bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_nX^n$$

显然, 如果 $f(X) \in A[X]^*$, 则 $\bar{f}(X) \in A/(\mathfrak{P})[X]$. 而后者系数在一整环内, 由*2* , 知 $\bar{a}_1 = \cdots = \bar{a}_n = 0$, 即 $a_1, \cdots, a_n$ 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.

♣ 利用*3*, 知 $a_1, \cdots, a_n$ 在 A 中所有素理想的交中, 即在 A 中所有幂零元形成的集合中, 故 $a_1, \cdots, a_n$ 均为幂零元. 再如*2*中设出 $g = f^{-1}$, 注意到*2*的结论成立不依赖 A 是整环这一条件, 于是 $a_0 \in A^*$. ♢

注: 本例也可直接设出 $g = f^{-1}$, 通过比较 $fg = 1$ 两侧的系数来直接得出结论, 但步骤较为繁琐.

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.

♣ 由初等数论知识, 我们知道 $mod\ p$ 的原根存在, 不妨设为 g, 则由原根定义, 知 g 为 $\mathbb{F}_p^*$ 中的 $p-1$ 阶元, 故 $\mathbb{F}_p^*$ 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:$a \mapsto (\frac{a}{p})$.

♣ 该同态被原根 g 的像唯一决定. 考虑原根 g 在该同态下的像: 若为 1, 则该同态是 id; 若为-1, 则该同态将 g^k 映射到 $(-1)^k$. 这就是从 $\mathbb{F}_p^*$ 到 $\{\pm 1\}$ 的唯一的非平凡群同态.(事实上即为 Legendre 符号). ♢

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.

♣ 仍考虑原根 g, 则 g 在该同态下的像为 $g^{\frac{p-1}{2}} = -1 \in \mathbb{F}_p^*$. 故该同态取值于 $\{\pm 1\} \subset \mathbb{F}_p^*$, 且为非平凡群同态. ♢

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

♣ 考虑群同态 $\{\pm 1\} \subset \mathbb{F}_p^* \to \{\pm 1\} \subset \mathbb{C}^*, \bar{1} \mapsto 1, -\bar{1} \mapsto -1$. 将这个群同态与*3*中的群同态复合, 得到一非平凡群同态 (因为 $p \neq 2$)$\mathbb{F}_p^* \to \{\pm 1\} \subset \mathbb{C}$. 利用*2*及该同态的存在唯一性, 可知对 $\forall a \in \mathbb{F}_p^*$, 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.

♣ 在 $\mathbb{Z}[i]$ 上定义范数:

$$N\colon \mathbb{Z}[i] \to \mathbb{N}$$

$$a+bi \mapsto a^2+b^2$$

容易验证, 该范数与我们先前定义过的范数一样保持乘法. 对于 $\forall a,b \in \mathbb{Z}[i]$, 试图寻找 $q \in Z[i]$, 使得 $N(r) = N(a-bq) < N(b)$. 为此, 我们将 N 的定义域扩大到 $\mathbb{Q}[X]$ 上 (注意此时 N 仍是乘法群同态), 考虑等价式 $N(\frac{a}{b}-q) = N(r)/N(b) < 1$. 我们知道 $\frac{a}{b} \in \mathbb{Q}[i]$, 故 $N(\frac{a}{b}-q) \leqslant (\frac{1}{2})^2+(\frac{1}{2})^2 = 1/2 < 1$, 故我们想要寻找的 q 总是存在的. 因此 $\mathbb{Z}[i]$ 为 Euclide 整环. ♢

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

♣ 利用*1*中定义的范数易得此结论. ♢

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 $\{(a+ib),(a-ib)\} = \{\mathfrak{P}_1, \mathfrak{P}_2\}$.

♣ 考虑环同构 $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2+1)$, 并利用 2022-02-28 讲义中例 2的结论即可 (注意 $X^2+1=0$ 在 $\mathbb{F}_p$ 中有重根等价于 $p=2$, 有两异根等价于 $p \equiv 1 \ mod\ 4$, 无根等价于 $p \equiv 3 \ mod\ 4$). ♢

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.

♣ 设 $n = m^2 n_0$, n_0 是 n 的无平方因子部分.

$\Leftarrow$: 如果 $n_0 = 1$, 则 $n = m^2 + 0^2$. 若 $n_0 \geqq 2$, 则 $n_0 = p_1 \cdots p_s, p_1, \cdots, p_s$ 为 $s \geqq 1$ 个不同的素数, 并且 $p_i = 2$ 或者 $p_i \equiv 1 \ mod\ 4$. 若 $p_i = 2$, 则 $p_i = 1^2 + 1^2$. 若 $p_i \equiv 1 \ mod\ 4$, 则由 *3* 知存在 $a, b \in \mathbb{Z}$ 使得 $p = a^2 + b^2$. 再由: 若 n 和 m 均可以表示成两个整数的平方和, 则 nm 也可以表示成两个整数的平方和, 知 $n_0 = p_1 \cdots p_s$ 可以表示成两个整数的平方和, 故 n 可以表示成两个整数的平方和.

$\Rightarrow$: 假设 n 可以表示成两个整数的平方和, 则 $\mathbb{Z}[i]$ 中有 $a + bi$ 使得 $N(a + bi) = a^2 + b^2 = n$. 如果存在素数 $p \equiv 3 \ mod\ 4$, 使得 $p \mid n_0$, 则 $n = m^2 n_0$ 在 $\mathbb{Z}[i]$ 中的素因子分解式中包含 p 的奇次幂. 但另一方面, $a + bi$ 和 $a - bi$ 在 $\mathbb{Z}[i]$ 中的素因子分解式中 p 的幂次相同 (考虑共轭作用), 因此 $n = (a + bi)(a - bi)$ 在 $\mathbb{Z}[i]$ 中的素因子分解式中 p 的幂次为偶数, 矛盾! ♢

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.

♣ 同样构造范数 $N(a + bi\sqrt{2}) = a^2 + 2b^2$, 仿照上例中的*1*可证. ♢

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

♣ 设 $i\sqrt{2} = xy$, 则 $N(x)(y) = N(xy) = N(i\sqrt{2}) = 2$, 知 x 与 y 中至少有一个是 $\mathbb{Z}[i\sqrt{2}]$ 中单位. ♢

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 $(y + i\sqrt{2}) = (z)^3$;
- $(x, y) = (3, \pm 5)$.

♣ 简单分析可知 x, y 都只能为奇数. 由于 $\mathbb{Z}[i\sqrt{2}]$ 是 UFD, 可设 $p = pgcd(y + i\sqrt{2}, y - i\sqrt{2})$, 则 $p \mid 2y, p \mid 2i\sqrt{2}$, 结合 y 是奇数, 可知 $p \mid 2$, 则 $p = \pm 2i, \pm 2, \pm\sqrt{2}, \pm\sqrt{2}i, \pm i, \pm 1$, 但 $p \mid (y + i\sqrt{2})$, 故 p 只能是单位, 即 $(y + i\sqrt{2}, y - i\sqrt{2}) = 1$. 由此知 $(y + i\sqrt{2})$ 与 $(y - i\sqrt{2})$ 作为 $\mathbb{Z}[i\sqrt{2}]$ 中元素是互素的. 考虑 x 在 $\mathbb{Z}[i\sqrt{2}]$ 中的唯一因子分解 $x = p_1 \cdots p_n$, 知 $(y + i\sqrt{2})(y - i\sqrt{2}) = (p_1 \cdots p_n)^3$, 由互素知 $(y + i\sqrt{2}) = (p_{k_1} \cdots p_{k_s})^3$, 记 $p_{k_1} \cdots p_{k_s} = z$, 即有 $y + i\sqrt{2} = z^3$, 故作为理想有 $(y + i\sqrt{2}) = (z^3) = (z)^3$. 设 $z = a + bi\sqrt{2}$, 比较 $(y + i\sqrt{2}) = (a + bi\sqrt{2})^3$ 展开后系数, 可得 $b = 1, a = \pm 5, y = \pm 5$, 故 $x = 3$. ♢

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.

♣ 构造范数 $N(a + bj) = a^2 - ab + b^2$. 类似先前所做, 容易证明 $\mathbb{Z}[j]$ 是 Euclide 整环. 此时建议先完成下一小问, 然后容易据其结论确定不可约元: 所有模 3 余-1 的素数以及所有的 $(x + yj)$ 使得 $N(x + yj) = p$, 其中 p 为模 3 余 1 或 0 的素数. ♢

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

♣ 与我们之前所做的事几乎相同. 主要是考虑 Legendre 符号 $(\dfrac{-3}{p})$. ♢

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

♣ 利用环同构 $\mathbb{Z}[j] \simeq \mathbb{Z}[X]/(X^2 + X + 1)$. 考虑 $X^2 + X + 1 = 0$ 在 $\mathbb{F}_3$ 和 $\mathbb{F}_7$ 中的行为. ♢

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.

♣ 对 $\Phi_p(X+1)$ 用 Eisenstein 判别法即可. ♢

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

♣ 考虑 ζ_p 在 $\mathbb{Q}[X]$ 上的极小多项式, 由*1*知这就是 $\Phi_p(X)$, 故类似我们在讲义 2022-02-28例 1中所做的那样, 可以得到一个环同构 $\mathbb{Z}[\zeta_p] \simeq \mathbb{Z}[X]/(\Phi_p(X))$. ♢

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?

♣(q) 为 $\mathbb{Z}[\zeta_p]$ 中素理想, 等价于商环 $\mathbb{Z}[\zeta_p]/(q)$ 是整环 (注意有限整环是域). 而 $\mathbb{Z}[\zeta_p]/(q) \simeq \mathbb{F}_q/(\Phi_p(X))$, 这是整环等价于 $\Phi_p(X)$ 是 $\mathbb{F}_q[X]$ 中的不可约多项式. $p \neq q$ 时考虑扩域 $F_q(\zeta_p)$, 其中 ζ_p 是代数闭域 $\bar{\mathbb{F}}_q$ 中的 p 次本院单位根, 及其 Galois 群 (由 Frobenius 自同构生成). 此时可知 $\Phi_p(X)$ 不可约等价于 ζ_p 的共轭轨道长度是 $p-1$, 等价于 q 是模 p 的原根. ♢

注: 这个例子是要探究 $\mathbb{Z}$ 上的素理想 (q) 在分圆域上的分歧情况.(没有想到能用现有知识解决的方法, 许金兴老师本来给出的提示是: 证明这里 $\Phi_p(X)$ 在 $\mathbb{F}_q$ 中可约等价于有根, 后者等价于 $p|q-1$)

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

♣ 考虑 Euclide 整环 $\mathbb{Z}[i]$, 并将原式变为 $(y+2i)(y-2i)$, 类似例 3分析即可. ♢

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).

♣ 若 x 是奇数, 则 y 是偶数, 但此时 mod 8 可得矛盾. 故 x 是偶数, y 是奇数. 将原方程写为 $(x+\sqrt{-13})(x-\sqrt{-13})=y^3$. 利用代数数论中的事实:$\mathbb{Z}[\sqrt{-13}]$ 中素理想都是极大理想, 所有理想可以在不计次序的意义下唯一地写成一些素理想的乘积 (因此可以说理想的整除. 可以证明, 对两个理想 I,J, 有:$I \mid J \Leftrightarrow J \subset I$.). 我们证明理想 $(x+\sqrt{-13})$ 和 $(x-\sqrt{-13})$ 作为理想互素. 假设有素理想 $\mathfrak{p}$, 使得 $\mathfrak{p} \mid (x+\sqrt{-13}), \mathfrak{p} \mid (x-\sqrt{-13})$, 则 $(x+\sqrt{-13}) \in \mathfrak{p}, (x-\sqrt{-13}) \in \mathfrak{p}$, 故 $2x \in \mathfrak{p}$, $2\sqrt{-13} \in (p)$. 但 $p \mid (y^3)$, 故 $p \mid (y) \Rightarrow y \in (p)$. 又观察原方程知 $pgcd(2x, y) = 1$, 故 $1 \in (p)$, 矛盾! 因此, 理想 $(x+\sqrt{-13}$ 和 $(x-\sqrt{-13})$ 互素, 可得 $(x+\sqrt{-13}) = I^3, (x-\sqrt{-13}) = J^3$. 由 $\mathbb{Q}(\sqrt{-13})$ 的类数 $(class\ number)$ 为 2, 可知 I^2 与 J^2 均为主理想, 从而 $(x+\sqrt{-13}) = (s)I$, 知 I 为主理想. 设 $I = (a+b\sqrt{-13})$, 则 $\pm(a+b\sqrt{-13})^3 = x+\sqrt{-13} \Rightarrow \pm(-13b^3+3a^2b) = -1$(因为 $\mathbb{Q}[\sqrt{-13}]$ 中单位只有 ± 1). 故 $b = \pm 1$, 再由 $-13b^2 + 3a^2 = \pm 1$, 解出 $a = \pm 2$, 故 $x = \pm 70, y = 17$. ♢

注: 类数为 2 指 $\mathbb{Q}[\sqrt{-13}]$ 的理想类群商去其中的主理想子群后得到的陪集数为 2.

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.

♣ 直接验证即可. 注意 A 不一定是整环. ♢

将等价类集合 $A \times S/\backsim$ 记为 $S^{-1}A$ 或 A_S. 将一个等价类 $[(a, s)]$ 记为 $\frac{a}{s}$. 定义 A_S 上的加法运算和乘法运算如下:

$$A_S \times A_S \to A_S$$
$$(\frac{a}{s_1}, \frac{b}{s_2}) \mapsto \frac{a}{s_1} + \frac{b}{s_2} := \frac{as_2 + bs_1}{s_1 s_2}$$

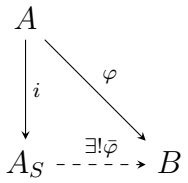
$$A_S \times A_S \to A_S$$
$$(\frac{a}{s_1}, \frac{b}{s_2}) \mapsto \frac{ab}{s_1 s_2}$$

验证上述定义是良好的 (不依赖代表元的选取), 并且在这样的加法和乘法运算下, A_S 成为一个环, 称为 A 在 S 处的局部化. 注意自然映射 $A \to A_S, a \mapsto \frac{a}{1}$ 为环同态.

♣ 直接验证即可. ♢

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:



♣ 定义 $\bar{\varphi}\colon A_S \to B, \frac{a}{s} \mapsto \varphi(a)(\varphi(s)^{-1}$. 验证这就是满足条件的环同态. 唯一性是因为 $\bar{\varphi}(\frac{a}{1})$ 由 $\varphi(a)$ 所确定, $\bar{\varphi}(\frac{1}{s}) = (\bar{\varphi}(\frac{s}{1}))^{-1}$ 由 $\varphi(s)$ 所确定. 故 $\bar{\varphi}$ 被唯一确定. ♢

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.

♣ 易见此时 i 为满射, 又 i 是单射, 故 i 是同构. ♢

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 φ 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. $I \subset IB \cap A$

♣ 注意 I 的像当然包含在 IB 中, 于是其自然包含在 IB 的原像 $IB \cap A$ 中. ♢

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

♣ 注意 $J \cap A$ 的像包含在 J 中, 其生成的理想 $(J \cap A)B$ 自然包含在 J 中. ♢

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.

♣ 由2, 只需证明 $J \subset (J \cap A)A_S$. 对 $\forall\, \dfrac{a}{s} \in J$, 有 $\dfrac{a}{1} = \dfrac{a}{s} \cdot \dfrac{s}{1} \in J$, 故 a 作为环同态 $A \to A_S$ 下 $\dfrac{a}{1}$ 的一个原像, 被包含在 $J \cap A$ 中. 因此 $\dfrac{a}{s} = \dfrac{a}{1} \cdot \dfrac{1}{s} \in (J \cap A)A_S$. 因此, A_S 中任意理想 J 均可写作 IA_S 的形式, 其中 $I = J \cap A$ 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 φ 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.

♣. 考虑 A_S 中任意一个理想 J, 则 $J \cap A$ 作为 Noether 环 A 中理想是有限生成的, 不妨记生成元为 $a_1, \ldots, a_n$, 利用3, 知 $\dfrac{a_1}{1}, \ldots, \dfrac{a_n}{1}$ 是 J 的一组生成元. 故 J 作为 A_S 中理想也是有限生成的, 这就说明了 A_S 也是 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.

♣ 对 $\forall \frac{a}{s_1}, \frac{b}{s_2}$ 使得 $\frac{a}{s_1}\cdot\frac{b}{s_2} \in \mathfrak{P}A_S$, 由 $\mathfrak{P}A_S$ 的定义, 知 $\frac{ab}{s_1s_2} = \sum_{i=1}^{k} \frac{x_i}{1}\cdot\frac{c_i}{t_i}$, 其中 $x_i \in \mathfrak{P}, \frac{c_i}{t_i} \in A_S, i = 1, \ldots, k$. 将这个等式右侧通分, 可得 $\frac{ab}{s_1s_2} = \frac{\sum_{i=1}^{k} x_i\tilde{c_i}}{t} \in A_S$, 由我们定义的等价关系, 知这表明存在 $s \in S$, 使得 $s(tab - s_1s_2\sum_{i=1}^{k} x_i\tilde{c_i}) = 0$, 即 $stab = ss_1s_2\sum_{i=1}^{k} x_i\tilde{c_i}$. 等式右侧是理想 $\mathfrak{P}$ 中元素, 故 $stab \in \mathfrak{P}$. 再由 $st \in S, \mathfrak{P} \cap S = \varnothing$, 可知 $ab \in \mathfrak{P}$. 由 $\mathfrak{P}$ 是素理想, 知 a, b 中至少有一个在 $\mathfrak{P}$ 中, 不妨设为 a, 则 $\frac{a}{s_1} = \frac{a}{1}\cdot\frac{1}{s_1} \in \mathfrak{P}A_S$. 故 $\mathfrak{P}$ 是 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:

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

♣ 由上一小问, 及环同态下素理想的原像是素理想, 可知题中两个映射都是良定的. 接下来我们证明这两个映射确实给出了所要的双射. 我们已经证明了习题 4 的*1*和*3*, 于是只需证明, 对 A 中所有与 S 无交的素理想 I, 有 $IA_S \cap A \subset I$. 对于 $a \in IA_S \cap A$, 有等式 $\frac{a}{1} = \sum_{i=1}^{k} \frac{x_ia_i}{s_i} = \frac{\sum_{i=1}^{k} x_i\tilde{a_i}}{s}$(最后一个等号是通分). 那么存在 $t \in S$, 使得 $t(sa - \sum_{i=1}^{k} x_i\tilde{a_i},$ 再结合 $I \cap S = \varnothing$, 可知 $a \in I$, 即证得 $IA_S \cap A \subset I$, 故 $IA_S \cap A = I$. 至此即给出了所需要的双射. ♢

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

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

♣ 由习题 5可知, $\mathrm{Spec}A_f$ 一一对应到 A 中所有与 $\{f^n \mid n \in \mathbb{N}\}$ 无交的素理想. 但 $f \in \cap_{\mathfrak{P}\in\mathrm{Spec}A}\mathfrak{P}$. 故不存在这样的素理想, 因此 $\mathrm{Spec}A_f = \varnothing$. ♢

2. A_f 为零环.

♣ 由于交换环中的极大理想一定是素理想, *1*表明 A_f 中没有极大理想, 故 A_f 为零环.(Krull 定理: 只要 A_f 中有非零元, 就一定存在包含这个非零元的极大理想.) ♢

3. f 为幂零元.

♣ 对 $\frac{1}{1} \in A_f$, 由上一问知 $\frac{1}{1} = 0 = \frac{0}{1}$, 也即存在 $n \in \mathbb{N}$, 使得 $f^n(1 \cdot 1 - 1 \cdot 0) = f^n = 0$, 故 f 幂零. ♢

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

♣ 我们已经证明了 $\cap_{\mathfrak{P} \in \mathrm{Spec}A} \mathfrak{P} \subset \{f \in A \mid f \text{ 为幂零元}\}$. 对 $\forall f, f$ 幂零, 存在 $n \in \mathbb{N}$, 使得 $f^n = 0 \in \mathfrak{P}$, 故 $f \in \mathfrak{P}$ 对 $\forall \mathfrak{P} \in \mathrm{Spec}A$ 成立, 即有 $f \in \cap_{\mathfrak{P} \in \mathrm{Spec}A} \mathfrak{P}$. 故 $\cap_{\mathfrak{P} \in \mathrm{Spec}A} \mathfrak{P} = \{f \in A \mid f \text{ 为幂零元}\}$. ♢

利用局部化的万有性质, 证明如下局部化与商的交换性:

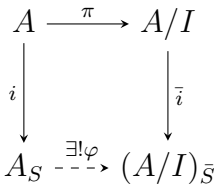
习题 **7.** 设 S 为环 A 的乘法子集, 设 I 为 A 的理想. 记 $\bar{S} \in A/I$ 为 S 在商映射 $A \to A/I$ 下的像.

1. $\bar{S}$ 为 A/I 中的乘法子集.

♣ 首先 $\bar{1} \in \bar{S}$, 因为 $1 \in S$. 其次, 任意 $\bar{s}_1, \bar{s}_2 \in \bar{S}$, 我们可以分别找到两个原像 $s_1 \in S, s_2 \in S$, 故 $s_1 s_2 \in S \Rightarrow \bar{s}_1 \bar{s}_2 \in \bar{S}$. ♢

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

♣ 考虑以下交换图表:



其中 π 为商映射, i 和 $\bar{i}$ 为相应的局部化环同态. 由于 $\bar{i}\circ\pi(S)=\{s+I\mid s\in S\}\in(A/I)^*_{\bar{S}}$, 由习题 2中所证明的局部化的万有性质, 知存在唯一的映射 $\varphi\colon A_S\to(A/I)_{\bar{S}}$, 使得图表交换. 回顾我们在习题 2中对 φ 的构造, 可知 $\varphi(\frac{a}{s})=\bar{i}\circ\pi(a)(\bar{i}\circ\pi(s))^{-1}=\frac{a+I}{s+I}$, 故 φ 是满射, 且 $\ker\varphi=\{\frac{a}{s}\mid a\in I\}=IA_S$. 故由同态基本定理可得环同构:$A_S/IA_S\simeq(A/I)_{\bar{S}}$. ♢

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 $D(f):=\{\mathfrak{P}\in\mathrm{Spec}A|f(\mathfrak{P})\neq0\}=\{\mathfrak{P}\in\mathrm{Spec}A|f\notin\mathfrak{P}\}$.

♣ 我们先验证这确实给出了一个 $Zariski$ 拓扑, 这是因为:

$$V(I)\cap V(J)=V(I+J)$$

$$V(I)\cup V(J)=V(IJ)$$

$$\mathrm{Spec}A=V(\{0\})$$

$$\varnothing=V(A)$$

其中 $V(I)\cup V(J)=V(IJ)$ 是因为: 若 $IJ\subset\mathfrak{P}$, 则 $I\subset\mathfrak{P}$ 或 $J\subset\mathfrak{P}$, 否则可取出 $a\in I\backslash\mathfrak{P}$ 和 $b\in J\backslash\mathfrak{P}$, 由于 $\mathfrak{P}$ 是素理想, 知 $ab\notin\mathfrak{P}$, 这与 $IJ\subset\mathfrak{P}$ 矛盾. 故 $V(I)\cup V(J)\subset V(IJ)$. 而另一个方向的包含是显然的. ♢

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

♣ 首先说明 $D(f)$ 是该 $Zariski$ 拓扑中的开集, 这等价于 Spec$A\backslash D(f)$ 是一个闭集. 记主理想 $(f)=I_f$, 则有 Spec$A\backslash D(f)=\{\mathfrak{P}\in\mathrm{Spec}A|f\in\mathfrak{P}\}=\{\mathfrak{P}\in\mathrm{Spec}A|I_f\subset\mathfrak{P}\}=V(I_f)$. 故 $D(f)$ 作为闭集 $V(I_f)$ 的补集是一个开集. 下面证明 $\{D(f)|f\in A\}$ 构成了 Spec$A$ 中的一组开集基. 对 Spec$A$ 中某开集 U, 其补集 Spec$A\backslash U$ 为闭集, 则 U 可以表示成一些 $D(f)$ 的并集等价于 Spec$A\backslash U$ 可以表示成一些 Spec$A\backslash D(f)$ 的交集. 我们知道, 存在理想 $I\subset A$ 使得闭集 Spec$A\backslash U=V(I)$. 因此只需找到一些 $D(f)$, 使得 $V(I)=\cap(\mathrm{Spec}A\backslash D(f))=\cap V(I_f)=V(\sum I_f)$. 因此我们只需让 f 取遍 I 中元素 (若 I 为有限生成理想, 则只需要取遍 I 的生成元), 即有 Spec$A\backslash U=V(I)=V(\sum I_f)=\cap V(I_f)=\cap(\mathrm{Spec}A\backslash D(f))=\mathrm{Spec}A\backslash(\cup D(f))$. 因此 $\{D(f)|f\in A\}$ 构成了 Spec$A$ 中的一组开集基. ♢

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 $\frac{a}{f^n} \in A_f$, 对于 $\mathfrak{P} \in D(f)$, 取值为 $\frac{a}{f^n}(\mathfrak{P}) := a(\mathfrak{P})/f(\mathfrak{P})^n$. 此为 A_f 的几何解释, 即看作开子集 $D(f)$ 上的函数环.

♣ 注意 $D(f) = \{\mathfrak{P} \in \mathrm{Spec}A | f \notin \mathfrak{P}\} = \{\mathfrak{P} \in \mathrm{Spec}A | \{f, f^2, f^3, \ldots\} \cap \mathfrak{P} = \varnothing\} \leftrightarrow \mathrm{Spec}A_f$(通过习题 5给出的双射). 那么对于 $\frac{a}{f^n} \in A_f$, 对于 $\mathfrak{P} \in D(f)$, 通过这个双射给出取值规则:$\frac{a}{f^n}(\mathfrak{P}) := \frac{a}{f^n}(\mathfrak{P}A_f) = \overline{(\frac{a}{f^n})} \in (A_f)_{\mathfrak{P}A_f}/\mathfrak{P}A_f(A_f)_{\mathfrak{P}A_f}$(同构于 $Frac(A_f/\mathfrak{P}A_f)) \mapsto \frac{\bar{a}}{\bar{f}^n} = a(\mathfrak{P})/f(\mathfrak{P})^n \in Frac(A_f/\mathfrak{P}A_f)$. 这便解释了我们为何如此定义 A_f 中元素在 $D(f)$ 上的取值. ♢

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 $\{[(f,U)|f(x) = 0\}$.

♣ 对于 $[(f,U)]$ 使得 $f(x) \neq 0$. 由 f 连续, 存在 x 的邻域 V, 使得 $f(y) \neq 0, \forall y \in V$. 取 $[(g,V)]$, 其中 $g(x) = (f(x))^{-1}$. 这自然给出了 $[(f,U)]$ 的一个逆. 换言之, $\mathcal{C}^*_{X,x} = \{[(f,U)|f(x) \neq 0\}$. 现在考虑 $\{[(f,U)|f(x) = 0\}$, 这个集合确实是一个理想, 且包含了所有 $\mathcal{C}_{X,x}$ 中的不可逆元. 由此知这是 $\mathcal{C}_{X,x}$ 的唯一极大理想. ♢

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 $\mathcal{C}_{X,x}$.

♣ 我们只需证明: 将开集 U,V,W 均换为一个固定的开集基中的元素后新得到的函数芽环中的等价类包含原先的每一个等价类. 对于原先的某个等价类 $[(f,U)]$, 由开集基的定义可知, 存在开集基中的元素 O, 使得 $x \in O \subset U$, 为此有等价关系 $(f,U) \sim (f,O)$. 因此我们可以简单地将所有开集换为某个开集基中的元素, 同时保持原来所有的等价类. ♢

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 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 φ 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 $J\cap A := \varphi^{-1}(J)$)

♣ 首先该映射良定. 考虑 $\bar{b} = b + J \in B/J$, 由于 b 在 A 上整, 存在 $n \geq 1, a_0, \cdots, a_{n-1} \in A$, 使得 $b^n + \varphi(a_{n-1})b^{n-1} + \cdots + \varphi(a_1)b + \varphi(a_0) = 0$. 将这个式子两边模去理想 J, 有 $\bar{b}^n + \overline{\varphi(a_{n-1})}\bar{b}^{n-1} + \cdots + \overline{\varphi(a_1)}\bar{b} + \overline{\varphi(a_0)} = 0$. 那么, 可以选择 $\bar{a_i} \in A/J\cap A, 0 \leq i \leq n-1$, 使得 $\varphi(\bar{a_i}) = \overline{\varphi(a_i)}$. 于是得到系数在 $\varphi(A/J\cap A)$ 中的关于 $\bar{b}$ 的首一零化多项式, 也就说明了 B/J 在 $A/A\cap J$ 上是整的. ♢

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.)

♣ 由 φ 是环同态, 知 $\varphi(S)$ 为 B 中乘法系. 由 $\varphi(S) \subset B_S^*$, 诱导映射 $A_S \to B_S$. 取 $\dfrac{b}{s_0} \in B_S$, 其中 $s_0 = \varphi(s), s \in A$. 考虑 b 的首一零化多项式 $b^n + \varphi(a_{n-1})b^{n-1} + \cdots + \varphi(a_1)b + \varphi(a_0) = 0$, 那么 $(\dfrac{b}{s_0})^n + \varphi(\dfrac{a_{n-1}}{s})(\dfrac{b}{s^0})^{n-1} + \cdots + \varphi(\dfrac{a_1}{s^{n-1}})\dfrac{b}{s_0} + \varphi(\dfrac{a_0}{s^n}) = 0$. 这便

说明了 $\dfrac{b}{s_0}$ 在 A_S 上整, 于是 $A_S \to B_S$ 是整扩张. ♢

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.

♣ $\Rightarrow$: 取 $0 \neq b \in B$, 则有 $n \geq 1, a_0, \cdots, a_{n-1} \in A$, 使得 $b^n + \varphi(a_{n-1})b^{n-1} + \cdots + \varphi(a_1)b + \varphi(a_0) = 0$ (由于 B 是整环, 总可以使得 $\varphi(a_0) \neq 0$, 再由 φ 是单同态, 知 $a_0 \neq 0$), 则 $b \cdot (-\varphi(a_0^{-1})(b^{n-1} + \varphi(a_{n-1})b^{n-2} + \cdots + \varphi(a_1))) = 1$, 故 $b \in B^*$, 即 B 是域.

$\Leftarrow$: 取 $0 \neq a \in A$, 则由于 φ 是单同态, 有 $0 \neq \varphi(a) \in B$, 其在 B 中有逆 $\varphi(a)^{-1}$, 考虑其首一零化多项式:$(\varphi(a)^{-1})^n + \varphi(a_{n-1})(\varphi(a)^{-1})^{n-1} + \cdots + \varphi(a_1)\varphi(a)^{-1} + \varphi(a_0) = 0$. 在该式两侧同乘 $\varphi(a)^{n-1}$, 可得 $\varphi(a)^{-1} = -(\varphi(a_{n-1}) + \cdots + \varphi(a_1)\varphi(a)^{n-2} + \varphi(a_0)\varphi(a)^{n-1}) \in \varphi(A)$. 故存在唯一 $c \in A$, 使得 $\varphi(c) = \varphi(a)^{-1}$, 由 φ 是单同态, 知 $a^{-1} = c \in A$. 故 A 是域. ♢

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.

♣ 利用*1*和习题 1, 可知 $A/J \cap A \to B/J$ 是整环之间的单同态, 同时也是整扩张, 因此 $A/J \cap A$ 是域 $\Leftrightarrow$ B/J 是域, 也即 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 $\mathfrak{P} \cap A \neq (0)$.

♣ 在 $S = A \backslash \mathfrak{P} \cap A$ 处作局部化. 那么可以验证 $A_S \to B_S$ 仍然是整环之间的单同态 (直接验证 ker 为 0), 同时也是整扩张 (习题 1.*2*). 于是, $\mathfrak{P}B_S$ 作为 B_S 的理想, 其原像 $\mathfrak{P}B_S \cap A_S = (\mathfrak{P} \cap A)A_S$ 是 A_S 的极大理想. 故由 *2.* 知 $\mathfrak{P}B_S$ 为 B_S 的极大理

想, 且非零 (题设), 从而 B_S 不是域, 于是由1知 A_S 不是域, 进而 $(\mathfrak{P}\cap A)A_S\neq 0$ 得到 $\mathfrak{P}\cap A\neq 0$. ♢

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.

♣ 由 f 的不可约性知 $\mathbb{C}[x,y]/(f)$ 是整环. 由于 $\mathbb{C}[x]$ 的像里 y 的次数均为 0, 故该同态的 ker 为 0, 是单同态. $\mathbb{C}[x,y]/(f)$ 在 $\mathbb{C}[x]$ 上由 $\bar{y}$ 生成, 而 f 即成为 $\bar{y}$ 的首一零化多项式, 故 $\bar{y}$ 在 $\mathbb{C}[x]$ 上整, 进而该扩张为整扩张. ♢

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 $\mathfrak{m}/(f)\cap\mathbb{C}[x]=(x-a)$.

♣ 由商环中的理想与 $\mathbb{C}[x,y]$ 中包含 (f) 的理想的对应, 极大理想对应到极大理想, $\mathfrak{m}/(f)$ 为 $\mathbb{C}[x,y]/(f)$ 的极大理想. 利用习题 2 中的2, 立刻得到此结论. ♢

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

♣ 由理想对应关系知 $\mathfrak{m}/(f,x-a)$ 是 $\mathbb{C}[x,y]/(f,x-a)$ 中的极大理想. 每个 $c_i(x)-c_i(a)\in(x-a)$, 故 $f(x,y)-f(a,y)\in(x-a)$, 从而 $(f,x-a)=(f(a,y),x-a)$, 进而 $\mathbb{C}[x,y]/(f,x-a)\simeq\mathbb{C}[x,y]/(f(a,y),x-a)\simeq\mathbb{C}[y]/(f(a,y))$. ♢

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

♣ $\mathfrak{m}/(f,x-a)$ 对应到 $\mathbb{C}[y]/(f(a,y))$ 中的极大理想, 进而对应到 $\mathbb{C}[y]$ 中包含 $(f(a,y))$ 的极大理想, 具有形式 $(y-b)$, 也即 $\mathfrak{m}/(f,x-a)\simeq(y-b)/(f(a,y))$. 由该同构的对应知 $y-b+(f,x-a)\in\mathfrak{m}/(f,x-a)$, 即 $(y-b)\in\mathfrak{m}$, 故 $(x-a,y-b)\subseteq\mathfrak{m}$.

由 $(x-a, y-b)$ 的极大性即得到 $\mathfrak{m} = (x-a, y-b)$. ♢

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:

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

♣ 考虑 $g(x,y) = h_n(x)y^n + \cdots + h_1(x)y^1 + h_0(x)$, 其中 $h_i(x) \in \mathbb{C}[x]$. 考虑各 h_i 中次数最高者, 设为 $h_m(x)$(若有多个则取 i 最大者), 并记 $h_i(x)$ 的次数为 d_i. 令 $k = n+1$, 则 $h_i(x)y^i$ 代换后得到 $\tilde{h}_i(x',y') = h_i(x'+y'^n)y'^i$, 且 $\tilde{h}_m(x',y')$ 中 y' 的次数为

$$(n+1)d_m + m \geq \begin{cases} (n+1)(d_m-1) + n + 1 > (n+1)d_i + i, & i > m \\ (n+1)d_i + m > (n+1)d_i + i, & i < m \end{cases}.$$

这说明 $\tilde{h}_m$ 中 y' 的次数唯一最高, 且最高次不含 x', 取 λ 为对应系数的逆即得. ♢

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.

♣ 由于 $g_1(x,y)g_2(x,y)$ 中 y 的最高次项直接由 g_1, g_2 各自的最高次项相乘得到, 故各自最高次系数为 $\mathbb{C}[x]$ 中可逆元, 故 g_1g_2 首一 $\Rightarrow g_1, g_2$ 首一. 由于 g 首一, 故不含 $\mathbb{C}[x]$ 中次数大于 0 的因子, 进而 h 首一, 且 y 的次数大于 0. ♢

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

♣ 对 $\mathbb{C}[x,y]$ 的任一极大理想 $\mathfrak{M}$, 由于 $\mathbb{C}[x,y]$ 不是域, $\mathfrak{M}$ 非 0. 任取其中一非零元

g, 由5. 中的变量代换给出 $\mathbb{C}$-代数同态

$$\varphi\colon \mathbb{C}[x,y]\to\mathbb{C}[x',y']$$

$$x\mapsto x'+y'^k,\quad y\mapsto y'$$

且 $x'\mapsto x-y^k$, $y'\mapsto y$ 给出逆, 故 φ 为同构, 且 $\varphi(g)$(也即5.中的 $\tilde{g}$) 关于 y 的首项系数可逆. 由于 $g\in\mathfrak{M}$, 故不为可逆元, 其关于 y 的次数大于 1, 所得到的 $\varphi(g)$ 恰符合6中条件, 故 $\varphi(g)$ 的不可约因子均关于 y 首一且次数大于 0. 由于 φ 是同构 $\varphi(\mathfrak{M})$ 为极大理想, 进而是素理想, 至少有一个 $\varphi(g)$ 的素因子属于 $\varphi(\mathfrak{M})$. 此时 $\varphi(\mathfrak{M})$ 含有一个关于 y 首一的不可约多项式, 利用4, 故存在 $a,b\in\mathbb{C}$ 使得 $\varphi(\mathfrak{M})=(x'-a,y'-b)$. 这给出 $\mathfrak{M}=(x-y^k-a,y-b)=(x-b^k-a,y-b)$. ♢

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 $a_1,\cdots,a_n\in\mathbb{C}$.

♣ 归纳证明. 假定结论对 $n-1$ 成立, 对任一极大理想 $\mathfrak{M}$ 取定非 0 元, 模仿5和6, 利用变量代换 $x_1\mapsto x_1'+x_n'^{k_1},\cdots,x_{n-1}\mapsto x_{n-1}'+x_n'^{k_{n-1}}$ 得到 $\mathfrak{M}$ 中的关于 x_n 次数大于 0 的首一不可约多项式 f, 模仿1.2.3.4. 依次验证 $\mathbb{C}[x_1,\cdots,x_{n-1}]\hookrightarrow\mathbb{C}[x_1,\cdots,x_n]/(f)$ 为整扩张, 则 $\mathfrak{M}/(f)\cap\mathbb{C}[x_1,\cdots,x_{n-1}]$ 为极大理想, 且由归纳假设知其形如 $(x_1-a_1,\cdots,x_{n-1}-a_{n-1})$, 由此给出同构

$$\mathbb{C}[x_1,\cdots,x_n]/(f,x_1-a_1,\cdots,x_{n-1}-a_{n-1})\simeq\mathbb{C}[x_n]/(f(a_1,\cdots,a_{n-1},x_n)),$$

进而模仿4即可证明结论. ♢

注: 我们再给出两种更简短的 Hilbert 零点定理弱形式的证明.

1. 设 $\mathfrak{m}$ 为 $\mathbb{C}[X_1,\cdots,x_n]$ 中的极大理想. 对 $1\leq i\leq n$, 定义代数同态 $\phi_i\colon \mathbb{C}[X_i]\to \mathbb{C}[X_1,\cdots,X_n]/\mathfrak{m}=:K,\ X_i\mapsto \bar{X_i}$. 我们断言 $K=\mathbb{C}$, 这只需证明 $\mathbb{C}[X_1,\cdots,X_n]/\mathfrak{m}$ 是 $\mathbb{C}$ 上的代数扩张 (由 $\mathbb{C}$ 为代数闭域可以立刻得到 $K=\mathbb{C}$). 由于 $\mathbb{C}$ 上的任何超越扩张作为 $\mathbb{C}$-线性空间都是不可数维的 (因其至少包含 $\mathbb{C}(x)$, 而 $\bigcup\limits_{\alpha\in\mathbb{C}}\{(x-\alpha)^{-1}\}$ 在 $\mathbb{C}(x)$ 中线性无关: 对 $(\alpha_1,\ldots,\alpha_n)\in\mathbb{C}^n$, 记 $F(x)=\sum\limits_{i=0}^{n}c_i(x-\alpha_i)^{-1}$, 则当 $x\to\alpha_i$ 时, 有 $|F(x)|\to\infty$, 因而 F 不可能是零函数, 也即 $\bigcup\limits_{\alpha\in\mathbb{C}}\{(x-\alpha)^{-1}\}$ 在 $\mathbb{C}(x)$ 中线性无关), 故 $\mathbb{C}[X_1,\cdots,X_n]/\mathfrak{m}$ 作为可数维 $\mathbb{C}$-线性空间一定是 $\mathbb{C}$ 的代数扩张, 从而 $K=\mathbb{C}$, 故 ϕ_i 是满射, 由第一同构定理得出 $\mathrm{Ker}(\phi_i)$ 为极大理想. 不妨设 $\mathrm{Ker}(\phi_i)=(X_i-a_i)$, 则 $\phi_i(X_i-a_i)=\bar{0}\in\mathbb{C}[X_1,\cdots,X_n]/\mathfrak{m}$, 这说明 $(X_i-a_i)\subset\mathfrak{m}$. 让 i 取遍 $1,\ldots,n$, 可知 $(X_1-a_1,\ldots,X_n-a_n)\subset\mathfrak{m}$, 而前者由 *1.* 知是一个极大理想, 故 $\mathfrak{m}=(X_1-a_1,\ldots,X_n-a_n)$. ♢

2. 任给极大理想 $\mathfrak{m}$, 考虑 $K=\mathbb{C}[x_1,\cdots,x_n]/\mathfrak{m}=\mathbb{C}[\bar{x}_1,\cdots,\bar{x}_n]$ 为域, 且有自然同态 $\mathbb{C}\to K$, 故是一个 $\mathbb{C}$ 的域扩张. 记以上商去 $\mathfrak{m}$ 的映射为 π, 我们将证明 K 在 $\mathbb{C}$ 上整 (代数), 从而由 $\mathbb{C}$ 代数闭知 $K=\mathbb{C}$, 这会导出诸 $\bar{x}_i\in\mathbb{C}$, 进而 $x_i-\bar{x}_i\in\ker(\pi)$, 再由 $(x_1-\bar{x}_1,\cdots,x_n-\bar{x}_n)$ 的极大性推出其正是 $\mathfrak{m}$. 我们只需证明 $\bar{x}_i$ 在 $\mathbb{C}$ 上整, 进一步, 我们直接证明如下引理即可得出结论.

引理. 设 k 为域, $K=k[\alpha_1,\cdots,\alpha_n]$ 为域, 则诸 α_i 在 k 上整 *(代数)*.

♣ 我们对 n 归纳证明结论. 当 $n=1$ 时, 若 $k[\alpha]$ 为域, 由于 α^{-1} 为 α 的 k 系数多项式, 设为 $a_n\alpha^n+\cdots+a_1\alpha+a_0$, 则 $0=\alpha\alpha^{-1}-1=a_n\alpha^{n+1}+\cdots+a_0\alpha-1$, 故 α 在 k 上整. 假定对扩进 $n-1$ 个元素结论成立, 假设结论对 n 不成立, 不妨设 α_1 不在 k 上整 (除以首项系数即首一). 由 K 为域知 $k[\alpha_1,\cdots,\alpha_n]=k(\alpha_1)[\alpha_2,\cdots,\alpha_n]$, 再由归纳假设知 $\alpha_2,\cdots,\alpha_n$ 均在 $k(\alpha_1)$ 上整. 假设 b_i 为 α_i 的 $k[\alpha_1]$ 系数的正次数零

化多项式的首项系数 (将 $k(\alpha_1)$ 系数的零化多项式通分即可得到), 我们扩进 b_i^{-1}, 即令 $A = k[\alpha_1, b_2^{-1}, \cdots, b_n^{-1}] \subseteq k(\alpha_1)$, 则各 α_i 在 A 上整. 注意 A 为 $k(\alpha_1)$ 的子环, 故为整环, 而 K 为 A 扩进 $\alpha_2, \cdots, \alpha_n$, 即 K 为 A 的整扩张, 且 K 为域. 由习题 2 中的*1.* 知 A 也为域, 于是 $A \supseteq k(\alpha_1) \Rightarrow A = k(\alpha_1)$, 此时 A 应含有 $k[\alpha_1]$ 中所有素元的逆. 但由于 α_1 不在 k 上整, 故 $k[\alpha_1] \simeq k[x]$ 为 UFD. 扩进每一个 b_i^{-1} 只得到 $k[\alpha_1]$ 中有限素元的逆 (由分式域的定义, 素元的定义和唯一分解性), 这说明 $k[\alpha_1]$ 只有有限个素元 $p_1, \cdots, p_k$, 但 $p_1 \cdots p_k + 1$ 的 deg 高于每个 p_i, 且与各 p_i 均互素, 导出矛盾. ♢

注: 事实上零点定理中的 $\mathbb{C}$ 可换成任一代数闭域. 此处的证法*1.*只能对势不可数的代数闭域证明, 证法*2.*可用于任意代数闭域.

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.

♣ 考虑 A-代数同态 ϕ: $A[x] \to A_f$, $x \mapsto \dfrac{1}{f}$. 由于 A_f 中元素均形如 $\dfrac{a}{f^n} = \phi(ax^n)$, 故 ϕ 为满同态. 以下计算 $\ker\phi$. 首先有 $\phi(1 - fx) = 1 - f^{-1}f = 0$, 故 $(1 - fx) \subseteq \ker\phi$. 若 $P(x) = a_n x^n + \cdots + a_1 x + a_0 \in \ker\phi$, 则 $0 = \phi(P) = \dfrac{a_n}{f^n} + \cdots + \dfrac{a_1}{f} + \dfrac{a_0}{f^0}$, 通分得到

$$\frac{a_n + a_{n-1}f + \cdots + a_1 f^{n-1} + a_0 f^n}{f^n} = 0.$$

由局部化定义, 这等价于

$$\exists k \geq 0, \quad f^k(a_n + a_{n-1}f + \cdots + a_1 f^{n-1} + a_0 f^n) = 0.$$

另一方面, 我们有

$$\begin{aligned} f^{n+k}P(x) &= f^{n+k}(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) \\ &= f^k\Big(a_n(fx)^n + a_{n-1}f(fx)^{n-1} + \cdots + a_1 f^{n-1}(fx) + a_0 f^n\Big) \\ &= f^k\left(\sum_{i=1}^{n} a_i f^{n-1}((fx)^i - 1)\right) \\ &= f^k(fx-1)\left(\sum_{i=1}^{n} a_i f^{n-i}\sum_{j=0}^{i-1}(fx)^j\right) \\ &\in (1-fx) \end{aligned}$$

其中第二个等号是减去前面等于 0 式子. 故 $x^{n+k}f^{n+k}P(x) \in (1-fx)$, 而又有 $(fx)^{n+k}-1 \in (1-fx)$, 故 $P(x) = x^{n+k}f^{n+k}P(x) - ((fx)^{n+k}-1)P(x) \in (1-fx)$, 也就证明了 $\ker\phi = (1-fx)$, 从而 $A[x]/(1-fx) \simeq A_f$. 该同构说明 A_f 为有限生成 A-代数, 故为有限生成 $\mathbb{C}$-代数. ♢

注: 由于这里 A 不一定为整环, $\ker\phi = (1-fx)$ 并不平凡. 例如考虑 $A = \mathbb{C}[x_1]/(x_1^2 - x_1)$, $f = \bar{x}_1$, 则 $\phi(x-1) = \dfrac{1}{f} - 1 = \dfrac{1-f}{f} = \dfrac{f(1-f)}{f^2} = 0$, 即 $x-1 \in \ker\phi = (1-\bar{x}_1 x)$, 但这并不容易直接观察得到 (在此例子下 $\bar{x}_1$ 在 $A_{\bar{x}_1}$ 中为 1, 此时 $A_{\bar{x}_1} = \mathbb{C}$).

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.

♣ $A_f \simeq A[x]/(1-fx) = \mathbb{C}[x_1, \cdots, x_n, x]/(I, 1-fx)$(此时为 f 任指定多项式环

中的一个代表元), 任给 A_f 的极大理想 $\mathfrak{p}$, 其对应到 $\mathbb{C}[x_1,\cdots,x_n,x]$ 的一个包含 I 和 $1-fx$ 的极大理想 $\mathfrak{P}$. 由于 $1-fx$ 与 f 互素, 故 $f\notin\mathfrak{P}$. 由弱零点定理, $\mathfrak{P}$ 具有形式 $(x_1-a_1,\cdots,x_n-a_n,x-a)$. 考虑 $I\subseteq\mathfrak{M}:=\mathfrak{P}\cap\mathbb{C}[x_1,\cdots,x_n]=(x_1-a_1,\cdots,x_n-a_n)$, 且由 $1-fx\in\mathfrak{P}$ 知 $f(a_1,\cdots,a_n)a=1$, 故 $f\notin\mathfrak{M}$(f 在 $(a_1,\ldots,a_n)$ 上的取值可逆, 故非 0), 于是我们将 $\mathfrak{p}$ 对应到 $\mathbb{C}[x_1,\cdots,x_n]$ 的一个包含 I 且不含 f 的极大理想 $\mathfrak{M}$, 而这样的理想正对应 $A=\mathbb{C}[x_1,\cdots,x_n]/I$ 的不含 f 的极大理想 $\mathfrak{m}$. 反之, 任给一个这样的 $\mathfrak{m}$, 我们可以对应到 $\mathfrak{M}\subset\mathbb{C}[x_1,\cdots,x_n]$ 包含 I 而不含 f. 由弱零点定理 $\mathfrak{M}=(x_1-b_1,\cdots,x_n-b_n)$. 若其上方有极大理想 $\mathfrak{P}=(x_1-b_1,\cdots,x_n-b_n,x-b)\in\mathbb{C}[x_1,\cdots,x_n,x]$, 则其包含 I. 其包含 $1-fx$ 当且仅当 $1=bf(b_1,\cdots,b_n)$, 故存在唯一的 $\mathfrak{P}$ 满足之前的条件, 这给出其在 $A[x]/(1-fx)$ 中的对应 $\mathfrak{p}$, 我们也给出了 $\mathfrak{m}$ 到 $\mathfrak{p}$ 的对应. 从以上对应过程易于看出这给出 $\{A_f$的极大理想$\}$ 与 $\{A$中不包含f的极大理想$\}$ 之间的一对互逆双射. ♢

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.

♣ 由*2*立得 A_f 无极大理想, 也即 A_f 为零环. 这表明 $\frac{1}{f}=0$, 由局部化定义, 存在 $k\in\mathbb{N}^*$, 使得 $f^k=0$, 即 f 为 A 中幂零元. ♢

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 $f\in\sqrt{I}:=\{h\in\mathbb{C}[x_1,\cdots,x_n]\mid\exists m\geq1,h^m\in I\}$.

♣ 设 $A=\mathbb{C}[x_1,\cdots,x_n]/I$, 并在 f 处对 A 作局部化. 此时 A 中的极大理想对应到 $\mathbb{C}[x_1,\cdots,x_n]$ 中包含 I 的极大理想, 即形如 $\mathfrak{m}=(x_1-a_1,\cdots,x_n-a_n)$, $I\subset\mathfrak{m}$ 的极大

理想. 而这些极大理想一一对应到 $V(I) = \{x \in \mathbb{C}^n \mid g(x) = 0, \forall g \in I\}$. 由题设知这些极大理想都包含 f. 应用3, 知 f 是 $A = \mathbb{C}[x_1, \cdots, x_n]/I$ 中的幂零元, 即 f 在根式理想 $\sqrt{I}$ 中. ♢

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

♣ 这是局部环的另一个等价定义. 因为一切不可逆元都一定包含在某个极大理想中 (Krull), 即 m 中. ♢

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

♣ 若 $a\in A^*$, 则取 $k=0,u=a$ 即可. 否则 $\pi|a$, 若不存在题中所述表示, 考虑理想升链 $(a)\subsetneq(\frac{a}{\pi})\subsetneq(\frac{a}{\pi^2})\subsetneq\cdots$, 这自然与 A 是 Noether 环矛盾. ♢

3. A 为主理想整环 (PID) 从而为 (UFD).

♣ 由*2*可知所有理想均形如 (π^k), $k\in\mathbb{N}$. 事实上, 对任意理想 I, 考虑其中元素作形如*2.*分解后所得 k 的最小值, 那么 $I\subset(\pi^k)$, 但同样有 $(\pi^k)=(u\cdot\pi^k)\subset I$, 故 $I=(\pi^k)$. 因此 A 为主理想整环 (PID) 从而为 (UFD). ♢

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

♣ 主理想整环中一切素理想均为极大理想. ♢

离散赋值环的例子:$\mathbb{Z}_p,\mathbb{C}[[x]]$, 以及 $\mathbb{Z}_{(p)}:=\{\frac{a}{b}\mid a\in\mathbb{Z},p\nmid b\}$($\mathbb{Z}_{(p)}$ 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.

♣ 对任意 A 的非零素理想 $\mathfrak{P}$, 考虑包含 $\mathfrak{P}$ 的极大理想 I, 则 I 也是素理想, 作局部化得一离散赋值环 A_I, 那么由讲义 2022-03-09 习题 5.2知, $\mathfrak{P}A_I$ 是 A_I 中一非零素理想. 据习题 1.4, 知 $\mathfrak{P}A_I = IA_I$, 故 $\mathfrak{P} = I$. 即 $\mathfrak{P}$ 为一极大理想. ♢

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 $P_i = \{(x_1, \cdots, x_n) \in A \mid x_i = 0\}$.

♣ 对素理想 $P \subseteq L_1 \times \cdots \times L_n$, 若不存在 $1 \leq i \leq n$, 使得 $\forall a \in P, \pi_i(a) = 0$(其中 π_i 为典范投影 $\pi_i : L_1 \times \cdots \times L_n \to L_i, (x_1, \cdots, x_n) \mapsto x_i$), 则 $\exists a_1, \ldots, a_n \in L_1 \times \cdots \times L_n$, 使得 $\pi_i(a_i) \neq 0$. 取 $a_i' = \pi(a_i)^{-1} \cdot (0, ..., 1(\text{第 } i \text{ 位}), ..., 0)a_i = (0, ..., 1(\text{第 } i \text{ 位}), ..., 0) \in P$, 则 $\sum_{i=1}^{n} a_i' = \mathbb{1}_{L_1 \times \cdots \times L_n} \in P$, 与 P 为真理想矛盾. 故 $\exists 1 \leq i \leq n$, 使得 $\forall a \in P, \pi_i(a) = 0$. 而对任意使得 $\pi_i(a) = 0$ 的 a, 均有 $a \cdot (0, \ldots, 1(\text{第 } i \text{ 位}), \ldots, 0) = 0 \in P$, 故由 P 素, 知 $a \in P$, 因此 $P = \{(x_1, \cdots, x_n) \in A | x_i = 0\}$. 这样的 P 自然为一素理想, 且给出了 $L_1 \times \ldots \times L_n$ 的所有素理想. ♢

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

♣ 由 $\pi_i : A \to L_i$ 保证 $\pi_i(A \backslash P_i) \subset L_i^*$, 故诱导

$$s : A_{P_i} \to L_i, \frac{a}{f} \mapsto \pi_i(a) \cdot \pi_i(f)^{-1}$$

并定义

$$r : L_i \to A_{P_i}, a \mapsto \frac{(0,\ldots,a,\ldots,0)}{(1,\ldots,1,\ldots,1)}$$

那么 $s \circ r = id|_{L_i}$. 而对 $\forall \frac{a}{f} \in A_{P_i}$, 记 $\frac{a}{f} = \frac{(a_1,\ldots,a_n)}{(f_1,\ldots,f_n)}$, 其中 $f_i \neq 0$. 则有

$$r \circ s(\frac{a}{f}) = \frac{(0,\ldots,a_i f_i^{-1},\ldots,0)}{(1,\ldots,1\ldots,1)} = \frac{(a_1,\ldots,a_I,\ldots,a_n)}{(f_1,\ldots,f_i,\ldots,f_n)} \in A_{P_i}$$

(回顾定义局部化时所引入的那个等价关系, 取 $(0,\ldots,1,\ldots,0) \in A\backslash P$ 验证), 故 $r \circ s = id|_{A_{P_i}}$, 故有同构 $A_{P_i} \simeq L_i$. ♢

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

♣ 由于 $P_i A_{P_i}$ 是 A_{P_i} 中一素理想, 而 $A_{P_i} \simeq L_i$ 为域, 故这个理想只能是 0. ♢

4. 设 $f(x) \in \mathbb{Z}[x]$ 为首一的不可约多项式, 记 $B = \frac{\mathbb{Z}[x]}{(f(x))}$. 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.

♣ $B/(p) \simeq \mathbb{F}_p[x]/(\overline{f(x)})$. 因为 $\overline{f(x)} \in \mathbb{F}_p[x]$ 在 $\mathbb{F}_p$ 上无重根, 假设 $\overline{f(x)}$ 在 $\mathbb{F}_p$ 上分解为 $\overline{f_1(x)}\cdots\overline{f_n(x)}$, 由中国剩余定理, $\mathbb{F}_p[x]/(\overline{f(x)}) = \mathbb{F}_p[x]/\prod_{i=1}^{n}(\overline{f_i(x)}) \simeq \prod_{i=1}^{n}\mathbb{F}_p[x]/(\overline{f_i(x)})$ 为有限个域的乘积 (此处 f_i 均不可约, 两两互素). 再由我们在 2022-03-14 讲义中所证明的 (局部化与商交换): $(B/(p))_{\bar{P}} \simeq B_P/(p)B_P$, 故 $(p)B_P \subset B_P$ 为极大理想, 因为由*2*可知 $(B/(p))_{\bar{P}}$ 为域. 故 $(p)B_P = PB_P$ 为 B_P 中极大理想, 且 $PB_P/(p) \subsetneq B_P/(p) \simeq (B/(p))_{\bar{P}}$, 故由*3*知 $PB_P/(p) = 0$, 因此 $PB_P = (p)$ 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.

♣ 依据习题 3 给出的方法验证即可. ♢

注: 实际上这几个环都对应了某个代数数域的代数整数环,(代数整数环: 如果 K 是 $\mathbb{Q}$ 的代数扩域, 那么 K 中所有在 Q 上整的元素的集合形成一个环, 记这个环为 K 的代数整数环 $\mathcal{O}_K$) 而所有代数整数环都是 Dedekind 整环.(可以参考 [6] 第二章)

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.

♣ 考虑 $\Phi_p(x)$ 并使用 Eisenstein 判别法. ♢

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

♣ 因为 $\Phi_p(x)$ 是 ζ_p 在 $\mathbb{Q}$ 上的极小多项式. 类似我们在讲义 2022-02-28例 1所做的那样, 可以得到这个同构. ♢

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

♣ 对 $P \subset \mathbb{Z}[\zeta_p] \simeq \mathbb{Z}[x]/(\Phi_p(x))$, 考虑整环间的单的整扩张 $\varphi\colon \mathbb{Z} \hookrightarrow \mathbb{Z}[x]/\Phi_p(x)$, 知 $P \cap \mathbb{Z} \neq 0$ (见 2022-03-14 讲义习题 2.*3.*), 不妨设 $P \cap \mathbb{Z} = (q)$.

• 若 $p \neq q$, 有 $(\overline{\Phi_p(x)}, \overline{\Phi_p(x)'}) = 1 \in \mathbb{F}_q[x]$, 记 $A = \mathbb{Z}[x]/(\Phi(x))$, 由习题 3.*4*, 可知 $PA_P = (q)$, 即 A_P 为 DVR.

• 若 $p = q$, 有 P 为 $\mathbb{Z}[x]/(\Phi(x))$ 的素理想, $P/(p)$ 为 $\mathbb{F}_p[x]/(\overline{\Phi_p(x)})$ 的素理想, 对应 $\mathbb{F}_p[x]$ 中含 $(\overline{\Phi_p(x)})$ 的素理想 P', 则 $(\bar{x} - 1)^p = (\bar{x} - 1) \cdot \overline{\Phi_p(x)} \in P'$, 故 $x - 1 \in P'$, 且 $(\bar{x} - 1)^{p-1} = \overline{\Phi_p(x)}$, 故 $P' = (\bar{x} - 1)$(因 $F_p[x]$ 为 PID). 那么 $P = (p, x - 1)$. 而由 $\Phi_p(1) = p$, 知 : $\Phi_p(x) = (x - 1) \cdot g(x) + p \in \mathbb{Z}[x]$, 故在 $\mathbb{Z}[x]/(\Phi_p(x))$ 中, 有 $x - 1 \mid p$. 这个整除关系在局部化中依然保持, 故 $P(\mathbb{Z}[x]/(\Phi_p(x)))_P = (x - 1)$. 即局部化所得环也为

DVR.

综上即知 $\mathbb{Z}[\zeta_p]$ 为 Dedekind 整环. ♢

注: 事实上 $\mathbb{Z}[\zeta_p]$ 是 $\mathbb{Q}[\zeta_p]$ 的代数整数环.

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

♣ 先证明 $\Phi_{p^n}(x) := \dfrac{x^{p^n}-1}{x^{p^{n-1}}-1}$ 不可约. 只需要对 $\Phi_{p^n}(x)$ 用 Eisenstein 判别法即可. 注意我们可以直接看 $\bmod p$ 下:

$$\overline{\Phi_{p^n}(Y+1)} = \frac{\overline{(Y+1)^{p^n}}-1}{\overline{(Y+1)^{p^{n-1}}}-1} = \frac{\bar{Y}^{p^n}+1-1}{\bar{Y}^{p^{n-1}}+1-1} = \bar{Y}^{p^n-p^{n-1}},$$

且 $\Phi_{p^n}(1) = p$. 这就足以用 Eisenstein 判别法说明 $\Phi_{p^n}(x)$ 不可约. 于是我们有 $\mathbb{Z}[\zeta_{p^n}] \simeq \mathbb{Z}[x]/(\Phi_{p^n}(x))$. 再类似*3.*中考虑该环中素理想 P 和 $\mathbb{Z}$ 的交 (q), 分 $p \neq q$ 和 $p = q$ 讨论即可. ♢

注: 事实上 $\mathbb{Z}[\zeta_{p^n}]$ 是 $\mathbb{Q}[\zeta_{p^n}]$ 的代数整数环. 更一般地, 设 N 为一正整数, 则 $\mathbb{Z}[\zeta_N]$ 是 $\mathbb{Q}[\zeta_N]$ 的代数整数环, 进而是 Dedekind 整环, 其中 $\Phi_N(x) := \prod\limits_{1\leq i\leq N,\ (i,N)=1}(x-\zeta_N^i)$, $\zeta_N = e^{\frac{2\pi i}{N}}$.(利用 Möbius 反演可以证明 $\Phi_N(x) = \prod\limits_{d|N}(x^d-1)^{\mu(\frac{N}{d})} \in \mathbb{Q}[X]$, 进而说明 $\Phi_N(x) \in \mathbb{Z}[X]$.)

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.

♣ 不妨设不存在 $(a,b) \in \mathbb{C}^2$, 使得 $f(a,b) = \dfrac{\partial f}{\partial Y}(a,b) = 0$. 像 2022-03-14 习题 3.*5*那样, 通过变量代换, 使得 f 作为 Y 的多项式是首一的. 考虑 $\dfrac{\mathbb{C}[X,Y]}{f(X,Y)}$ 的某个素理

想 P, 由于整扩张 $\mathbb{C}[x] \hookrightarrow \dfrac{\mathbb{C}[X][Y]}{f(X,Y)}$ 是整环之间的单同态, 可知 $P \cap \mathbb{C}[X]$ 是 $\mathbb{C}[X]$ 上的非零素理想 (由 $\mathbb{C}[X]$ 是 PID 知这个理想也是极大理想), 由 Hilbert 零点定理弱形式, 可将其设为 $(x-a)$, 那么 $\dfrac{\mathbb{C}[X,Y]}{f(X,Y)}/(x-a) \simeq \dfrac{\mathbb{C}[Y]}{f(a,Y)}$(2022-03-14 习题 3.*3*), 后者由于 $f(a,Y)$ 是无重根 (否则存在 $(a,b) \in \mathbb{C}^2$, 使得 $f(a,b) = \dfrac{\partial f}{\partial Y}(a,b) = 0$) 多项式而分裂为域的乘积, 再模仿本节讲义的习题 3.*4*, 可利用商与局部化交换证明 $P(\dfrac{\mathbb{C}[X,Y]}{f(X,Y)})_P$ 为 $(\dfrac{\mathbb{C}[X,Y]}{f(X,Y)})_P$ 中的极大理想, 于是 $\dfrac{\mathbb{C}[X,Y]}{f(X,Y)}$ 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 $\mathrm{Spec}_m A$ 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 $P \in \mathrm{Spec}_m A$, 设 π_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 $v_P(f+g) \geq min\{v_P(f), v_P(g)\}$.

♣ 写出 f 和 g 在 $Frac(A_P)^*$ 中用 u 和 π 表示的唯一分解即可. ♢

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

♣ 同样写出 f 的分解式即可. ♢

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.

♣ 首先有 $A\subset \cap_{P\in \mathrm{Spec}_m A}A_P$. 其次, 若 $x\in \cap_{P\in \mathrm{Spec}_m A}A_P$, 考虑理想 $P=\{a\in A\mid ax\in A\}$, 如若 $P=A$, 则 $x\in A$, 命题得证. 否则, 取包含 P 的极大理想 I, 那么 $x\in A_I$, 这说明 $\exists b\notin I$(特别地, $b\notin P$), 使得 $xb\in A$, 这与 P 的定义矛盾. ♢

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

♣ 利用*2*和*3*. ♢

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.

♣ 考虑商环 $A/(f)$, 则 $\{P\in \mathrm{Spec}_m A\mid f\in P\}$ 一一对应到 $A/(f)$ 中的素理想. 而由于 A 是 Noether 环, 知 $A/(f)$ 也是 Noether 环, 其极小素理想只有有限个 (运用 Noether 归纳法证明, 可参考讲义 2022-04-08习题 1), 对应到 A 中包含 f 且不真包含另一个包含 f 的素理想的素理想只有有限多个. 但是 A 为 Dedekind 整环, 任何素理想均极大 (否则对大的素理想作局部化后, 小的素理想会对应到局部化环中的某个非素理想), 因此 $\{P\in \mathrm{Spec}_m A\mid f\in P\}$ 中的元素不存在包含关系. 故 $\{P\in \mathrm{Spec}_m A|f\in P\}$ 中元素个数恰为 $A/(f)$ 中的极小素理想个数, 为有限个. ♢

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

♣ 记 $f=\dfrac{a}{b}\in Frac(A)^*$, 其中 $a,b\in A$, 则 $v_P(f)=v_P(a)-v_P(b)$. 而由*1.*知 $\{P\in \mathrm{Spec}_m A\mid v_P(a)\neq 0\}$ 和 $\{P\in \mathrm{Spec}_m A\mid v_P(b)\neq 0\}$ 都是有限集, 于是 $\{P\in \mathrm{Spec}_m A\mid v_P(f)\neq 0\}$ 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:

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

♣ 利用习题 7和习题 8. ♢

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

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 [6] 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 $n_P = 0 \Leftrightarrow IA_P = A_P \Leftrightarrow I \nsubseteq P$. 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 $div(IJ) = div(I) + div(J)$.

♣ 取定素理想 P, 据定义有

$$(IJ)A_P = IA_PJA_P = (\pi_P)^{n_P(I)}(\pi_P)^{n_P(J)} = (\pi_P)^{n_P(I)+n_P(J)},$$

于是 $n_P(IJ) = n_P(I) + n_P(J)$, 从而 $div(IJ) = div(I) + div(J)$. ♢

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 $f = 0$.

♣ 考虑理想 $Ann(f) := \{x \in B \mid xf = 0\}$. 若 $Ann(f) \neq B$, 取包含 $Ann(f)$ 的极大理想 P, 并作局部化 B_P, 那么 $f = 0 \in B_P$, 说明存在不属于 P, 特别地, 不属于 $Ann(f)$ 中的元素 b, 使得 $bf = 0$, 这与 $Ann(f)$ 的定义矛盾. 从而 $Ann(f) = B$, 故 $f = 0$. ♢

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 $f \in J$.

♣ 考虑理想 $I := \{x \in B \mid xf \in J\}$. 若 $I \neq B$, 取包含 I 的极大理想 P, 并作局部化 B_P, 那么 $f \in JB_P$, 说明存在不属于 P, 特别地, 不属于 I 中的元素 b, 使得 $bf \in J$, 这与 I 的定义矛盾. 故 $I = B$, 从而 $f \in J$. ♢

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 $I = J$.

♣ 对 $\forall f \in I$, 注意到2中条件满足 (因为任取 A 的素理想 (同时也是极大理想)P, 总有 $IA_P = JA_P$), 故 $f \in J$. 因此 $I \subset J$, 同理 $J \subset I$. 因此 $I = J$. ♢

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 $I = P_1^{n_1} \cdots P_k^{n_k}$.

♣ 注意到 $div(P_1^{n_1} \cdots P_k^{n_k}) = n_1P_1 + \cdots + n_kP_k = div(I)$, 则由3立知 $I = P_1^{n_1} \cdots P_k^{n_k}$. ♢

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.

♣ 条件表明 $v_P(f) \geq 0$, 由习题 7.4可知 $f \in A$, 从而 (f) 为 A 中的主理想, 由定义有 $v_P(f) = n_P((f))$, 从而 $div(I) = div((f))$, 由4即得结论. ♢

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

♣ 由4可知, 环 A 中所有理想可表为 $P_1^{n_1} \cdots P_k^{n_k}$ 的形式. 而 $Cl(A) = 0 \Leftrightarrow \varphi$(在习题 9 前定义) 是满射, 这表明对所有形如 $I = P_1^{n_1} \cdots P_k^{n_k}$ 的理想均存在 $f \in Frac(A)^*$ 使得 $div(I) = \varphi(f) = (f)$, 由5可知 $I = (f)$, 故而 A 中所有理想均为主理想. ♢

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 ψ, 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

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

证明: 该定义等价于说 $R \to A$ 为环同态, 并且 R 的像在 A 的中心里.

♣ A 是 R-模 $\Rightarrow R \to A, r \mapsto r \cdot 1 \in A$ 是环同态, 且在定义里取 $b = 1 \in A$ 即有 $ra = ar$, 因此 R 的像也就在 A 的中心里. ♢

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

♣ 任取 $0 \neq a \in A$, 考虑环同态 $\varphi\colon A \to A, x \mapsto xa$, 由 A 是整环知 $\ker\varphi$=0, 故这个有限环同态是单同态故也是满同态, 故存在 $b \in A$ 使得 $ab = 1 \in A$, 也即 $b = a^{-1}$, 故 A 是域. ♢

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.

♣ 任取 $0 \neq a \in A$, 考虑映射 $A \to A, x \mapsto ax$, 由于 A 是整环, 则这个映射是线性空间之间的单射, 而 A 为有限维线性空间, 从而该映射也是满射, 故存在 $b \in A$, 使得 $ab = 1$, 也即 $b = a^{-1}$, 从而 A 是域. ♢

2. A 中素理想均为极大理想.

♣ 考虑 A 的素理想 P, 则 A/P 是整环, 且仍是有限维 k-代数, 利用*1*可知 A/P 是域, 从而 P 是极大理想. ♢

3.A 中只有有限个素理想, 记为 $P_1, \cdots, P_n$.

♣ 由于 A 是有限维线性空间, 那么其任意理想升链都是维数严格增大的线性子空间升列, 因而有限, 故 A 是 Noether 的, 因而极小素理想有限. 但 A 的素理想都是极大的, 所以 A 的素理想都是既极大也极小的 (两两没有包含关系), 因此 A 只有有限多个素理想. ♢

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

♣$(\cap_{i=1}^n P_i)^m$ 为理想, 也是有限维 k-代数, 因而可以取定一组基. 又因为这组基都在 $(\cap_{i=1}^n P_i)^m$ 中, 因而都是幂零元, 因而 $(\cap_{i=1}^n P_i)^m$ 中任意一个元素作为这组基的一个线性组合, 其有限幂次后一定得到 0, 且这个次数只由这组基的个数和每个基各自的幂零指数有关, 因而是统一的. 将之记为 m, 即可得此结论. ♢

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

♣ 首先 $\prod_{i=1}^n P_i^m = (\prod_{i=1}^n P_i)^m \subset (\cap_{i=1}^n P_i)^m = (0)$, 其次, 因为 P_i 两两互素, 则 P_i^m 两两互素 (比如 $m = 2$ 时, 考虑互素的理想 P 和 Q, 则存在 $a \in P$ 和 $b \in Q$, 使得 $xa + yb = 1 \in A$, 其中 $x, y \in A$. 那么 $xb(a^2) + ya(b^2) = ab, x(ab) + y(b^2) = b, y(ab) + x(a^2) = a$, 写成一个式子就是 $(x^2 + 2x^2yb)a^2 + (2xy^2a + y^2)b^2 = 1$, 因此 P^2 和 Q^2 也互素. 类此可归纳说明 P^m 和 Q^m 互素, $\forall m \geq 1$.) 由中国剩余定理可得:

$$A = A/(0) \simeq A/\prod_{i=1}^n P_i^m \simeq \prod_{i=1}^n A/P_i^m.$$

而 A/P_i^m 是局部环, 等价于说 A 中包含 P_i^m 的极大理想只有一个. 而由先前讨论不难看出, P_i^m 与 P_j^n 在 $i \neq j$, $m, n \in N^*$ 时互素, 故包含 P_i^m 的素理想只有 P_i, 特别地, 包含 P_i^m 的极大理想也只有 P_i, 故 A/P_i^m 是局部环, 唯一极大理想是 P_i/P_i^m. ♢

6. $A \simeq \prod_{i=1}^{n} A_{P_i}$.

♣ 我们首先证明 $A_{P_i} \simeq A/P_i^m$. 由*5*可知 A/P_i^m 为局部环, 因此在其极大理想 P_i/P_i^m 处作局部化得到的环还是 A/P_i^m(因为所有不在 P_i/P_i^m 中的元素都可逆). 由商与局部化交换可知, $A/P_i^m = (A/P_i^m)_{P/P_i^m} \simeq A_{P_i}/(P_i^m A_{P_i})$, 但由于 $\prod_{i=1}^{n} P_i^m = 0$, 且对 $j \neq i$, 总有 $P_j^m \nsubseteq P_i$, 所以对 $P_i^m A_{P_i}$ 中的元素 $\frac{a}{s}$, 总可找到 $A\backslash P_i$ 中 (因为 P_i 为素理想) 的元素 b, 使 $ab = 0$(具体而言, a 一定可以写成 $\sum_{k=1}^{t} a_k s_k$ 的形式, 其中 $a_k \in P_i^m, s_k \in A\backslash P_i$. 由于 $\prod_{i=1}^{n} P_i^m = 0$, 我们总可取 $0 \neq b_j \in P_j^m \backslash P_i, 1 \leq j \leq n, j \neq i$. 记 $b = \prod_{1 \leq j \leq n, j \neq i}^{n}$, 则因为 P_i 是素理想, 仍有 $b \notin P_i$. 对 $\forall 1 \leq k \leq t$, 有 $ba_k = 0 \in A$, 故 $ba = 0$), 故 $\frac{a}{s} = \frac{0}{1} \in A_{P_i}$, 则 $A_{P_i}/(P_i^m A_{P_i}) \simeq A_{P_i}$. 故 $A_{P_i} \simeq A/P_i^m$, 再由*5*可知 $A \simeq \prod_{i=1}^{n} A/P_i^m \simeq \prod_{i=1}^{n} A_{P_i}$. ♢

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.

♣ 若 A 中没有非零的幂零元, 说明 $(\cap_{i=1}^{n} P_i)^m = (0)$, 即*4*中可取 $m = 1$, 由*5*立知 $A \simeq \prod_{i=1}^{n} A/P_i$, 而 P_i 为极大理想, 故 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.

♣ 仿照讲义 2022-03-02,03-07例 2分析即可.

结论: (2) 上方只有一个素理想, 为理想 $(2, \sqrt{3})$. (3) 上方只有一个素理想, 为主理想 $(\sqrt{3})$. 当素数 $q \notin \{2, 3\}$ 时, 若 $(\frac{3}{q}) = 1$, 则 (q) 上方有两个素理想, 分别是 $(q, \sqrt{3} - a)$ 和 $(q, \sqrt{3} + a)$, 其中 $a^2 \equiv d \mod q$. 若 $(\frac{3}{q}) = -1$, 则 (q) 上方只有一个素理想 (q). ♢

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:

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

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

♣ 见 2022-03-09习题 5. ♢

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, $\varphi\colon A \to A_S$ 为自然同态.

1. 证明:A_S 为 Noether 环.

♣ 见 2022-03-09 习题 4.*4*. ♢

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

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

♣ 不妨设 $y = \dfrac{a}{s} \in A_S$, 其中 $a \in A, s \in S$. 考虑 $\varphi^{-1}(J)$ 和 $Ann(a)$. 首先, 如若 $\varphi^{-1}(J) \nsubseteq Ann(a)$, 则 $\exists x \in \varphi^{-1}(J)$, 使得 $xa \neq 0$. 但 $\varphi(x) \cdot y = \dfrac{xa}{s} = 0$, 于是存在 $s_1 \in S$, 使得 $s_1 xa = 0$. 故 $Ann(a) \subsetneq Ann(s_1 a)$. 再接着比较 $\varphi^{-1}(J)$ 与 $Ann(s_1 a)$, 如若仍有 $\varphi^{-1}(J) \nsubseteq Ann(s_1 a)$, 我们可以类似地找到 s_2, 使得 $Ann(s_1 a) \subsetneq Ann(s_1 s_2 a)$. 但由于 A 是 Noether 的, 这个过程必在有限步后终止 (否则会得到一条理想的严格

升链), 故我们可以取出 $s' \in S$, 使得 $\varphi^{-1}(J) \subseteq Ann(s'a)$. 而 $\forall t \in Ann(s'a)$, 总有 $\varphi(t) \cdot y = \dfrac{t}{1} \cdot \dfrac{a}{s} = \dfrac{at}{s} = 0$, 因为 $s'at = 0$. 故 $Ann(s'a) \subseteq \varphi^{-1}(J)$. 取 $x = s'a$, 即证得此命题. ♢

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

♣ 见 2022-03-14 习题 2.*1*. ♢

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 $f(x) \in m$.

♣ 首先存在次数大于零的多项式 $f(x) \in m$. 若否, 则 $m = m \cap \mathbb{Z}$ 为 $\mathbb{Z}$ 的一个素理想, 记为 (p), 则 $m \subsetneq (p, x) \subsetneq \mathbb{Z}[x]$, 与 m 是极大理想矛盾. 再取 f 的一个正次数不可约因式即可. 特别地, 我们在这里将 f 取为 m 中次数最小的不可约多项式. ♢

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.

♣ 由于 $\mathbb{Z}$ 是整环, 因此 $\mathbb{Z}_n$ 也是整环. 而 $f(x)$ 为 $\mathbb{Z}[x]$ 中不可约多项式, 则亦为 $\mathbb{Z}_n[x]$ 中的不可约多项式 (否则 $f(x)$ 是 $\mathbb{Q}[x]$ 中的可约多项式, 矛盾)(具体而言, 记 $f(x) = g(x)p(x)$, 其中 $g(x), p(x) \in \mathbb{Q}[x]$, 将右侧整系数化有 $rsf(x) = (rg(x))(sp(x))$, 考虑浓度立得 $rsc_f = rs = 1$(因为 f 本原), 故 $g(x), p(x) \in \mathbb{Z}[x]$, 与 $f(x)$ 是 $\mathbb{Z}[x]$ 中不可约多项式矛盾) 故 $\mathbb{Z}_n[x]/(f(x))$ 也是整环. 而 $f(x)$ 首项系数为 n, 故 $f(x)$ 是 $\mathbb{Z}_n[x]$ 中的首一多项式, 因此 $\mathbb{Z}_n \to \mathbb{Z}_n[x]/(f(x))$ 是整扩张. 将系数扩至 $\mathbb{Q}$ 上, 则此时 ker 为 $f(x)\mathbb{Q}(x)$, 与 $\mathbb{Z}_n[x]$ 的交就是 $f(x)\mathbb{Z}_n[x]$(因为 $f(x)$ 本原). 故整扩张 $\mathbb{Z}_n \to \mathbb{Z}_n[x]/(f(x))$ 为整环之间的单同态. ♢

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

♣ 由*2*知 $m \cap \mathbb{Z}$ 为 $\mathbb{Z}$ 的素理想 (2022-03-14 习题 2), 故存在素数 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 $m = (p, g(x))$.

♣ 考察如下交换图.

$$\begin{array}{ccccc} \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n[x] & \longrightarrow & \dfrac{\mathbb{Z}_n[x]}{(f(x))} \\ \uparrow & & & & \downarrow \simeq \\ \mathbb{Z} & \longrightarrow & \dfrac{\mathbb{Z}[x]}{(f(x))} & \longrightarrow & (\dfrac{\mathbb{Z}[x]}{(f(x))})_n \end{array}$$

在商同态 $\mathbb{Z} \to \mathbb{Z}[x]/(f(x))$ 下, m 对应到 $\mathbb{Z}[x]/(f(x))$ 中的一个极大理想 g(因为 $f(x) \in m$). 考虑 $m/(p) \subset \mathbb{Z}[x]/(p) \simeq \mathbb{F}_p[x]$, $m/(p)$ 对应到 $g/(p)$, 对应到 $\mathbb{Z}[x]/(f(x), p)$ 的一个极大理想, 对应到 $\dfrac{\mathbb{F}_p[x]}{(f(x))}$ 中的一个极大理想 P, 那么 P 作为 $\mathbb{F}_p[x]$ 中的素理想, 且 $n \notin P$(因为 $n \notin m$, 否则 $f(x) - nx^{\deg f} \in m$, 如若 $\deg f = 1$, 则由于 $1 \notin m$, 一定有 $m \subsetneq (x, q)$, 其中 q 是 $f(x) - nx$ 的极小素因子. 如若 $\deg f \geq 2$, 则 $f(x) - nx^{\deg f} \in m$, 与我们在 *1* 中所要求的 f 次数最小性矛盾.) 通过局部化 $\dfrac{\mathbb{Z}[x]}{(f(x))} \to \left(\dfrac{\mathbb{Z}[x]}{(f(x))}\right)_n$ 对应到 $\left(\dfrac{\mathbb{Z}[x]}{(f(x))}\right)_n$ 中的素理想 $P\left(\dfrac{\mathbb{F}_p[x]}{(f(x))}\right)_n$, 再通过局部化与商交换, 对应到 $\dfrac{(\mathbb{F}_p)_n[x]}{(f(x))}$ 中的某个素理想. 但是 $p \nmid n$(否则 $n \in m$), 故 $(\mathbb{F}_p)_n = \mathbb{F}_p$, 即对应到 $\dfrac{(\mathbb{F}_p)[x]}{(f(x))}$ 中的某个素理想, 再通过商同态 $\mathbb{F}_p[x] \to \dfrac{(\mathbb{F}_p)[x]}{(f(x))}$ 对应到 $\mathbb{F}_p[x]$ 中含有 $\overline{f(x)}$ 的一个素理想, 由于 $\mathbb{F}_p[x]$ 是主理想整环, 这个素理想同时也是一个极大理想, 即为 $(\overline{g(x)})$, 其中 $\overline{g(x)}$ 是 $\overline{f(x)}$ 在 $\mathbb{F}_p[x]$ 中的某个不可约因式. 逐步对应回去, 即有 $m = (p, g(x))$. ♢

习题 **9.** 举出一个 UFD 但不是 PID 的例子.

♣ $\mathbb{Z}[x]$ 为 UFD, 但 $(2) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$. ♢

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.

♣ 设 A 中一组素元为 $p_1, \cdots, p_n$, 则对 $x \in K$, 且 x 在 A 上整, 有 $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, 其中 $a_i \in A, 1 \leq i \leq n-1$. 记 $x = up_1^{s_1} \cdots p_n^{s_n}$, 如果存在 $s_j < 0$, 那么在等式两侧同乘 $p_j^{ns_j}$ 后立得矛盾. 故 $s_i \geq 0, 1 \leq i \leq n-1$, 即 $x \in A$. 故 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.

♣ 见讲义 2022-03-16 习题 7.*3*. ♢

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

♣ 注意 $Frac(A_P) = Frac(A) = K$, 且整闭这一性质在取环的交时仍保持, 因此 $A = \cap_{P \in \mathrm{Spec}A} A_P$ 为整闭的, 因此 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.

♣ 见讲义 2022-03-16习题 5. ♢

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.

♣ 考虑环同态 $\varphi\colon \mathbb{Z}[x_0, \cdots .x_{n-1}][x] \to \mathbb{Z}[t][x], x_i \mapsto t, 1 \leq i \leq n-1, x \mapsto x$. 那么 $\varphi(f(x)) = g(x) = x^n + tx^{n-1} + \cdots + tx + t \in \mathbb{Z}[t][x]$. 由于 $\mathbb{Z}[t][x]$ 为 UFD, 且 t 为其上不可约元, 则由 Eisenstein 判别法可知 $g(x)$ 不可约, 因此 $f(x)$ 不可约 (因为 $\deg g = \deg f$). ♢

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 $\mathbb{Z}_{(p)} := \{\frac{a}{b} \mid a \in \mathbb{Z}, p \nmid b\}$(即 $\mathbb{Z}_{(p)}$ 为 $\mathbb{Z}$ 在素理想 (p) 处的局部化) 均为离散赋值环.

♣ $\mathbb{Z}_p$ 的唯一极大理想是 (p), 所有真理想均形如 (p^n), $n \in N^*$, 故任意理想升链稳定, 因此 $\mathbb{Z}_p$ 是 Noether 的, 因而是 DVR. $\mathbb{C}[[x]]$ 的唯一极大理想是 (x), 所有真理想均形如 (x^n), $n \in N^*$, 故任意理想升链稳定, 因此 $\mathbb{C}[[x]]$ 是 Noether 的, 因而是 DVR. $\mathbb{Z}_{(p)}$ 的唯一极大理想是 $(\frac{p}{1})$, 所有真理想均形如 $(\frac{p^n}{1}), n \in N^*$, 故任意理想升链稳定, 因此 $\mathbb{Z}_{(p)}$ 是 DVR. ♢

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.

♣ 见讲义 2022-03-16习题 1. ♢

2022-03-21 代数不变量理论

设 G 为群, ρ: $G \to GL(V)$ 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, ρ: $G \to GL(V)$ 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.

♣ 令 $(e_1, \cdots, e_n)$ 为 V 的一组基, 并令 $(e_1^*, \cdots, e_n^*)$ 为 V^* 中相应的对偶基, 则 e_i^* 本身为多项式函数. 令 φ: $\mathbb{C}[x_1, \cdots, x_n] \to \mathbb{C}[V]$, $x_i \mapsto e_i^*$. 则由定义 $\forall f \in \mathbb{C}[V]$, f 为 $e_1^*, \cdots, e_n^*$ 的多项式组合, 故 $f \in \mathrm{Im}\varphi$. 此时多项式 $P(x_1, \cdots, x_n)$ 在 $a_1e_1 + \cdots, +a_ne_n$ 处的取值为 $P(e_1^*, \cdots, e_n^*)(a_1e_1 + \cdots, a_ne_n) = P(a_1, \cdots, a_n)$, 故 $\varphi P = 0 \Rightarrow P = 0$, 即 $\ker \varphi = 0$, 故给出同构. 我们利用该同构和前面给出的 G 在 $\mathbb{C}[V]$ 上的作用即给出 G 在多项式环 $\mathbb{C}[x_1, \cdots, x_n]$ 上的作用. $\mathbb{C}[x_1, \cdots, x_n]$ 为分次代数, 由于 G 线性作用于上面, 我们只需验证 G 稳定每一个分次. 令 $P(x_1, \cdots, x_n)$ 为一 m 次齐次多项式, $f = \varphi(P)$, 则 $(g \cdot f)(a_1e_1 + \cdots a_ne_n) = f((e_1, \cdots, e_n)\rho(g^{-1})(a_1, \cdots, a_n)^T) = f(\sum \rho_{ij}(g^{-1})a_je_i) = P\left(\sum_{j=1}^{n} \rho_{1j}(g^{-1})a_j, \cdots, \sum_{j=1}^{n} \rho_{nj}(g^{-1})a_j\right)$ 仍为 $(a_1, \cdots, a_n)$ 的 m 次齐次多项式, 即证. ♢

注: 此处 $g \in G$ 在 $\mathbb{C}[V]$ 上的作用只由 $g \cdot e_1^*, \cdots, g \cdot e_n^*$ 决定, 是一个 $\mathbb{C}$-代数同构,

即我们应该有 $(g\cdot h_1)(g\cdot h_2)=g\cdot(h_1h_2)$. 事实上, 上面的计算已经给出

$$g\cdot\varphi(P)=P\left(\sum_{j=1}^{n}\rho_{1j}(g^{-1})e_j^*,\cdots,\sum_{j=1}^{n}\rho_{nj}(g^{-1})e_j^*\right)=P(g\cdot e_1^*,\cdots,g\cdot e_n^*),$$

也即

$$g\cdot P=P(g\cdot x_1,\cdots,g\cdot x_n).$$

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 $I=(f_1,\ldots,f_k)$.

♣ 由 Hilbert 基定理, 知 $\mathbb{C}[x_1,\ldots,x_n]$ 是 Noether 的, 因此 I 是有限生成的. 记 $I=(h_1,\ldots,h_m)$. 我们令 $\tilde{h}_i=\dfrac{1}{|G|}\sum\limits_{g\in G}g\cdot h_i$, 则对任意 G-不变正次数齐次多项式 f, 由于 $f\in I$, 存在 $g_1,\cdots g_m\in\mathbb{C}[x_1,\cdots,x_n]$ 使得 $f=g_1h_1+\cdots+g_mh_m$. 注意 I 是由正次数齐次多项式生成的, 故 h_i 无常数项, 因而 $\tilde{h}_i\in I$. 我们有 $f=\dfrac{1}{|G|}\sum\limits_{g\in G}g\cdot f=\dfrac{1}{|G|}\sum\limits_{g\in G}g\cdot(g_1h_1+\cdots+g_mh_m)=g_1\dfrac{1}{|G|}\sum\limits_{g\in G}g\cdot h_1+\cdots+g_m\dfrac{1}{|G|}\sum\limits_{g\in G}g\cdot h_m=g_1\tilde{h}_1+\cdots+g_m\tilde{h}_m$. 故 $\tilde{h}_i$ 生成所有 G-不变正齐次多项式, 进而也生成 I, 故可直接假定每个 h_i 是 G-不变的. 若 h_1 不是齐次的, 则可以将 h_1 根据次数分为 $\mathbb{C}[x_1,\ldots,x_n]^G$ 中的有限个齐次元素, 用这些齐次元素替代 h_i, 仍可保持生成元个数有限. 因此 I 可以由 $\mathbb{C}[x_1,\ldots,x_n]^G$ 中的有限个正次数齐次多项式生成, 即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:$f=g_1f_1+\cdots+g_kf_k$.

♣ 由 $f\in I$, 可知存在 $h_1,\ldots,h_k\in\mathbb{C}[x_1,\ldots,x_n]$, 使得 $f=h_1f_1+\ldots+h_kf_k$. 设 $\deg f=d,\deg f_i=d_i$. 由于 G 的作用保持次数, 只需取 g_i 为 h_i 中次数为 $d-d_i$ 的项

即可 (左边为 d 次齐次多项式, 右边次数不为 d 的项求和只能为 0). 因此存在齐次多项式 $g_1,\ldots,g_k$ 使得:$f=g_1f_1+\cdots+g_kf_k$. ♢

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:$f=g_1f_1+\cdots+g_kf_k$.

♣ 由于 G 是有限群, 故令 $\dfrac{1}{|G|}\sum\limits_{g\in G}g\cdot g_i$ 为新的 g_i, 即有 $g_i\in\mathbb{C}[x_1,\ldots,x_n]^G$, 且仍为齐次多项式 ($G$ 的作用保持次数). 则 $f=g_1f_1+\cdots+g_kf_k$(相当于把*3*中的式子用 G 中全体元素作用后再取平均). ♢

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.

♣ 注意到*4*中所得到的齐次多项式 $g_1\in\mathbb{C}[x_1,\ldots,x_n]^G$, 如果 $\deg g_1>0$, 则 $g_1\in I$, 故 g_1 可以被 $f_1,\ldots,f_k$ 如*4*中那样表示. 由于 $\deg f_i>0$, 这样得到的表示中 f_i 的“系数多项式”相较于 g_1 一定是严格减的. 故对这些系数继续进行这样的表示, 则此操作一定在有限步后终止, 因而 g_1 可以被 $f_1,\ldots,f_k$ $\mathbb{C}$-有限生成. 故 $f=g_1f_1+\ldots+g_kf_k$ 也可以被 $f_1,\ldots,f_k$ $\mathbb{C}$-有限生成, 进而 $\mathbb{C}[x_1,\ldots,x_n]^G$ 中所有正次数齐次多项式都可以被 $f_1,\ldots,f_k$ $\mathbb{C}$-有限生成, 这给出 $\mathbb{C}[x_1,\ldots,x_n]^G$ 可以被 $f_1,\ldots,f_k$ $\mathbb{C}$-有限生成, 也即 $\mathbb{C}[x_1,\ldots,x_n]^G$ 为有限生成 $\mathbb{C}$-代数. 通过我们在*1*中建立的同构, 可知 $\mathbb{C}[V]^G$ 也为有限生成 $\mathbb{C}$-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 σ_i 为 $x_1,\ldots,x_n$ 的 i 次初等对称多项式.

♣ 由前一题 *1* 的注记, 我们有 $\sigma\cdot e_i^*(a_1e_1+\cdots+a_ne_n)=e_i^*(a_1e_{\sigma^{-1}(1)}+\cdots+$

$a_n e_{\sigma^{-1}(n)}) = e_i^*(a_{\sigma(1)}e_1 + \cdots + a_{\sigma(n)}e_n) = a_{\sigma(i)} = e_{\sigma(i)}^*(a_1e_1 + \cdots + a_ne_n)$. 进而诱导的 $\mathfrak{S}_n$ 在 $\mathbb{C}[x_1, \cdots, x_n]$ 上的作用为 $\sigma \cdot x_i = x_{\sigma(i)}$. 由对称多项式基本定理 (见 2022-05-23习题 6和习题 7), $\mathbb{C}[V]^{\mathfrak{S}_n} \simeq \mathbb{C}[x_1, \cdots, x_n]^{\mathfrak{S}_n} = \mathbb{C}[\sigma_1, \cdots, \sigma_n]$, 即证结论. ♢

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 $\det(\lambda I_n - A) = \lambda^n - \sigma_1(A)\lambda^{n-1} + \cdots + (-1)^n\sigma_n(A)$.

♣ 由于 $\det(\lambda I_n - A) = \det(P^{-1}(\lambda I_n - A)P) = \det(\lambda I_n - P^{-1}AP)$, 即相似作用不改变特征多项式, 故 $\sigma_i \in \mathbb{C}[M_n(\mathbb{C})]^{GL_n(\mathbb{C})}$. 令一方面, 若 $f \in \mathbb{C}[M_n(\mathbb{C})]^{GL_n(\mathbb{C})}$, 对任意 $A \in M_n(\mathbb{C})$, 考虑 A 的 Jordan 标准型 $J_A = P^{-1}AP$, 则 $f(A) = f(J_A)$, 而 J_A 的矩阵元只有 A 的特征值和 $1, 0$. 记 A 的 n 个特征值 (计重数) 为 $\lambda_1, \cdots, \lambda_n$, 则 $f(A)$ 是这 n 个特征值的多项式函数. 若 J_A 为对角阵, 则置换对角元前后互相相似, 故 f 限制在可对角化矩阵上, 看作 n 个特征值的对称多项式, 进而由对称多项式基本定理,$f|_{diag} \in \mathbb{C}[\sigma_1, \cdots, \sigma_n]$. 另一方面, $f : M_n(\mathbb{C}) \to \mathbb{C}$ 为多项式函数, 故作为 $\mathbb{C}^{n^2} \to \mathbb{C}$ 的函数是连续的, 而可对角化矩阵在 $M_n(\mathbb{C})$ 中稠密, 故在可对角化矩阵上的像将唯一决定 f, 从而 $f \in \mathbb{C}[\sigma_1, \cdots, \sigma_n]$. 于是给出反包含关系. ♢

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.

♣ 包含关系 $\mathbb{C}[M_n(\mathbb{C})]^{SL_n(\mathbb{C})} \supseteq \mathbb{C}[\det]$ 是易见的. 若 $A \in GL_n(\mathbb{C})$, 考虑 $J = \mathrm{diag}(1, \cdots, 1, \det A)$, 则 $JA^{-1} \in SL_n(\mathbb{C})$, 故 J 与 A 在 $SL_n(\mathbb{C})$ 作用的同一轨道上, 于是任意的 $f \in \mathbb{C}[M_n(\mathbb{C})]^{SL_n(\mathbb{C})}$, 将 f 限制在 $GL_n(\mathbb{C})$ 上 f 是 $\det$ 的多项式, 不妨假设 $f(A) = F(\det A)$, $\forall A \in GL_n(\mathbb{C})$, 其中 $F \in \mathbb{C}[X]$. 对于一般的 A, 考虑 $f(A) - F(\det A)$

是关于 A 的矩阵元的多项式, 且限制在 $GL_n(\mathbb{C})$ 上为 0. 将 $M_n(\mathbb{C})$ 等同到 $\mathbb{C}^{n^2}$ 并赋予相应拓扑, 则 $GL_n(\mathbb{C})$ 为 $\det M \neq 0$ 所确定的集合, 为开集. 故其中包含一个形如 $U_1 \times \cdots \times U_{n^2}$ 的子集, 其中 U_i 为 $\mathbb{C}$ 中的开球. 事实上, 若一个 n 元多项式在一个 $\mathbb{C}^n$ 的形如 $U_1 \times \cdots \times U_n$ 上的子集取值为 0, 其中每个 U_i 为无穷集, 则该多项式为 0. 可直接归纳证明: 对 $n = 1$ 时结论自然成立, 假设对 $n-1$ 维成立, 对于 $h \in \mathbb{C}[X_1, \cdots, X_n]$ 满足以上条件, 将 h 按 X_n 降幂排列, 并看作 $\mathbb{C}[X_1, \cdots, X_{n-1}][X_n]$ 中元素, 则 $\forall a \in U_1 \times \cdots \times U_{n-1}, b \in U_n$ 有 $h(a, b) = 0$, 这说明 $h(a, X_n)$ 有无穷多个零点, 故 $h(a, X_n) = 0$, 进而每个 X_n^k 的系数 $c_k(X_1, \cdots, X_{n-1})$ 在 $U_1 \times \cdots \times U_{n-1}$ 上为 0, 从而由归纳假设, $h = 0$. 于是 $f = F(\det)$, 这说明反向的包含关系. ♢

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

♣ $SL_2(\mathbb{C})$ 在 2×4 矩阵上的左乘作用为分别作用在各列上, 即 $P(A_1\ A_2\ A_3\ A_4) = (PA_1\ PA_2\ PA_3\ PA_4)$, $A_i \in M_{2\times 1}(\mathbb{C})$. 记 $\det(A_i\ A_j) = \det_{ij}$, 则首先有对任意 $S \in SL_2(\mathbb{C})$, $\det_{ij}(S(A_1\ A_2\ A_3\ A_4)) = \det(S(A_i\ A_j))$, 故 $\mathbb{C}[\det_{ij}, i < j] \subseteq \mathbb{C}[M_{2\times 4}(\mathbb{C})]^{SL_2(\mathbb{C})}$. 令一方面, 假定 $A = (A_1\ A_2)$, $B = (A_3\ A_4)$, 且 A 为可逆方阵, 则 $(A\ B)$ 可被作用到 $(\mathrm{diag}(1\ \det A))(I_2\ A^{-1}B)$, 而若 $A^{-1}B = (X_1\ X_2)$, 则它们分别是方程 $AX_1 = A_3$ 和 $AX_2 = A_4$ 的解. 由 Cramer 法则, 可知 $X_1 = (\dfrac{\det(A_3\ A_2)}{\det A}\ \dfrac{\det(A_1\ A_3)}{\det A})^T$, $X_2 = (\dfrac{\det(A_4\ A_2)}{\det A}\ \dfrac{\det(A_1\ A_4)}{\det A})^T$, 进而得到

$$(\mathrm{diag}(1\ \det A))(I_2\ A^{-1}B) = \begin{pmatrix} 1 & & -\dfrac{\det_{23}}{\det_{12}} & \dfrac{\det_{13}}{\det_{12}} \\ & \det_{12} & -\det_{24} & \det_{14} \end{pmatrix}.$$

这说明 $\mathbb{C}[M_{2\times 4}(\mathbb{C})]^{SL_2(\mathbb{C})}$ 中的元素限制在 $GL_2(\mathbb{C}) \times M_2(\mathbb{C})$ 上是这些 $\det_{ij}$ 的多项式,

而这是 $\mathbb{C}^8$ 的开集, 同上一题论述可知 $\mathbb{C}[M_{2\times 4}(\mathbb{C})]^{SL_2(\mathbb{C})} \subseteq \mathbb{C}[\det_{ij}, 1 \leq i < j \leq 4]$. $\diamondsuit$

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 Δ 为判别式函数 : $\forall f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$, $\Delta(f) = b^2 - 4ac$.

$\clubsuit$ 令 $F \in \mathbb{C}[Pol_{2,2}]^{SL_2(\mathbb{C})}$. 按定义 $\forall A \in SL_2(\mathbb{C})$, $(A \cdot F)(f(x_1, x_2)) = F((A^{-1} \cdot f(x_1, x_2))) = F(f((x_1, x_2)A^{-1}))$. 考虑 $Pol_{2,2}$ 中的非零元, 先假设 $a \neq 0$, 则存在 $\lambda_1, \lambda_2 \in \mathbb{C}$ 为 $at^2 + bt + c = 0$ 的两根, 且 $ax_1^2 + bx_1x_2 + cx_2^2 = a(x_1 - \lambda_1 x_2)(x_1 - \lambda_2 x_2)$. 先做换元 $x_1 \mapsto y_1 = x_1 + \lambda_1 x_2$, $x_2 \mapsto y_2 = x_2$, 则得到 $ax_1(x_1 + (\lambda_1 - \lambda_2)x_2)$. 考虑 $b^2 - 4ac \neq 0$, 于是此时 $\lambda_1 \neq \lambda_2$. 再做换元 $x_1 \mapsto x_1$, $x_2 \mapsto x_2 - \dfrac{1}{\lambda_1 - \lambda_2} x_1$, 于是得到 $a(\lambda_1 - \lambda_2)x_1x_2$. 将 $Pol_{2,2}$ 等同到 $\mathbb{C}^3$, 令 U 为由 $a \neq 0$ 和 $b^2 - 4ac \neq 0$ 确定的开集, 则 F 在 U 上是 $a(\lambda_1 - \lambda_2)$ 的多项式. 而 $a^2(\lambda_1 - \lambda_2)^2 = b^2 - 4ac$, 进而 F 作为 a, b, c 的多项式只能是 $b^2 - 4ac$ 的多项式. 同样仿照习题 4的论证可延拓到整个 $Pol_{2,2}$ 上. 另一方面, 易验证 $\delta \in \mathbb{C}[Pol_{2,2}]^{SL_2(\mathbb{C})}$, 故 $\mathbb{C}[Pol_{2,2}]^{SL_2(\mathbb{C})} = \mathbb{C}[\Delta]$. $\diamondsuit$

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.

♣ 对 $\Phi_p(x+1)$ 用 Eisenstein 判别. ♢

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.

♣ 见讲义 2022-03-16 习题 3.*4*. ♢

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.

♣ 将 f 视作 $\mathbb{Z}[t][x]$ 中的多项式, 则由 $\mathbb{Z}[t]$ 是 UFD, t 是 $\mathbb{Z}[t]$ 中的不可约元, 对 f 用 Eisenstein 判别可知 f 在 $\mathbb{Z}[t][x]$ 中不可约, 即在 $\mathbb{Z}[t,x]$ 中不可约. ♢

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.

♣ 见口试第一轮题目 习题 13. ♢

• 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 $fg_1 = gf_1$.

♣ $\Rightarrow$: 如果 $pgcd(f,g) = d, \deg d > 0$, 则 $f = df_1, g = dg_1$, 满足 $\deg f_1 \leq n-1, \deg g_1 \leq m-1$, 并且 $fg_1 = gf_1$. $\Leftarrow$: 如果 $pgcdf, g = d, \deg d = 0$, 那么 $fg_1 = gf_1 \Rightarrow f|pgcd(f,g)f_1$, 比较次数即得矛盾. ♢

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 $\mathrm{Res}(f,g) := \det M$.

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

♣ 由于 A 是 UFD, 考虑 $K:=Frac(A)$, 将 M 看作 $M_{m+n}(K)$ 中元素.$\Rightarrow$: 如果 f,g 在 $A[x]$ 中存在次数大于零的公因子, 那么由习题 3知存在 $f_1,g_1\in A[x]$, 满足 $\deg f_1\leq n-1,\deg g_1\leq m-1$, 且 $fg_1-gf_1=0$. 故 $\ker(M)\neq 0$, 因此 $\mathrm{Res}(f,g)=\det M=0$. $\Leftarrow$: 如若 $\mathrm{Res}(f,g)=0$, 则 $\ker(M)\neq 0$, 故可取出向量 $0\neq v\in K^{m+n}$, 且 $M\cdot v=0$. 由于 $K=Frac(A)$, 自然可以将 v 乘以某 A 中元素 s, 使得 $0\neq sv\in\ker(M)$, 将 sv 对应到 f_1,g_1 的 $m+n$ 个系数, 即得 $f_1,g_1\in A[x]$, 且 $\deg f_1\leq n-1,\deg g_1\leq m-1$, 并有 $fg_1=gf_1$. 由习题 3知 f 和 g 在 $A[x]$ 中存在次数大于零的公因子. ♢

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

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

♣ 取 Q^* 为 Q 的伴随矩阵, 即 $QQ^*=\det Q\cdot I_n$. 取 $(x_1,\cdots,x_n)^t=Q^*(1,0\cdots,0)^t$, 即有 $Q\cdot(x_1,\cdots,x_n)^t=Q\cdot Q^*(1,0\cdots,0)^t=\det Q\cdot(1,0\cdots,0)^t=(\det Q,0\cdots,0)^t$. ♢

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 $fg_1-gf_1=\mathrm{Res}(f,g)$.

♣ 在*1*中取 $Q=M$, 得到 $x_1,\cdots,x_n\in A$, x_1 令 $f1=\sum_{i=0}^{n-1}-x_{n+i}x^i$, $g_1=\sum_{j=0}^{m-1}x_jx^j$, 即有 $fg_1-gf_1=\mathrm{Res}(f,g)$. ♢

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

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

♣ 记对角阵 $T=diag(1,t,\ldots,t^{m+n-1})$, 那么 $T\cdot M$ 的每一列均 "齐次"(第一列关于 t 的次数不超过 n, 第二列关于 t 的次数不超过 $n+1,\ldots$, 第 m 列关于 t 的次数不超过 $m+n-1$, 第 $m+1$ 列关于 t 的次数不超过 m, 第 $m+2$ 列关于 t 的次数不超过 $m+1,\ldots$, 第 $m+n$ 列关于 t 的次数不超过 $m+n-1$), 因此 $\deg\det(TM)\leq(n++\ldots+m+n-1+m+\ldots+m+n-1)=2mn+\dfrac{m(m-1)+n(n-1)}{2}$, 而 $\deg\det(T)=(1+2+\ldots+m+n-1)=\dfrac{(m+n-1)(m+n)}{2}$. 因此 $\deg\det(M)=\deg\det(TM)-\deg\det(T)\leq 2mn+\dfrac{m(m-1)+n(n-1)-(m+n-1)(m+n)}{2}=mn$. 这便完成了证明. ♢

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

$$\mathrm{Res}(f,g)=ha_n^mb_m^n\prod_{i=1}^{n}\prod_{j=1}^{m}(y_j-x_i)^{m_{ij}}$$

♣ 首先 $\mathrm{Res}(f,g)\in B$, 注意到 $x_i=y_j$ 时, 有 $\mathrm{Res}(f,g)=0$, 故 $(y_j-x_i)\mid\mathrm{Res}(f,g)$. 另一方面, 由于 $f(x)=a_n\prod_{i=1}^{n}(x-x_i), g(x)=b_m\prod_{j=1}^{m}(x-y_j)\in B[x]$, 观察 f 和 g 对应习题 3中定义的矩阵 M 的系数, 可知 $\det M$ 恰被 $a_n^mb_m^n$ 整除. 因此 $\mathrm{Res}(f,g)$ 可以写成

$ha_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(y_j - x_i)^{m_{ij}}$ 的形式, 其中 $h \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$, $m_{ij} \geq 1$. ♢

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 $\mathrm{Res}(f_t, g_t)$ 作为 t 的多项式的次数 $\deg \mathrm{Res}(f_t, g_t) \leq mn$.

♣ 此时若记 $f_t(x) = \sum_{i=0}^{n} a_i(t)x^i, g_t(x) = \sum_{j=0}^{m} b_j(t)x^j$, 那么 $a_0(t), \ldots, a_n(t), b_0(t), \ldots, b_m(t) \in B[t]$ 且 $\deg a_i(t) \leq n - i, \deg b_j(t) \leq m - j, \forall 0 \leq i \leq n, 0 \leq j \leq m$. 由习题 6可知, 作为 t 的多项式, $\deg \mathrm{Res}(f_t, g_t) \leq mn$. ♢

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

♣ 考虑 $\mathrm{Res}(f_t, g_t) = ha_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(ty_j - tx_i)^{m_{ij}}$, 其中 m_{ij} 和 h 与*1*中相同. 故 $\deg \mathrm{Res}(f_t, g_t) = \sum_{i=1}^{n}\sum_{j=1}^{m} m_{ij} + \deg h \geq mn$. 由*2*知 $\deg \mathrm{Res}(f_t, g_t) \leq mn$, 故 $\mathrm{Res}(f_t, g_t) = mn$, 因此 $\deg h = 0, m_{ij} = 1, \forall i, j$. 如若 $h \notin \mathbb{Z}$, 那么 $h \in \mathbb{Z}[x_1 t, \ldots, x_n t, y_1 t, \ldots, y_m t] \backslash \mathbb{Z}$ 的表达式中一定含有 t, 矛盾. 因此 $h \in \mathbb{Z}$. ♢

4. 在 *1* 中, $h = \pm 1$.

♣ 如果存在素数 p, 使得 $p|h$, 则在环 $B[x]/(p) = \mathbb{F}_p[a_n, b_m, x_1, \ldots, x_n, y_1, \ldots, y_m][x]$ 中, $\mathrm{Res}(\bar{f}, \bar{g}) = \overline{\mathrm{Res}(f, g)} = 0$. 这说明 $\bar{f}$ 与 $\bar{g}$ 有公因式. 但 $\bar{a}_n, \bar{b}_m, x_i$ 与 y_j 是变元, 因此 $\bar{f}$ 与 $\bar{g}$ 互素 (在上面的 UFD 上互素, 易见各 $x - x_i$, $x - y_j$ 均为素元), 这与 $\mathrm{Res}(\bar{f}, \bar{g}) = 0$ 矛盾. 故 $h = \pm 1$. ♢

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

♣ 以上论述知 h 的取值只至多与 m 和 n 有关, 我们对每个 (n, m) 取多项式 $f(x) = x^n - 1$ 和 $g(x) = x^m$, 此时有 $\mathrm{Res}(f, g) = \det M = 1$. 而考虑*1*中等式在相应取值映射下的像有 $1 = h \prod_{i=1} \prod_{j=1}^{m} \zeta_n^i = h$, 即 $\mathrm{Res}(f, g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(y_j - x_i)$. ♢

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

♣ 若记 $f(x)=a_n(x-x_1)\cdot\ldots\cdot(x-x_n), g(x)=b_m(x-y_1)\cdot\ldots\cdot(x-y_m)$, 则

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

再由 $f'(x_i)=a_n(x_i-x_1)\cdot\ldots\cdot(x_i-x_{i-1})(x_i-x_{i+1})\cdot\ldots\cdot(x_i-x_n)$, 知

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

即为要证等式 ♢

7. 设 $f(x)=a_n\prod\limits_{i=1}^{n}(x-x_i)=a_nx^n+\ldots+a_0$, 定义 f 的判别式 (discriminant) 为 $\Delta(f):=a_n^{2n-2}\prod\limits_{1\le i<j\le n}(x_i-x_j)^2$. 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.

♣ 直接由*6*中给出的 $\mathrm{Res}(f,f')$ 的表达式和 $\Delta(f)$ 的定义式, 可知 $\mathrm{Res}(f,f')=(-1)^{\frac{n(n-1)}{2}}a_n\Delta(f)$. 再注意到 $\mathrm{Res}(f,f')$ 是一个元素全为 a_i 的整数倍的矩阵的行列式, 因此 $\mathrm{Res}(f,f')$ 是关于 a_i 的 $2n-1$ 次齐次多项式. 注意这个矩阵的最后一行是 a_n 和 na_n, 因此 $a_n\mid\mathrm{Res}(f,g)$, 故 $\Delta(f)$ 是关于变量 $a_0,\ldots,a_n$ 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 $\Delta(f)$.

♣ 对 $f(x)=a_2x^2+a_1x+a_0$, $\Delta(f)=a_2^2(x_1-x_2)^2=a_2^2(x_1^2+x_2^2-2x_1x_2)=a_2(-a_1x_1-a_0-a_1x_2-a_0-2a_0)=-a_1(-a_1)-2a_2a_0-2a_2a_0=a_1^2-4a_0a_2$. 对于 $f(x)=a_3x^3+a_2x^2+a_1x+a_0$, 有 $\Delta(f)=a_2^2a_1^2-4a_3a_1^3-4a_2^3a_0-27a_3^2a_0^2+18a_3a_2a_1a_0$.♢

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.

♣ 假设 $V(f,g)$ 是无限集, 分别将其投射到 x 分量和 y 分量, 知这两个投射得到的结果中至少有一个是无限的. 不妨设是 x, 那么视 $f,g\in\mathbb{C}(x)[y]$, 由于 f 与 g 在 $\mathbb{C}[x][y]$ 中互素等价于在 $\mathbb{C}(x)[y]$ 中互素, 而 $\mathbb{C}(x)[y]$ 是 PID, 因此存在 $a,b\in\mathbb{C}(x)[y]$, 使得 $af+bg=1$. 将之通分后, 左侧为 $\mathbb{C}[x][y]$ 中多项式, 右侧为 $\mathbb{C}[X]$ 中多项式, 但左侧代入 V 中元素后取值都是 0, 于是 V 到 x 的投影都是右侧多项式的零点, 从而右侧关于 x 的多项式有无穷多个零点, 矛盾! ♢

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

♣ 首先存在 $\mathbb{C}^2$ 的某个线性自同构 φ, 使得 $\varphi(V(f,g))$ 到 x 轴 $\mathbb{C}$ 的投影为单射. 利用该坐标变换 φ 后, 每个 $x=a\in\mathbb{C}$ 至多只对应一个解 $y=b\in\mathbb{C}$, 使得 $(a,b)\in V(f,g)$. 视 $f(x,y)=a_n(x)y^n+\ldots+a_0(x), g(x,y)=b_m(x)y^m+\ldots+b_0(x)$, 做线性换元:

$$\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}a&b\\c&d\end{pmatrix}\cdot\begin{pmatrix}x\\y\end{pmatrix}$$

使得 f 和 g 关于 y 首一. 那么对于 $a\in\pi(V(f,g))$, 总可以保证变换后的 f 与 g 在代入 $x=a$ 后, y 的最高次项系数非零 (以便我们使用结式). 而 a 由至多 $m+n$ 次 (习

题 6) 多项式 $\mathrm{Res}_y(f(a,y),g(a,y))=0$ 的零点确定, 故知 $|V(f,g)|\leq \deg f\cdot\deg g$. ♢

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 α 和 β 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:

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

♣ 由于 $f(\gamma-x)$ 和 $g(x)$ 的系数均可由 a_i,b_j,γ 生成, 故两多项式均在 $\mathbb{Z}[a_0,\cdots,a_{n-1},b_0,\cdots,b_{m-1},\gamma][x]$ 中, 进而 $\mathrm{Res}(f(\gamma-x),g(x))\in\mathbb{Z}[a_0,\cdots,a_{n-1},b_0,\cdots,b_{m-1},\gamma]=\mathbb{Z}[a_0,\cdots,a_{n-1},b_0,\cdots,b_{m-1}][\gamma]$, 故有 $h(x)\in\mathbb{Z}[a_0,\cdots,a_{n-1},b_0,\cdots,b_{m-1}][x]$ 使得 $h(\gamma)=\mathrm{Res}(f(\gamma-x),g(x))$. 记 $a_n=b_m=1$, 考虑

$$f(\gamma-x)=\sum_{k=0}^{n}a_k(\gamma-x)^k=\sum_{k=0}^{n}\sum_{i=0}^{k}a_k\gamma^{k-i}(-1)^ix^i=\sum_{i=0}^{n}\left(\sum_{k=i}^{n}(-1)^ia_k\gamma^{k-i}\right)x^i$$

其各项系数 (记为 c_i) 均是关于 γ 的首一多项式, 且 γ 次数最高的为 x 的 0 次项系数 c_0. 写出结式定义中对应的矩阵, 在行列式中对 γ 的次数贡献最高的项为 $c_0^mb_m^n=c_0^m$ 为关于 γ 的首一多项式, 故 h 是首一的. ♢

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.

♣ 不妨设系数在 $\varphi(A)$ 中的首一多项式 $f(x)$ 和 $g(x)$ 分别是 α 和 β 的零化多项式, 那么由*1*知 $h(t)=\mathrm{Res}(f(t-x),g(x))\in\varphi(A)[t]$ 为关于 t 的首一多项式, 且 $h(\gamma)=0$(因

为此时 $f(\gamma-x)$ 和 $g(x)$ 有公共根 β, 又由 $x-b$ 首一, 可作带余除法得到整除关系, 故两多项式有公因式 $x-\beta$). 这就说明了 $\alpha+\beta$ 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.

♣ 不妨设系数在 $\varphi(A)$ 中的首一多项式 $f(x)$ 和 $g(x)$ 分别是 α 和 β 的零化多项式, 类似*1*可证 $T(t)=\mathrm{Res}(x^{\deg f}f(\frac{t}{x}),g(x))$ 为关于 t 的首一多项式, 且 $T(\alpha\beta)=0$(因为此时 $x^{\deg f}f(\frac{\alpha\beta}{x})$ 和 $g(x)$ 有公因式 $x-\beta$). 这就说明了 $\alpha\beta$ 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 $b\in C$.

♣ 参考 [6] 第一章 §2. ♢

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 $f(\varphi) = 0 \in End_A(M)$.

♣ 设 M 的一组生成元为 $x_1, \ldots, x_n, x_i \in M, 1 \leq i \leq n$. 则 φ 的作用可表示为:

$$\varphi(x_1, \ldots, x_n)^t = R \cdot (x_1, \ldots, x_n)^t$$

其中 $R \in M_n(A)$. 赋 M 以 $A[x]$-模:

$$\forall Q \in A[x], \forall m \in M, Q \cdot m := Q(\varphi)(m).$$

那么

$$(XI_n - R) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$$

而 $(XI_n - R)$ 是一个系数在 $A[x]$ 里的 n 阶矩阵. 在等式两侧同乘其伴随矩阵 $(XI_n - R)^*$, 可得

$$\det(XI_n - R) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$$

这表明 $f(X) = \det(XI_n - R)$ 是 $A[x]$-模的零化子. 因此 $f(\varphi) = 0 \in End_A(M)$. ♢

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.

♣ $\Leftarrow$: 设 $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ 为 a 的首一零化多项式, 则 $1, a, \ldots, a^{n-1}$ 为 $A[a]$ 的一组生成元.$\Rightarrow$: 在习题 1中, 令 $M = A[a]$, 并取 $\varphi \in End_A(A[a]), x \mapsto ax$ 则给出 $f(x) \in A[x]$, 使得 $f(\varphi) = 0 \in End_A(A[a])$, 也即 $f(a) = 0 \in B$. ♢

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.

♣ $\Leftarrow$: 直接由*1*, 取 $C = A[a]$. $\Rightarrow$: 在习题 1中, 令 $M = C$, 并取 $\varphi \in End_A(C), x \mapsto ax$ 则给出 $f(x) \in A[x]$, 使得 $f(\varphi) = 0 \in End_A(C)$, 也即 $f(a) = 0 \in B$. ♢

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

♣ 由*1*, 设 $A[a]$ 的一组生成元为 $1, a, \ldots, a^n$, $A[b]$ 的一组生成元为 $1, b, \ldots, b^m$, 则 $a^i b^j, 0 \le i \le n, 0 \le j \le m$ 给出了 $A[a, b]$ 的一组生成元. 而 $a + b \in A[a, b], ab \in A[a, b]$, 故由*2*知 $a + b$ 和 ab 均在 A 上整. ♢

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

♣ 设 M 的一组生成元为 $x_1, \ldots, x_n, x_i \in M, 1 \le i \le n$. 由 φ 是满的, 存在矩阵 $P \in M_n(A)$, 使得

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P \begin{pmatrix} \varphi(x_1) \\ \vdots \\ \varphi(x_n) \end{pmatrix} = \varphi(P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix})$$

前一个等号是因为 φ 是满射, 后一个等号是因为 $\varphi \in End_A(M)$, P 的系数均在 A

中. 如此则有:

$$(I_n-\varphi P)\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=0 \Rightarrow: (I_n-\varphi P)^*(I_n-\varphi P)\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=0 \Rightarrow \det(I_n-\varphi P)=0$$

于是 $\det(I_n-\varphi P)=0$ 即给出了 φ 的一个常数项为 1 的零化多项式 : $a_n\varphi^n+\ldots+a_1\varphi+1=0$, 这表明 $\varphi\in End_A(M)$ 有逆 $(-a_n\varphi^{n-1}-\ldots-a_1)$. 故 φ 为单同态, 也从而为同构. ♢

• 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:

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

♣ 容易验证这是一个复形, 因为对 $\forall\varphi\in\mathrm{Hom}_A(N,M'),\forall n\in N$, 有 $v\circ u\circ\varphi(n)=v\circ u(\varphi(n))=0$. 再验证 $\mathrm{Hom}_A(N,M')\xrightarrow{u\circ}\mathrm{Hom}_A(N,M)$ 是单射: 对 $\varphi\in\mathrm{Hom}_A(N,M')$, 如若 $u\circ\varphi=0$, 则由 u 是单射, 左消去可得 $\varphi=0$. 最后验证 $\mathrm{Ker}(v\circ)\subset\mathrm{Im}(u\circ)$.: 对于 $\phi\in\mathrm{Ker}(v\circ)$, $\forall a\in N, v\circ\varphi(a)=v(\varphi(a))=0$, 由 $\mathrm{Ker}\ v=\mathrm{Im}\ u$, 可知 $\exists!b\in M'$ 使得 $u(b)=a$. 定义 ψ: $a\mapsto b$, 可以验证这样给出的 ψ 是一个 A-模同态. 故 $\varphi=u\circ\psi$. 故 $\mathrm{Ker}\ (v\circ)\subset\mathrm{Im}(u\circ)$, 从而 $\mathrm{Ker}\ (v\circ)=\mathrm{Im}(u\circ)$. 因此原复形是一个正合列. ♢

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.

♣ 取 $N = A$, 利用同构 $\mathrm{Hom}_A(A, M') \simeq M', \varphi \mapsto \varphi(1_A)$, 即得 A-模正合列 $0 \to M' \xrightarrow{u} M \xrightarrow{v} M''$. ♢

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:

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

♣ 首先证明 $\mathrm{Hom}_A(M'', N) \xrightarrow{\circ v} \mathrm{Hom}_A(M, N)$ 是单射. 对 $f \in \mathrm{Hom}_A(M'', N)$, 若 $f \circ v = 0$, 由 v 是满射, 右消去有 $f = 0$, 故 $\mathrm{Hom}_A(M'', N) \xrightarrow{\circ v} \mathrm{Hom}_A(M, N)$ 是单射. 其次证明 $\mathrm{Ker}(\circ u) = \mathrm{Im}(\circ v)$. 对 $f \in \mathrm{Hom}_A(M'', N)$, 有 $f \circ v \circ u = f \circ (v \circ u) = 0$, 故 $\mathrm{Im}(\circ v) \subset \mathrm{Ker}(\circ u)$. 而 $\forall g \in \mathrm{Ker}(\circ u)$, 即 $g \circ u = 0$. 由 M'' 作为映射 u 的 Coker 的泛性质, 存在 $h \in \mathrm{Hom}_A(M'', N)$ 使得 $g = h \circ v$, 故 $g \in \mathrm{Im}(\circ)$. 即 $\mathrm{Hom}_A(M, N)$ 处正合. ♢

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.

♣ 对任意 A-模 N, 任意 $f \in \mathrm{Hom}_A(M, N)$, 若 $f \circ u = 0$, 则一定存在唯一的 (因为

$\circ v$ 是单射) 映射 $h \in \mathrm{Hom}_A(M'', N)$, 使得 $f = h \circ v$, 故 M'' 满足 u 的 Coker 的泛性质, 而此对象在同构意义下唯一, 即得原复形是正合列. ♢

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.

♣ 利用伴随函子和*2.*. 具体说, 就是对 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 $\Leftrightarrow$ 对任意 A-模 L, 有正合列 $\mathrm{Hom}_A(M_3 \otimes_A N, L) \xrightarrow{\circ\psi\otimes id} \mathrm{Hom}_A(M_2 \otimes_A N, L) \xrightarrow{\circ\varphi\otimes id} \mathrm{Hom}_A(M_1 \otimes_A N, L) \to 0$. 由伴随函子可知, 这等价于有正合列 $\mathrm{Hom}_A(M_3, \mathrm{Hom}_A(N, L)) \xrightarrow{\circ\psi} \mathrm{Hom}_A(M_2, \mathrm{Hom}_A(N, L)) \xrightarrow{\circ\varphi} \mathrm{Hom}_A(M_1, \mathrm{Hom}_A(N, L)) \to 0$. 而 $\mathrm{Hom}_A(N, L)$ 可以取遍任意 A-模 (利用 $\mathrm{Hom}_A(A, S) \simeq S$), 故由 *2* 知, 这等价于有正合列 $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3 \to 0$. 这就完成了证明. ♢

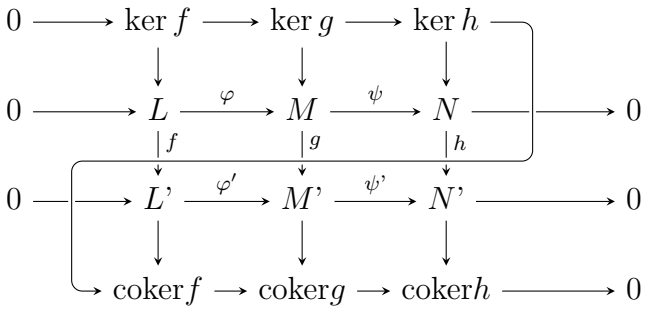
习题 **6.** (蛇引理) 设以下为 A-模的交换图表, 并且上下两行均为 (短) 正合列:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & L' & \longrightarrow & M' & \longrightarrow & N' & \longrightarrow & 0 \end{array}$$

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:



♣ 图中的长箭头是边缘同态 (boundary Homomorphism)d, 我们按以下方式来定义: 如果 $n \in \mathrm{Ker}(h)$, 那么存在 $m \in M$, 使得 $n = \psi(m)$, 而 $\psi(g(m)) = h(\psi(n)) = 0$, 故 $g(m) \in \mathrm{Ker}(\psi')$, 于是存在 $l' \in L'$, 使得 $f(m) = \varphi'(l')$. 那么定义 $d(n)$ 为 l' 在 $\mathrm{coker}(f)$ 中的像. 这个定义的合理性和序列 $0 \to \ker f \to \ker g \to \ker h \to \mathrm{coker} f \to \mathrm{coker} g \to \mathrm{coker} h \to 0$ 的正合性验证只需简单的追图. 而这可以在 [1] 中找到具体细节. ♢

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:

$$\begin{array}{ccccccccc}
\longrightarrow & C^i & \xrightarrow{d^i} & C^{i+1} & \xrightarrow{d^{i+1}} & C^{i+2} & \longrightarrow \\
 & \downarrow{\scriptstyle \varphi^i} & & \downarrow{\scriptstyle \varphi^{i+1}} & & \downarrow{\scriptstyle \varphi^{i+2}} & \\
\longrightarrow & C'^i & \xrightarrow{d'^i} & C'^{i+1} & \xrightarrow{d'^{i+1}} & C'^{i+2} & \longrightarrow
\end{array}$$

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 $H^i(\varphi^\bullet) : H^i(C'^\bullet) \to H^i(C^\bullet)$.

♣ 对于 $\forall i$, 由于有 $\in \mathbb{Z}, \varphi^{i+1} \circ d'^i = d^i \circ \varphi^i$, 可知 $\varphi^i(\ker\ d'^i) \subset \ker\ d^i, \varphi^{i+1}(\mathrm{Im}\ d'^i) \subset \mathrm{Im}\ d^i$, 故可以诱导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:

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

♣ 可直接由蛇引理推得 (用三次). 可以参考 [2] 的 CH.6 习题 6.5 给出的思路. ♢

• 单形的同调群

设 n 为正整数. 对 $0 \le m \le n$, 定义 $C_m(\Delta_n)$ 为符号集合 $\{\langle e_{i_0} e_{i_1} \cdots e_{i_m} \rangle \mid 0 \le i_0 \le i_1 \le \ldots \le i_m \le n\}$ 中的元素作为基生成的自由 $\mathbb{Z}$-模. 对于 $1 \le m \le n$, 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:$\forall 1 \le i \le n-1, \partial_i \circ \partial_{i+1} = 0$.

♣ 直接计算: $\partial_i \circ \partial_{i+1} \langle e_{k_0} e_{k_1} \cdots e_{k_{i+1}} \rangle = \partial_i \left(\sum_{j=0}^{i+1} (-1)^j \langle e_{k_0} \cdots \hat{e}_{k_j} \cdots e_{k_{i+1}} \rangle \right)$

$= \sum_{j=0}^{i+1} (-1)^j \left(\sum_{s=0}^{i+1} (-1)^s \langle e_{k_0} \cdots \hat{e}_{k_s} \cdots \hat{e}_{k_j} \cdots e_{k_{i+1}} \rangle + \sum_{s=j+1}^{i+1} (-1)^{s-1} \langle e_{k_0} \cdots \hat{e}_{k_j} \cdots \hat{e}_{k_s} \cdots e_{k-i+1} \rangle \right)$

$= \sum_{s<j} (-1)^{j+s} \langle e_{k_0} \cdots \hat{e}_{k_s} \cdots \hat{e}_{k_j} \cdots e_{k_{i+1}} \rangle + \sum_{j<s} (-1)^{j+s-1} \langle e_{k_0} \cdots \hat{e}_{k_j} \cdots \hat{e}_{k_s} \cdots e_{k_{i+1}} \rangle = 0.$

(第二行括号内后一项符号为 $(-1)^{s-1}$ 是因为 e_{k_s} 前的 e_{k_j} 已经被删去了, e_{k_s} 是第 $s-1$ 个) ♢

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 Δ_n 的第 i 阶同调群 (Homology group).

习题 **4.** 证明:

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

♣ 如下定义同态 $\delta_m \colon C_m(\Delta_n) \to C_{m+1}(\Delta_n)$

$$\delta_m(\langle e_{i_0} \cdots e_{i_m} \rangle) = \begin{cases} \langle e_0 e_{i_0} \cdots e_{i_m} \rangle, & i_0 \geq 1; \\ 0, & i_0 = 0. \end{cases}$$

可以验证, 这样定义的同态 δ_m 满足 $\partial_{m+1} \circ \delta_m + \delta_{m-1} \circ \partial_m = id$. 这个关系被称为同伦于零伦. 可以借此证明 $i_0 \geq 1$ 时同调群是 0. ♢

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 $\{\langle e_0 \cdots e_m\rangle \mid e_j \in S, \forall 0 \leq j \leq m\}$ 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: $g \cdot \langle g_0 g_1 \cdots g_m\rangle = \langle (gg_0)(gg_1) \cdots (gg_m)\rangle$, 并且 ∂'_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 $m \geq 0$, 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 $f \in C^n(G, V)$,

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

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 $\alpha_n(x_1, x_2, \ldots, x_n) = (g_1, \ldots, g_n)$, 其中

$$\begin{cases} g_1 = x_1 \\ g_2 = x_1 x_2 \\ \vdots \\ g_n = x_1 \cdots x_n \end{cases}$$

α_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:

$$\begin{array}{ccc} C^n(G,V) & \xrightarrow{d} & C^{n+1}(G,V) \\ \downarrow{\scriptstyle \beta_n} & & \downarrow{\scriptstyle \beta_{n+1}} \\ C^n(G,V) & \xrightarrow{\tilde{d}} & C^{n+1}(G,V) \end{array}$$

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

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

可以验证 β 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 $\det(PQ)=\det P\cdot\det Q$.

♣ 记 $P=(a_{ij}),Q=(b_{ij})$. 则 $\det PQ$ 是所有 a_{ij},b_{ij} 的多项式. 将矩阵系数均看作变元, 只需证明题设等式在多项式环 $\mathbb{Z}[a_{ij},b_{ij}\mid 1\leq i,j\leq n]$ 中成立. 此多项式本身与 A 的选取无关, 而已知 A 为域时等式成立, 取 $A=\mathbb{Q}$, 两多项式在 $\mathbb{Q}^{2n^2}$ 上的取值相同.

一般地, 若两多项式 $f,g\in\mathbb{Z}[X_1,\cdots,X_m]$ 在 $\mathbb{Q}^m$ 上所有点取值相同, 则对任意 $(a_1,\cdots,\ a_{m-1})\in\mathbb{Q}^{m-1}$, 令

$$f_a(X_m)=f(a_1,\cdots,a_{m-1},X_m)\in\mathbb{Q}[X_m],\quad g_a(X_m)=g(a_1,\cdots,a_{m-1},X_m)\in\mathbb{Q}[X_m],$$

考虑 $f_a-g_a\in\mathbb{Q}[X_m]$ 有无穷个根, 故各项系数均为 0. 这说明将 f,g 看作 X_m 的一元多项式 (系数取在 $\mathbb{Z}[X_1,\cdots,X_n]$ 中), 每个对应项系数在 $\mathbb{Q}^{m-1}$ 中取值相同. 以此归纳将次数降到 1 次即可知 $f=g$. ♢

♣(另一证明) 令 $V=A^n$ 为自由 A-模, 可定义一般交换环上的张量代数和外代数

$$T(V):=\bigoplus_{i=0}^{\infty}V^{\otimes i},\quad I_{\bigwedge}(V):=\langle x\otimes x\mid x\in V\rangle,\quad \bigwedge(V):=T(V)/I_{\bigwedge}(V)$$

其中 $V^0=A$, $V^{\oplus n}$ 为 n 个 V 的 A-张量积, 则 $T(V)$ 以张量积为乘法成为一个环 (A-代数), $I_{\bigwedge}(V)$ 为形如 $x\otimes x$ 的元素生成的 $T(V)$ 的双边理想. 以下操作均可模仿线性空间的情形: $\bigwedge(V)$ 为分次代数 (graded algebra, algèbre graduée), det 是 $End_A(V)$ 上的反交换多重线性映射, 而对自由模有 $M_n(A)$ 到 $End_A(V)$ 的自然同构. 由外代数的泛性

质, 任给 $f \in End_A(V)$, 会唯一诱导 $\bigwedge(f) \in End_{A\text{-alg}}(\bigwedge(V))$ 使得以下图表交换

$$\begin{array}{ccc} \bigwedge(V) & \xrightarrow{\bigwedge(f)} & \bigwedge(V) \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle i} \\ V & \xrightarrow{f} & V \end{array}$$

且 $\bigwedge^n(V) \simeq A$ 为 $\bigwedge(V)$ 中的最高次, 故 $\bigwedge(f)$ 将 $\bigwedge^n(V)$ 映到 $\bigwedge^n(V)$ 中, 将其限制在 $\bigwedge^n(V)$ 上得到唯一的 A-模同态 $d(f) : A \to A$. $d(f)$ 完全由 1 的像 $d(f)(1)$ 刻画, 即 $d(f) : a \mapsto d(f)(1)a$. 由斜对称同态与外代数的对应知像 $d(f)(1)$ 正是 $\det(f)$. 对于 $f, g \in End_A(V)$ 考虑

$$\begin{array}{ccccc} & & \overset{\bigwedge(gf)}{\frown} & & \\ \bigwedge(V) & \xrightarrow{\bigwedge(f)} & \bigwedge(V) & \xrightarrow{\bigwedge(g)} & \bigwedge(V) \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle i} \\ V & \xrightarrow{f} & V & \xrightarrow{g} & V \end{array}$$

由 $\bigwedge(gf)$ 的唯一性知 $\bigwedge(g)\bigwedge(f) = \bigwedge(gf)$, 进而有 $\det(g)\det(f) = \det(fg)$. ♢

该结论可以用于证明 2022 年九章杯的一道代数试题, 以下我们直接给出试题的推广情形:

命题 **1.** 令 ($P_{i,j}$ 为 $M_n(A)$ 中一族两两交换的方阵,$1 \le i, j \le m$), 令 $P = (P_{i,j})_{i,j \in [\![1,m]\!]} \in M_{nm}(A) = M_m(M_n(A))$. 则有等式

$$\det P = \det\left(\sum_{\sigma \in \mathfrak{m}} \mathrm{sgn}(\sigma) \prod_{i=1}^{m} P_{i,\sigma(i)}\right)$$

♣ 考虑 $P_{i,j}$ 和 $A \cdot I_n$ 在 $M_n(A)$ 中生成的子环 (A-子代数)B, 这是一个交换环, 而以上等式左边是 P 作为 A 上 $mn \times mn$ 的方阵的行列式, 右侧括号内是 P 作为 B 上

$m \times m$ 的方阵的行列式. 我们在多项式环 $A[T]$ 上考虑方阵

$$P_T = \begin{pmatrix} P_{1,1} + TI_n & P_{1,2} & \cdots & P_{1,m} \\ P_{2,1} & P_{2,2} & \cdots & P_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ P_{m,1} & P_{m,2} & \cdots & P_{m,m} \end{pmatrix},$$

并记 P_T 作为 $M_{mn}(A[T])$ 中元素的行列式为 $f(T) \in A[T]$, 而作为 $M_m(B[T])$ 中的元素的行列式为 $Q(T) \in B[T]$, 并再将 $Q(T)$ 看作 $M_n(A[T])$ 的元素取行列式得到 $g(T) \in A[T]$. 于是我们只需证明在 $A[T]$ 上有等式 $f(T) = g(T)$, 再令两多项式取 0 值即可证得结论. 令 $h(T) = \det(P_{1,1} + TI_n) \in A[T]$. 直接展开计算知 $h(T)$ 中最高次项为 T^n, 即 $h(T)$ 首一, 于是它不是 $A[T]$ 中的零因子. 将环 $A[T]$ 对 h 生成的乘法子集做局部化得到 $A[T]_h$, 由 h 不是零因子, 自然映射 $A[T] \to A[T]_h$ 为单射. 此时, h 在 $A[T]_h$ 中为可逆元, 故由习题 1, $P_{1,1} + TI_n$ 为 $A[T]_h$ 上的可逆方阵. 于是有

$$\begin{aligned} Q(T) &= (P_{1,1} + TI_n) \det_{M_m(B[T]_h)} \begin{pmatrix} I_n & P_{1,2} & \cdots & P_{1,m} \\ (P_{1,1} + TI_n)^{-1} P_{2,1} & P_{2,2} & \cdots & P_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ (P_{1,1} + TI_n)^{-1} P_{m,1} & P_{m,2} & \cdots & P_{m,m} \end{pmatrix} \\ &= (P_{1,1} + TI_n) \det_{M_m(B[T]_h)} \begin{pmatrix} I_n & 0 & \cdots & 0 \\ 0 & P'_{2,2} & \cdots & P'_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & P'_{m,2} & \cdots & P'_{m,m} \end{pmatrix} \\ &= (P_{1,1} + TI_n) \det_{M_{m-1}(B[T]_h)} \begin{pmatrix} P'_{2,2} & \cdots & P'_{2,m} \\ \vdots & \ddots & \vdots \\ P'_{m,2} & \cdots & P'_{m,m} \end{pmatrix} \end{aligned}$$

将以上 $M_{m-1}(B[T]_h)$ 中的矩阵记为 P', 将 $g(T)$ 视为 $A[T]_h$ 中的元素, 有

$$g(T) = \det_{M_n(A[T])}(Q(T)) = h \cdot \det_{M_n(A[T])}(\det_{M_{m-1}(B[T])} P').$$

另一方面, 直接将 P_T 看作 $A[T]_h$ 上的矩阵, 我们有

$$\begin{aligned} f(T) &= \det P_T \\ &= \det \begin{pmatrix} I_n & P_{1,2} & \cdots & P_{1,m} \\ (P_{1,1}+TI_n)^{-1}P_{2,1} & P_{2,2} & \cdots & P_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ (P_{1,1}+TI_n)^{-1}P_{m,1} & P_{m,2} & \cdots & P_{m,m} \end{pmatrix} \cdot \det \begin{pmatrix} P_{1,1}+TI_n & & & \\ & I_n & & \\ & & \ddots & \\ & & & I_n \end{pmatrix} \\ &= \det \begin{pmatrix} I_n & \\ & P' \end{pmatrix} \cdot \det(P_{1,1}+TI_n) \\ &= h \cdot \det P' \end{aligned}$$

由于 $A[T] \to A[T]_h$ 为单射, 只需在 $A[T]_h$ 上证明 $f(T) = g(T)$ 即得到在 $A[T]$ 上相等. 以 P' 代替 P, 我们即可归纳证明 $f(T) = g(T)$(由于 $m = 1$ 时等式自然成立). 再考虑 $f(0) = g(0)$ 即证原题等式. ♢

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

♣ 将 P 右方补上 $m-n$ 行零, 记作 P', 将 Q 下方补上 $m-n$ 列零, 记作 Q'. 则 $PQ = P'Q' \in M_m(A)$. 但 $P', Q' \in M_m(A)$, 且 $\det P' = \det Q' = 0$, 由习题 1可知 $\det(P'Q') = 0$. 故 $\det(PQ) = 0$. ♢

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

♣ 假设 $m > n$, 设 $e'_1, \ldots, e'_n$ 为 A^n 的基, $e_1, \ldots, e_m$ 为 A^m 的基. 记 $f_i = \varphi(e'_i), 1 \leq$

$i \leq n$. 记 $(f_1, \ldots, f_n) = (e_1, \ldots, e_m)P$, 其中 $P \in M_{m\times n}(A)$. 由 φ 为满同态, 知存在矩阵 $Q \in M_{n\times m}(A)$ 使得 $(e_1, \ldots, e_m) = (f_1, \ldots, f_n)Q$. 从而得 $(e_1, \ldots, e_m) = (e_1, \ldots, e_m)PQ$, 再由 $e_1, \ldots, e_m$ 为 A^m 的基, 知 $PQ = I_m$. 但由习题 2可知, $\det PQ = 0$, 矛盾. ♢

注: 也可以直接取 A 的极大理想 I, 对同态 $\varphi\colon A^n \to A^m$ 作用函子 $-\otimes_A A/I$ 得到满 (回顾 $-\otimes_R R$ 是右正合函子, 保满射) 的 A/I-线性映射 (这里利用了 $A\otimes_A A/I \times A/I$ 以及 $\otimes$ 与 $\oplus$ 交换)$(A/I)^n \to (A/I)^m$. 由线性代数知 $n \geq m$.

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 $Px = 0$.

♣ 设 $r \leq n$ 为最大的使得 P 存在行列式非零的 r 阶子方阵的正整数. 由 $\det P = 0$ 知 $r \leq n-1$. 不妨设 P 的左上角的 r 阶子方阵的行列式非零, 并记 P 的左上角的 $r+1$ 阶子方阵为 P_1, 则有

$$P = \begin{pmatrix} P_1 & * \\ Q & * \end{pmatrix}$$

取 $y \in A^{r+1}$ 为 P_1 的伴随方阵 P_1^* 的最后一列, 则 $y \neq 0$ 并且 $P_1 y = 0$. 由于将 P_1 的最后一行换为 Q 的任何一行后, 得到的方阵的行列式都为 0, 可知 $Qy = 0$. 从而 $x := \begin{pmatrix} y \\ 0 \end{pmatrix} \in A^n$ 即满足 $Px = 0$, 且 $x \neq 0$. ♢

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 $Px = 0$.

♣ 将 P 下方补上 $m-n$ 行零, 记为 P', 则 $P' \in M_m(A)$, 且 $\det P' = 0$. 由*1* 知存在非零列向量 $x \in A^m$, 使得 $P'x = 0$. 而 $P'x = \begin{pmatrix} Px \\ 0 \end{pmatrix} \in A^m$, 故 $Px = 0$. ♢

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

♣ 假设 $n > m$, 设 $e_1', \ldots, e_n'$ 为 A^n 的基, $e_1, \ldots, e_m$ 为 A^m 的基. 设 $\varphi(e_1', \ldots, e_n') =$

$(e_1,\dots,e_m)P$, 其中 $P\in M_{m\times n}(A)$, 则映射 φ 在这组基下的表示为: $A^n\to A^m, x\mapsto Px$. 由2知存在非零列向量 $x\in A^n$ 使得 $Px=0$, 这与 φ 是单射矛盾! 故 $n\le m$. ♢

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

1. $m\ge n$.

♣ 若 $n>m$, 考虑 A^n 的一组基 $e_1,\dots,e_n$, 并记 $(f_1,\dots,f_m)=(e_1,\dots,e_n)P$, 其中 $P\in M_{n\times m}(A)$. 因为 $f_1,\dots,f_m$ 是生成元, 所以 $(e_1,\dots,e_n)=(f_1,\dots,f_m)Q$, 其中 $Q\in M_{m\times n}(A)$. 由此 $(e_1,\dots,e_n)=(e_1,\dots,e_n)PQ$, 由于 $e_1,\dots,e_n$ 是基, 可知 $PQ=I_n$. 这与 $\det PQ=0$(习题 2) 矛盾. ♢

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.

♣ 若 $(A,\mathfrak{m})$ 为局部环, 考虑 f_i 在剩余类域 $k=A/\mathfrak{m}$ 中的像 $\bar{f}_i$, 它们可用 A 系数生成 k^n, 进而也 k 系数生成. k^n 为线性空间, 可从 $\bar{f}_1,\cdots,\bar{f}_m$ 中选取 n 个元素成为 k^n 的一组基. 由 Nakayama 引理, 它们的原像 $f_{i_1},\cdots,f_{i_n}$ 是 A^n 的一组生成元, 故不妨直接假设 $m=n$, 并证明 $f_1,\cdots,f_n$ 为基. 记 A^n 的一组基为 $e_1,\cdots,e_n$, 由于 $f_1,\cdots,f_n$ 为生成元, 我们令 $\varphi\colon A^n\to A^n$, $e_i\mapsto f_i$, 这给出一个满同态. 于是有正合列

$$0\to\ker\varphi\xrightarrow{i}A^n\xrightarrow{\varphi}A^n\to 0.$$

对每个 e_i 取一个 φ 下的原像 g_i, 即满足 $\varphi(g_i)=e_i$, 则此时令 $\psi\colon A^n\to A^n$, $e_i\mapsto g_i$, 其是 φ 的一个右逆, 即满足 $\varphi\circ\psi=\mathrm{id}$. 令 $(i,\psi)\colon \ker\varphi\oplus A^n\to A^n$, $(a,b)\mapsto i(a)+\psi(b)$. 其有逆映射 $A^n\to\ker\varphi\oplus A^n$, $a\mapsto(a-\psi(\varphi(a)),\varphi(a))$, 故这给出同构 $\ker\varphi\oplus A^n\simeq A^n$.

两边用 $-\otimes_A k$ 作用得到

$$(\ker\varphi\otimes_A k)\oplus k^n\simeq(\ker\varphi\otimes_A k)\oplus(A^n\otimes_A k)\simeq(\ker\varphi\oplus A^n)\otimes_A k\simeq A^n\otimes_A k\simeq k^n$$

为 k-线性空间同构. 两端比较维数知 $\ker\varphi\otimes_A k=0$, 再由 Nakayama 引理知 $\ker\varphi=0$. 于是 φ 为同构, 换言之, 各 f_i 是 A-线性无关的, 从而构成 A^n 的一组基. ♢

注: 关于 Nakayama 引理可见后面的第二轮口试题目 (选题 3). 事实上, 对本题我们有更强的结论: A 为交换环, M 为有限生成 A 模, 若 $\varphi\colon M\to M$ 为 A-模满自同态, 则 φ 为同构. 证明如下.

♣ 我们首先假定 A 为 Noether 环, 则 M 为 Noether 模. 此时, $\ker\varphi^k$ 为一列子模升链, 我们假定从 $k=n$ 起全相等. 由于 φ 为满同态, 任取 $x_1\in\ker\varphi$, 有 $\varphi(x_1)=0$, 且存在 $x_2,x_3,\cdots,x_{n+1}$ 满足 $x_i=\varphi(x_{i+1})$, $\forall i\in[\![1,n]\!]$. 故 $0=\varphi(x_1)=\varphi^2(x_2)=\cdots=\varphi^{n+1}(x_{n+1})\Rightarrow x_{n+1}\in\ker\varphi^{n+1}=\ker\varphi^n$, 故 $x_1=\varphi^n(x_{n+1})=0$. 这说明 $\ker\varphi=0$, 故 φ 为同构. 对于一般的情形, 我们仍先任取 $x\in\ker\varphi$, 并假定 M 的一组生成元为 $x_1,\cdots,x_m$. 由满射, 取定 x_i 的原像 y_i, 则存在 $a_{ij}\in A$ 使得 $y_i=\sum_{j=1}^m a_{ij}x_j$, 且存在 $b_{ij}\in A$ 使得 $\varphi(x_1)=\sum_{j=1}^m b_{ij}x_j$, 存在 $c_i\in A$ 使得 $x=\sum_{i=1}^m c_ix_i$. 考虑环 B 为 a_{ij},b_{ij},c_i 在 A 中生成的子环. A 中 1 生成的子环 R 为 $\mathbb{Z}$ 或 $\mathbb{Z}/n\mathbb{Z}$, 而 $B=R[a_{ij},b_{ij},c_i,1\leq i,j\leq n]$, 它是多项式环 $\mathbb{Z}[X_{ij},Y_{ij},Z_i,1\leq i,j\leq n]$ 的商环, 进而为 Noether 环. 此时 M 可看作 B-模, 且 φ 为 B-模同态, 但此时未必有限生成. 考虑 M 中由 $x_1,\cdots,x_m$ 生成的 B-子模 N, 由上面的定义, 每个 x_i 在 φ 下的像和原像均在 N 中, 故将 φ 限制下来得到满同态 $\varphi|_N\colon N\to N$. 由于 x 也在 N 中, 且仍在 ker 里, 于是归约到 Noether 的情形, 我们得到 $x=0$. ♢

又注: 许金兴老师审稿时指出本命题的标准证明方法是用行列式技巧: ♣ 设 $e_1, \cdots, e_n$ 为 M 的生成元, 则由 ϕ 为满同态, 知存在 A 上的 n 阶方阵 P, 使得

$$\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \varphi P \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix},$$

从而

$$(I_n - \varphi P) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 0.$$

两边同时乘以 $(I_n - \varphi P)^*$ 得到 $\det(I_n - \varphi P) = 0$. 这样若 $x \in Ker\varphi$, 则

$$0 = \det(I_n - \varphi P)x = x.$$

♢

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.
- $\forall y \in U_x$, φ 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.** $E = X \times \mathbb{C}^n$, π 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.

♣ 此时 $E = X\times\mathbb{C}^n$ 考虑投影 $p_2\colon E\to\mathbb{C}^n$, 我们给出映射 $p_{2*}\colon \Gamma(X,E)\to \mathrm{Hom}_*(X,\mathbb{C}^n)$, $s\mapsto p_2\circ s$. 其中 $*\in\{$连续, 光滑, 全纯, 正则,...$\}$ 代表一类映射, 集合 $\mathrm{Hom}_*(A,B)$ 代表全体 A 到 B 的相应的此类映射. 任给 $h\in\mathrm{Hom}_*(X,\mathbb{C}^n)$, 我们令 $\psi\colon \mathrm{Hom}_*(X,\mathbb{C}^n)\to\Gamma(X,E)$, 并定义 $\psi(h): x\mapsto (x,h(x))$. 易验证这是一个截面, 且给出的 ψ 恰与上面的 p_{2*} 互逆, 故均为双射. 与 $\Gamma(X,E)$ 类似, $\mathrm{Hom}_*(X,\mathbb{C}^n)$ 上有自然的 R-模结构, 即 $\forall f\in R$, $(f\cdot h)(x) := f(x)h(x)$(加法类似定义). 进一步地, 易验证 p_{2*} 为加法群同态, 且由定义有 $p_2\circ(f\cdot s) = f\cdot(p_2\circ s)$, 故 p_{2*} 为 R-模同构. 另一方面, 直接由 $f(x) = (f_1(x), f_2(x),\cdots,f_n(x))$ 给出 $f = (f_1,\cdots,f_n)$, 且每个 f_i 都与 f 一样满足连续 (光滑, 全纯, 正则,...), 故有有 $\mathrm{Hom}_*(X,\mathbb{C}^n) = \mathrm{Hom}_*(X,\mathbb{C})^n = R^n$(作为 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.

♣ 课程内容, 参考正课讲义. ♢

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 $\forall s_1,\ s_2 \in S,\ s_1 s_2 \in S$). 定义 $M \times S$ 上的一个关系 $\sim$ 如下:

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

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 $\dfrac{m_1}{s_1} + \dfrac{m_2}{s_2} := \dfrac{s_2 m_1 + s_1 m_2}{s_1 s_2}$, 数乘作用为 : $\dfrac{a}{s_1}\dfrac{m}{s_2} := \dfrac{am}{s_1 s_2}$. 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.

♣ 验证加法良定义: 若 $(m_1, s_1) \sim (n_1, r_1)$, $(m_2, s_2) \sim (n_2, r_2)$, 则存在 $t_1, t_2 \in S$, 使

得 $t_1(r_1m_1 - s_1n_1) = t_2(r_2m_2 - s_2n_2) = 0$, 这给出

$$\begin{aligned} & t_1t_2((s_2m_1 + s_1m_2)r_1r_2 - (r_2n_1 + r_1n_2)s_1s_2) \\ = & \, t_2r_2s_2t_1(r_1m_1 - s_1n_1) + t_1r_1s_1t_2(r_2m_2 - s_2n_2) \\ = & \, 0 \end{aligned}$$

于是 $\dfrac{s_2m_1 + s_1m_2}{s_1s_2} \sim \dfrac{r_2n_1 + r_1n_2}{r_1r_2}$, 也即加法良定义.

验证数乘良定义: 若 $(a, sf_1) \sim (b, r_1) \in A_S, (m, s_2) \sim (n, r_2) \in M_S$, 则有 $t_1, t_2 \in S$, 使得 $t_1(ar_1 - bs_1) = t_2(mr_2 - ns_2) = 0$, 这给出

$$t_1ar_1 = t_1bs_1, \ t_2mr_2 = t_2ns_2$$

两式相乘即有:

$$t_1t_2(amr_1r_2 - bns_1s_2) = 0$$

于是 $\dfrac{am}{s_1s_2} \sim \dfrac{bn}{r_1r_2}$, 也即乘法良定义. ♢

命题 **1.** 有如下的 A_S-模同构:

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

♣ 注意到 $M \otimes_A A_S$ 作为 A_S-模对应的数乘作用, 容易验证这是一个 A_S-模同态, 且对 $\forall \dfrac{m}{s} \in M_S$, 可以给出其在 $M \otimes_A A_S$ 中的一个原像 $m \otimes \dfrac{1}{s}$, 故这是一个满同态. 设

$\sum\limits_{i=1}^{n} m_i \otimes \dfrac{a_i}{s_i} \in \ker(\varphi)$, 记 $s = \prod\limits_{i=1}^{n} s_i$, 有

$$\begin{aligned}
&\sum_{i=1}^{n} m_i \otimes \frac{a_i}{s_i} \\
=& \sum_{i=1}^{n} m_i \otimes \frac{a_i \prod\limits_{j\neq i} s_i}{s} \\
=& \sum_{i=1}^{n} (a_i \prod_{j\neq i} s_i m_i) \otimes \frac{1}{s} \\
=& (\sum_{i=1}^{n} a_i \prod_{j\neq i} s_i m_i) \otimes \frac{1}{s}.
\end{aligned}$$

设 $m = \sum\limits_{i=1}^{n} a_i \prod\limits_{j\neq i} s_i m_i$, 则 $m \otimes \dfrac{1}{s} \in \ker(\varphi)$, 这表明存在 $t \in S$, 使得 $tm = 0 \in M$. 故在 $M \otimes_A A_S$ 中有 : $m \otimes \dfrac{1}{s} = tm \otimes \dfrac{1}{st} = 0$. 即 $\sum\limits_{i=1}^{n} m_i \otimes \dfrac{a_i}{s_i} = 0 \in M \otimes_A A_S$, 故 φ 为单射, 因此是 A_S-模同构. ♢

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 : $0 \to M_{1S} \to M_{2S} \to M_{3S} \to 0$.

♣ 由于 $- \otimes_A A_S$ 本身为右正合函子, 只需证明该函子保持单射. 考虑单射 $i \colon M_1 \to M_2$, 函子作用后诱导映射:

$$\begin{gathered}
\tilde{i} \colon M_{1S} \simeq M_1 \otimes_A A_S \to M_2 \otimes_A A_S \to M_{2S} \\
\frac{m_1}{s} \mapsto m_1 \otimes s \mapsto i(m_1) \otimes s \mapsto \frac{i(m_1)}{s}
\end{gathered}$$

故若 $\dfrac{m_1}{s} \in \ker(\tilde{i})$, 则有 $\dfrac{i(m_1)}{s} = 0 \in M_{2S}$, 故存在 $t \in S$, 使得 $t \cdot i(m_1) = 0 \in M_2$. 而 i 为 A-模单同态, 这表明 $i(tm_1) = 0 \Rightarrow tm_1 = 0 \in M_1$, 故 $\dfrac{m_1}{s} = 0 \in M_{1S}$, 说明 $\tilde{i}$ 为单射, 即 $- \otimes_A A_S$ 为正合函子. ♢

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 $m = 0$.

♣ 考虑 $I = \{a \in A \mid am = 0\}$, 容易验证这是 A 中的一个理想. 如果 $I = A$, 则 $m = 0$(因为 $1 \in I$, $1 \cdot m = m$). 否则 I 是 A 的真理想, 因而一定可以在 A 中找到一个包含 I 的极大理想 P. 在 P 处做局部化, 由 $\frac{m}{1} = 0$, 可知存在 $a \in A/P$, 使得 $am = 0$, 这与 $I \subset P$ 矛盾, 故 $I = A, m = 0$. ♢

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 π_P 为 DVR A_P 的极大理想的生成元.

♣ 对 M_P 赋予如下 A_P-模结构 (其中 $m_1, m_2, m \in M \subset K$):

$$\frac{m_1}{s_1} = \frac{m_2}{s_2} := \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$$

$$\frac{a}{s_1}\frac{m}{s_2} := \frac{am}{s_1 s_2}$$

类似我们在命题 1前所做的, 可以验证这是一个良好定义的 A_P-模结构, 于是 M_P 成为 $K = Frac(A_P)$ 的 A_P 子模. 设 M 作为有限生成 A-模的一组生成元是 $\{m_1, \ldots, m_n\}$, 那么 $\{\frac{m_1}{1}, \ldots, \frac{m_n}{1}\}$ 是 M_P 作为 A_P-模的一组生成元. 考虑每个 $\frac{m_i}{1}$ 在 $Frac(A_P)$ 中

的赋值, 取其中最小的整数记为 n_P(由于生成元个数有限, 故这个最小值存在), 可知 $M_P \subset A_P \cdot \pi_P^{n_P}$. 另一方面, M_P 中存在一个形如 $u \cdot \pi_P^{n_P}$ 的生成元, 其中 $u \in A_P^*$, 故 $A_P \cdot \pi_P^{n_P} \subset M_P$. 故 $M_P = A_P \cdot \pi_P^{n_P} \subset K$. ♢

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.

♣ 通过*1.*可以注意到, n_P 事实上由 M_P 生成元在 A_P 上的赋值决定. 因此只需要证明: 对每个生成元 $\frac{m_i}{1}$, 只有有限个非零素理想 P 使得 $\frac{m_i}{1}$ 在 $Frac(A_P)$ 上的赋值不是 0. 而这已经在阅读材料: Dedekind 整环的理想类群的习题 8中证明. ♢

3. 设 N 为 A 的一个分式理想. 则有:

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

♣ 如果 $Div(M) = Div(N)$, 仍然设 M 的一组生成元为 $m_i, i = 1, \ldots, l$, 设 N 的一组生成元为 n_j, $j = 1, \ldots, k$. 对每个 m_i, 我们将证明 $m_i \in N$. 考虑 A 的理想 $I := \{x \in A \mid xm_i \in N\}$. 如果 $I \neq A$, 取包含 I 的极大理想 P, 并作局部化 A_P, 那么 $\frac{m_i}{1} \in M_P = A_P \cdot \pi_P^{n_P} = N_P$, 可知存在不属于 P, 特别地, 不属于 I 中的元素 r, 使得 $rm_i \in N$. 具体地, 记 $m_i = \frac{a_i}{b_i} \in K$, 由于 $\frac{n_j}{1}$ 是 N_P 作为 A_P-模的一组生成元, 存在 $s_i \in A \backslash P$, $\frac{c_j}{t_j} \in A_P$, 使得

$$\frac{s_i a_i}{b_i} = \sum_{j=1}^{k} \frac{c_j}{t_j} \frac{n_j}{1} \in N_P$$

因此 $(s_i\prod_{j=1}^{k}t_j)m_i\in N$. 但 $r:=s_i\prod_{j=1}^{k}t_j\notin P$, 特别地,$(s_i\prod_{j=1}^{k}t_j)\notin I$, 这与 I 的定义矛盾. 因此 $I=A$, 从而 $m_i\in N$. 故 $M\subset N$. 对称地可以得到 $N\subset M$, 从而 $M=N$. ♢

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. 可以验证 (并不平凡, 主要因为证明逆元的存在并不容易), 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 $M=0$.

♣ 若 M 不为零模, 设 M 的一组个数最少 (因为 M 是有限生成模, 我们总可以做这样的假设) 的生成元为 $u_0,\ldots,u_n$, 则由 $M=mM$ 可知, 存在 $m_0,\ldots,m_n$, 使得 $u_0=m_0u_0+\ldots+m_nu_n$, 这给出 $(1-m_0)u_0=m_1u_1+\ldots+m_nu_n$. 而 m 是局部环 A 的唯一极大理想, 可知 $1-m_0\notin m\Rightarrow 1-m_0\in A^*$, 故 $u_0=\sum_{i=1}^{n}(1-m_0)^{-1}m_iu_i$, 也即 u_0 可以被 $u_1,\ldots,u_n$ 生成, 故 $u_1,\ldots,u_n$ 是 M 的一组元素个数更少的生成元, 矛盾 (注意 $n=0$ 的情形可以直接得出 $u_0=0$). 因此 M 只能是零模. ♢

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 $M=N$.

♣ 由于 M 有限生成就, 则商模 M/N 有限生成. 由 $M=n+mM$, 可知对 A-模 M/N 有 $M/N=mM/N$. 对其用命题 5, 可知 $M/N=0$, 即 $M=N$. ♢

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.

♣ 考虑由 $\{x_1,\ldots,x_n\}$ 生成的 M 的子模 N, 则 $M/mM=(N+mM)/mM$, 即有 $M=N+mM$, 由命题 6可知 $N=M$, 即 $x_1,\ldots,x_n$ 是 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 $m^k=(0)$.

♣ 由 A 为 Noether 环, 知 m^k 看作 A-模是有限生成模, 由 $m^k=m^{k+1}=m\cdot m^k$, 应用命题 5, 可知 $m^k=(0)$. ♢

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.

♣ 考虑 A 在 P 处的局部化 A_P, 则 PA_P 为局部环 A_P 的唯一极大理想. 由 A 是 Noether 整环可以推出 A_P 也为 Noether 整环. 若存在 $P^m=P^n, m<n$, 则 $P^m=P^{m+1}=\ldots=P^n$, 这给出 A_P 中有等式 $(PA_P)^m=(PA_P)^{m+1}$, 由*1.*即知 $(PA_P)^m=0$. 由整性, 只能是 $PA_P=0$, 这说明 P 中所有元素都是 A 中的幂零元, 而 A 为整环, 得出 P 为零理想, 矛盾! ♢

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.

♣ 由 M 有限生成, 设 A/m-线性空间 M/mM 的一组基为 $\bar{x}_1,\ldots,\bar{x}_n$, 则由命题 7可知 $x_1,\ldots,x_n$ 为 M 的一组生成元, 因此有满同态 $A^n\xrightarrow{\varphi}M$, $(a_1,\ldots,a_n)\to a_1x_1+$

$\ldots + a_n x_n$, 这给出正合列

$$0 \to \ker(\varphi) \to A^n \xrightarrow{\varphi} M \to 0$$

由于 M 是投射模, 该正合列可裂. 故有 A-模同构: $A^n \simeq \ker(\varphi) \oplus M$, 由 $- \otimes_A A/m$ 函子作用和直和交换, 可得

$$A^n \otimes_A A/m \simeq (\ker(\varphi) \otimes_A A/m) \oplus (M \otimes_A A/m)$$

由于对 A-模 N 总有同构 $N \otimes_A A/m \simeq N/mN$, 后者可视为 A/m 上的线性空间, 这给出 A/m-线性空间中的同构:

$$(A/m)^n \simeq \ker(\varphi)/(m\ker(\varphi)) \oplus M/mM$$

比较各部分作为 A/m-线性空间的维数, 可知 $\ker(\varphi)/(m\ker(\varphi)) = 0$. 因此 $- \otimes_A A/m$ 作用后得到的正合列为:

$$0 \to A^n \otimes_A A/m \xrightarrow{\bar{\varphi}} M \otimes_A A/m \to 0$$

这便给出了同构 $\bar{\varphi}$: $A^n \otimes_A A/m \to M \otimes_A A/m$. ♢

2. M 为自由 A-模.

♣ 在*1.*中我们证明了 $\ker(\varphi)/m\ker(\varphi) = 0$, 也即 $\ker(\varphi)$ 作为 A-模满足 $m\ker(\varphi) = \ker(\varphi)$. 由于 $\ker(\varphi)$ 是有限维自由模 A^n 的直和项 (见下方注记), 有 $\ker(\varphi)$ 作为 A-模有限生成, 援引命题 5, 可知 $\ker(\varphi) = 0$, 故 $M \simeq A^n$, 为自由 A-模.

注: 设 $A^n = M \oplus K$, A^n 的一组典范基记为 $(e_1, \ldots, e_n)$. 我们可以将其分解为 $e_i = m_i + k_i$, 使得 $m_i \in M$, $k_i \in K, i = 1, \ldots, n$. 对于 $\forall m \in M$, 存在 $a_1, \ldots, a_n \in A$, 使得 $m = \sum_{i=1}^{n} a_i e_i = \sum_{i=1}^{n} a_i(m_i + k_i) = \sum_{i=1}^{n} a_i m_i + \sum_{i=1}^{n} a_i k_i$. 由直和分解的唯一性, 得到 $m = \sum_{i=1}^{n} a_i m_i$, $\sum_{i=1}^{n} a_i k_i = 0$, 故 M 是有限生成 A-模, $m_1, \ldots, m_n$ 是其作为 A-模的一组生成元. ♢

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 $I^n M \cap N = I^{n-c}(I^c M \cap N)$.

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 $\sum_{i=1}^{m} f_i(y_1, \ldots, y_k)x_i \in N\}$. 证明: $I^n M \cap N = \{\sum_{i=1}^{m} f_i(y_1, \ldots, y_k)x_i \mid (f_1, \cdots, f_m) \in S_n\}$.

♣ 由定义, $I^n M$ 中的元素都是形如 $i_1 \cdots i_n \cdot m$, $i_1, \ldots, i_n \in I$, $m \in M$ 的元素的线性组合. 考虑 I 的一组生成元为 $y_1, \ldots, y_k$, M 的一组生成元为 $x_1, \ldots, x_m$, 将 $i_1, \ldots, i_n, m$ 用这些生成元表示出来, 可知

$$I^n M = \{\sum_{i=1}^{m} f_i(y_1, \ldots, y_k)x_i \mid (f_1, \ldots, f_m) \in R^m \text{且为 } n \text{ 次齐次多项式}\}$$

故 $I^n \cap N \subset \{\sum_{i=1}^{m} f_i(y_1, \ldots, y_k)x_i \mid (f_1, \ldots, f_m) \in S_n\}$.

另一方面, 由于 $f_i(y_1, \ldots, y_k)x_i \in I^n M$, 可知 $\sum_{i=1}^{m} f_i(y_1, \ldots, y_k)x_i \in I^n M$. 故对

$(f_1,\ldots,f_m)\in S_n$, 有 $\sum\limits_{i=1}^{m} f_i(y_1,\ldots,y_k)x_i \in I^nM\cap N$, 故 $I^nM\cap N=\{\sum\limits_{i=1}^{m} f_i(y_1,\ldots,y_k)x_i \mid (f_1,\cdots,f_m)\in S_n\}$. ♢

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.

♣ 由于 R^m 作为 R-模是有限生成的, 且由 Hilbert 基定理知 R 是 Noether 的, 因此 L 作为 R^m 的子模也是有限生成的. ♢

3. 证明 Artin-Rees 引理.

♣ 一方面, 容易验证当 $n\geq c$ 时, 有 $I^{n-c}(I^cM\cap N)\subset I^nM\cap N$.

另一方面, 由 S_n 的构造可知, 在*2.*中选取的这些生成元都是齐次的 (即作为 R^m 中的元素, 其每个分量都是 R 中同一次数的齐次多项式), 记为 $l_1,\ldots,l_t$. 对于每个 l_i, 设其次数为 c_i, 并记 $c=\max\limits_{1\leq i\leq t}c_i$. 我们证明这个 c 就是 $Artin-Rees$ 引理中需要的 c. 设 $n\geq c$, 根据*1.*中证明的对应关系, 对任意 $r\in I^nM\cap N$, 存在 $(f_1,\ldots,f_m)\in S_n$, 使得 $m=\sum\limits_{i=1}^{m} f_i(y_1,\ldots,y_k)x_i$. 根据 *2.*, 存在 $a_1,\ldots,a_t\in R$, 使得 $(f_1,\ldots,f_m)\sum\limits_{i=1}^{t} a_i\cdot l_i$. 注意每个 l_i 取自于 S_{d_i}, 且 $d_i\leq c$, 这表明 $a_i\in I^{n-d_i}$. 因此, 对每个 a_il_i, 记 $l_i=(h_1^i,\ldots,h_m^i)\in R^m$, $h_1^i,\ldots,h_m^i$ 均为 d_i 次齐次, 可知 $\sum\limits_{j=1}^{m} a_ih_j^i(y_1,\ldots,y_k)x_j\in I^{n-d_i}(I^{d_i}M\cap N)$, 由于 $d_i\leq c$, 简单验证可知 $I^{n-d_i}(I^{d_i}M\cap N)\subset I^{n-c}(I^cM\cap N)$. 这表明 $m=\sum\limits_{i=1}^{t}\sum\limits_{j=1}^{m} a_ih_j^i(y_1,\ldots,y_k)x_j\in I^{n-c}(I^cM\cap N)$. 于是 $I^nM\cap N\subset I^{n-c}(I^cM\cap N)$.

综上即说明了对任意 $n\geq c$, 都有 $I^nM\cap N=I^{n-c}(I^cM\cap N)$. ♢

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

♣ 注意到 J 是 A 的理想, 因而有限生成. 在 Artin-Rees 引理中, 取 $M=A,N=J$, $n=c+1$, 则 $I(I^c\cap J)=(I^{c+1}\cap J)$, 也即 $IJ=J$.

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

♣ 记 $M = \cap_{n=1}^{\infty} m^n$ 为有限生成 A-模. 由 *1.*, 知 $mM = M$. 由 Nakayama 引理第一形式 (本节选题 3.命题 5), 可知 $M = 0$, 即 $\cap_{n=1}^{\infty} m^n = (0)$. ♢

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

♣ 在 P 处作局部化, 得一 Noether 局部整环 A_P, 此时 PA_P 成为局部环 A_P 的唯一极大理想. 由*2.*可知 $(\cap_{n=1}^{\infty} P^n)A_P = \cap_{n=1}^{\infty}(PA_P)^n = (0)$. 由于 A 是整环, 这表明 $\cap_{n=1}^{\infty} P^n = (0)$. ♢

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 $x \in M, \pi_n(x \bmod I^{n+1}M) = x \bmod I^nM$. 令 $\hat{M}$ 为如下的 $\prod_{n=1}^{\infty} M/I^nM$ 的子模:

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

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.

♣ 用右正合函子 $-\otimes_A A/I^n$ 作用在原短正合列上 (注意 $M\otimes_A A/J\simeq M/JM$), 可得

$$M_1/I^nM_1\to M/I^nM\to M_2/I^nM_2\to 0$$

取出 ker, 进而有正合列

$$0\to M_1/(I^nM\cap M_1)\to M/I^nM\to M_2/I^nM_2\to 0$$

注意到 $M_1/(I^{n+1}M\cap M_1)\to M_1/(I^nM\cap M_1)$ 是满射, 对这组短正合列取逆向极限仍保持正合性, 即有如下短正合列:

$$0\to \varprojlim M_1/(I^nM\cap M_1)\to \hat{M}\to \hat{M}_2\to 0$$

一方面, $I^nM_1\subset I^nM\cap M_1$. 另一方面, 由 Artin-Rees 引理, 可知存在 $c\in\mathbb{N}$, 使得对任意 $n\in N$,$I^nM\cap M_1=I^{n-c}(I^cM\cap M_1)\subset I^{n-c}M_1$, 故 $\varprojlim\{M_1/(I^nM\cap M_1)\}=\varprojlim\{M_1/I^nM_1\}=\hat{M}_1$. 这即给出了正合列:

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

♢

注: 关于选题 4 的更多内容可以在 [1] 的第十章: 完备化 中找到。

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.ρ 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 $\mathbb{C}[V]^G\simeq\mathbb{C}[x_1,\ldots,x_n]^G$.

♣ 取定 V 的一组基 $(e_1,\ldots,e_n)$, 则 V^* 有一组基 $(e_1^*,\ldots,e_n^*)$. 对于 $v\in V$, 记 $v=x_1e_1+\ldots+x_ne_n$, 那么可以将 f 看作系数 $x_1,\ldots,x_n$ 的多项式:$f(x_1,\ldots,x_n):=f(x_1e_1+\ldots+x_ne_n)$. 为此, 在取定了这组基的情况下, 自然得到同构 $\mathbb{C}[V]\simeq\mathbb{C}[x_1,\cdots,x_n]$, 于是有 $\mathbb{C}[V]^G\simeq\mathbb{C}[x_1,\ldots,x_n]^G$. ♢

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 $c_j^{(i)}\in\mathbb{C}[x_1,\ldots,x_n]^G$.

♣ 由于 $f_i(x)$ 是 G-不变的, 则其各次数系数 c_j^i 也 G-不变, 即 $c_j^i\in\mathbb{C}[x_1,\ldots,x_n]^G$. ♢

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.

♣ 由 Hilbert 基定理, 立知 A 为 Noether 环的商环 (商去诸 $c_j^{(i)}$ 之间的代数关系), 因此 A 也是 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 (Hilbert 基定理). ♢

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

♣ $\mathbb{C}[x_1,\dots,x_n]^G$ 作为 Noether A-模 $\mathbb{C}[x_1,\dots,x_n]$ 的子模是有限生成的 A-模. ♢

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

♣ 注意到 A 是由有限个 $\mathbb{C}[x_1,\dots,x_n]^G$ 中的元素 $c_j^{(i)}$ 生成的, 则由*4*, $\mathbb{C}[x_1,\dots,x_n]^G$ 为有限生成 A-模, 这些生成元加上 $c_j^{(i)}$ 就作为 $\mathbb{C}$-代数的生成元生成了 $\mathbb{C}[x_1,\dots,x_n]^G$. 于是 $\mathbb{C}[x_1,\dots,x_n]^G$ 为有限生成 $\mathbb{C}$-代数. ♢

注: 很有趣的思路. 通过构造有限生成 $\mathbb{C}$-代数 A, 来间接证明 $\mathbb{C}[x_1,\dots,x_n]^G$ 是有限生成 $\mathbb{C}$-代数. 这里的关键是 $A\subset\mathbb{C}[x_1,\dots,x_n]^G$, 且 $\mathbb{C}[x_1,\dots,x_n]^G$ 作为 A-模是有限生成的. 对比我们在讲义 2022-03-21习题 2中给出的另一个证明, 可以发现此处的想法更好地利用了 Hilbert 基定理和 Noether 模的性质.

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

♣ (Noether 归纳法) 对 A 中的理想 I, 考虑命题 $P(I)$: 商环 A/I 的极小素理想个数有限. 令 $S=\{I|I$ 为 A 的理想, 且命题 $P(I)$ 不成立 $\}$. 假设 S 为非空集合, 由 A 为 Noether 环知 S 中存在极大元. 令 I_0 为 S 的一个极大元, 不难验证 I_0 不是素理想 (否则 A/I_0 为整环, 零理想是唯一极小素理想, 也即命题 $P(I_0)$ 成立, $I_0\notin P$, 矛盾), 因此存在 $x,y\in A$, 使得 x,y 均不在 I_0 中, 而 $xy\in I_0$. 由 I_0 的极大性可知 $I_0+(x), I_0+(y)$ 均不在 S 中, 而 $(I_0+(x))(I_0+(y))\subset I_0$. 将 A/I 的素理想对应到 A 中包含 I 的素理想, 可以验证:

$$\{A/I_0\text{的极小素理想}\}\subset\{A/I_0+(x)\text{的极小素理想}\}\cup\{A/I_0+(y)\text{的极小素理想}\}.$$

这与 $I_0 \in S, I_0 + (x) \notin S, I_0 + (y) \notin S$ 矛盾. 由此知 $S = \varnothing$, 即命题 $P(I)$ 对任意理想 I 均成立. 特别地, 取 I 为零理想, 则得到命题: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 $A/I \hookrightarrow M$.

♣ $\Rightarrow$: 考虑模同态 φ: $A \to M$, $a \mapsto ax$, 那么 $\ker(\varphi) = Ann(x) = I$, 故诱导模的单同态 $A/I \hookrightarrow M : a + I \mapsto ax$. $\Leftarrow$: 这个模同态的存在表明 $I \subset Ann(x)$. 又因为这是单同态, 可知 $Ann(x) \subset I$. 故 $I = Ann(x)$. ♢

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 $I \in Ass(M)$.

♣ 若 I 不是素理想, 则存在 $x, y \in A \backslash I$, 但 $xy \in I$. 于是由 I 的极大性可知 $I + (x) \notin \{Ann(x) | x \in M, x \neq 0\}$, $I + (y) \notin \{Ann(x) | x \in M, x \neq 0\}$. 设 $I = I + (xy) = Ann(m)$, 则 $xm \neq 0, ym \neq 0$, 但 $xym = 0$. 考虑理想 $S = \{t \in A \backslash I | ty \in I\}$. 则 $x \in S$, $S \neq \varnothing$. 考虑理想 $I + (S)$, 知 $I + (S) \subset Ann(ym)$. 另一方面, 若 $q \in Ann(ym)$, 则 $qy \in I$, 故 $q \in I + (S)$. 因此 $Ann(ym) = I + S$, 故 $I + S \in \{Ann(x) | x \in M, x \neq 0\}$, 这与 I 的极大性矛盾. 故 I 是素理想, 从而 $I \in Ass(M)$. ♢

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

♣ 首先 $Ann(1_M)$ 的存在保证了集合 $\{Ann(x)|x \in M, x \neq 0\}$ 非空. 由*2*可知 $Ass(M) \neq \varnothing$. ♢

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.

♣ 若 $\mathfrak{P} = Ann(m)$, 则 $\mathfrak{P}A_S = Ann(\frac{m}{1})$. 这是因为 $\frac{a_1}{s_1} \cdot \frac{m}{1} = 0 \Leftrightarrow \exists s \in S, sa_1m = 0 \Leftrightarrow sa_1 \in \mathfrak{P} \Leftrightarrow a_1 \in \mathfrak{P} \Leftrightarrow a_1 \in \mathfrak{P}$. 若 $\mathfrak{P}A_S = Ann(\frac{m}{s})$, 由第一轮口试题目习题 6, 可以构造 $m' \in M$, 使得 $\mathfrak{P} = Ann(m')$. 故 $Ass(M_S)$ 与 $\{P \in Ass(M)|P \cap S = \varnothing\}$ 一一对应. ♢

习题 **4.** A 的极小素理想均为伴随素理想.

♣ 设 $\mathfrak{P}$ 为极小素理想, 则局部化 A_P 中只有一个素理想, 从而由习题 2.*3*知 $\mathfrak{P}A_P$ 一定为 A_P 中的伴随素理想. 对应回 $\mathfrak{P}$ 为 M 的伴随素理想. ♢

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

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

♣ 设 $\mathfrak{P} \in Ass(M)$, 则 $A/\mathfrak{P} \hookrightarrow M$, 考察 M 的子模的交: 若 $A/\mathfrak{P} \cap M_1 = 0$, 则 $A/\mathfrak{P} \cap \ker \pi = 0$, 故存在 $A/\mathfrak{P} \hookrightarrow M_2$, 也即 $\mathfrak{P} \in Ass(M_2)$. 若 $A/\mathfrak{P} \cap M_1 \neq 0$, 则设 $0 \neq x \in A/\mathfrak{P}$, 则 $Ann(x) = \mathfrak{P}$(设 $A/\mathfrak{P} \hookrightarrow M, 1 \mapsto m$, 则 $x = am, a \in A$. 故 $tx = 0 \Leftrightarrow tam = 0 \Leftrightarrow ta \in \mathfrak{P} \Leftrightarrow t \in \mathfrak{P}$), 从而 $\mathfrak{P} \in Ass(M_1)$. ♢

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.

♣ 考虑 $A/\mathfrak{P} \hookrightarrow M$. 取 $M_1 \subset M$, 使得 $M_1 \simeq A/\mathfrak{P}$. 记 N 为所有 M 的满足存在如下升链的子模中最大的 (存在性由 M 有限生成 A-模进而 Noether 保证):

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_k = N, M_{i+1}/M_i \simeq A/\mathfrak{P}_i, \mathfrak{P}_i \subset A\text{为素理想}$$

若 $M \neq N$, 考虑 M/N 有子模 $M'/N \simeq A/\mathfrak{P}'$, 则 M' 可作为上述升链的一个延伸, 矛盾. 故我们可以构造形如

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_k = M, M_{i+1}/M_i \simeq A/\mathfrak{P}_i, \mathfrak{P}_i \subset A\text{为素理想}$$

的升链. 再由 $M_1 \simeq A/\mathfrak{P}$, 可知 $Ass(M_1)$ 有限 (因为若 $x \in A/\mathfrak{P}$, , 则 $Ann(x) = \mathfrak{P}$.), 进而由*1*归纳可知 $Ass(M)$ 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.

♣ 若 P 在 $A[X]$ 中可约, 则存在 $Q,R\in A[X]$, 使得 $P=QR$, 且 $\deg P=\deg Q=1$ (因为 P 的各项系数均为 1, 若有 $\lambda\in A$ 使得 $\lambda|P$, 直接可以得出 λ 是 A 中可逆元).

我们定义 A 中范数如下:

$$\varphi\colon A\to\mathbb{N},\ a+b\sqrt{3}i\mapsto a^2+3b^2$$

此时 φ 为乘法同态. 记 $Q=q_1x+q_2,\ R=r_1x+r_2$, 其中 $q_1,q_2,r_1,r_2\in A$, 比较 $P=QR$ 两侧系数可知 $q_1r_1=1,q_2r_2=1$. 将 φ 作用在这两个式子上, 可得 $\varphi(q_1)\varphi(r_1)=\varphi(q_2)\varphi(r_2)=1$. 由于 φ 取值于 $\mathbb{N}$, 立有 $\varphi(q_1)=\varphi(q_2)=\varphi(r_1)=\varphi(r_2)=1$, 进而有 $\{q_1,q_2,r_1,r_2\}\subset\{\pm1\}$, 逐一验证可知均不满足 $PQ=R$. 故 P 为 $A[x]$ 中不可约多项式. ♢

1.2 证明 P 视作 $K[x]$ 中的多项式时是可约的.

♣ 在 $K[x]$ 中直接给出分解: $P=X^2-X+1=(X-\dfrac{1+\sqrt{3}i}{2})(X-\dfrac{2}{1+\sqrt{3}i})$. ♢

1.3 得出结论: A 不是唯一分解整环.

♣ 若 A 是唯一分解整环, 我们知道 $A[X]$ 上的所有不可约元可分为两类

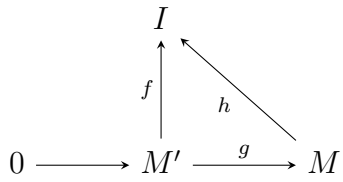
(i)A 中的不可约元.

(ii)$K[X]$ 中正次数的本原不可约多项式.

而前两问中证明了 P 不满足这两个条件中的任意一个, 但是 P 是 $A[X]$ 中的不可约多项式, 这便给出矛盾. 因此环 $A=\mathbb{Z}[i\sqrt{3}]$ 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:



(ii) 形如

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

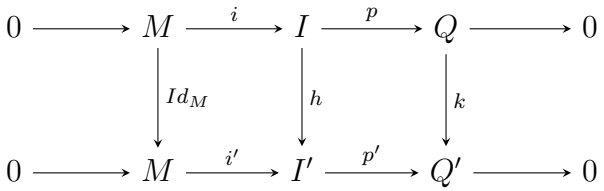
的 A-模正合列均可裂.

以下假设 I 和 I' 为内射 A-模, 且有如下两个正合列:

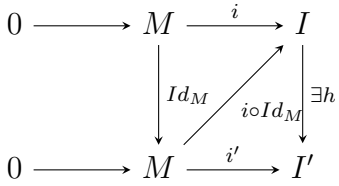
$$0 \longrightarrow M \xrightarrow{i} I \xrightarrow{p} Q \longrightarrow 0$$

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

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:



♣ 首先考虑单同态 $i \circ Id_M$ 和同态 i':



由于 I' 是内射模, 根据定义(i), 存在 A-模同态 $h\colon I \to I'$, 使得 $h \circ (i \circ Id_M) = i'$, 也即 $h \circ i = i' \circ Id_M$. 因此这个 h 可以保证左半边图表交换.

然后我们如下定义 A-模同态 k:

对 $\forall q \in Q$, 由 p 为满射, 可以取出 $i_0 \in I$, 使得 $p(i_0) = q$. 我们定义 $k\colon Q \to Q'$, $q \mapsto p'(h(i_0))$. 由于 $p'(h(\mathrm{Ker}\ p)) = p'(h(\mathrm{Im}\ i)) = p'(h(i(M)) = p'(i'(M)) = 0$, 可知 k 良定. 且根据 k 的定义, 立刻得到右半边图表交换.

综上便给出了所需的 A-模同态 h 和 k. ♢

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:

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

♣ 容易有 r 和 s 为 A-模同态. 我们逐步验证正合性.

(1) 首先说明 r 为单射. 若有 $x \in I$, 使得 $r(x) = (p(x), h(x)) = 0$, 那么 $p(x) = h(x) = 0$, 因此 $x \in \mathrm{Ker}\ p = \mathrm{Im}\ i$, 即存在 $m \in M$, 使得 $x = i(m)$. 同时这个 m 满足 $h(x) = h(i(m)) = i'(m) = 0$. 而 i' 为单射, 可知 $m = 0$, 因此 $x = 0$. 故 r 为单射.

(2) 再说明 $\mathrm{Ker}\ s = \mathrm{Im}\ r$. 对 $\forall x \in I$, 由图表交换有 $s \circ r(x) = s(p(x), h(x)) = k \circ p(x) - p' \circ h(x) = 0$. 故 $\mathrm{Ker}\ s \subset \mathrm{Im}\ r$. 若 $(q, x') \in \mathrm{Ker}\ s$, 即 $k(q) = p'(x')$. 由 p 为满射, 取 $x \in I$, 使得 $p(x) = q$, 故有 $p'(x' - h(x)) = p'(x') - k(p(x)) = p'(x') - k(q) = 0$. 因此

$x'-h(x)\in\operatorname{Ker}p'=\operatorname{Im}i'=\operatorname{Im}h\circ i\subset\operatorname{Im}h$, 故存在 $i_1\in\operatorname{Im}i$, 使得 $h(i_1)=x'-h(x)$. 由 $i_1\in\operatorname{Im}i=\operatorname{Ker}p$, 有 $p(x+i_1)=p(x)=q$, 且 $h(x+i_1)=h(x)+h(i_1)=h(x)+x'-h(x)=x'$, 故 $r(x+i_1)=(q,x')$. 因此 $\operatorname{Ker}s\subset\operatorname{Im}r$. 于是 $Q\oplus I'$ 处正合.

(3) 最后说明 s 为满射. 对 $q'\in Q'$, 由 q' 满射, 取出 $x'\in I'$ 使得 $p'(x')=q'$, 那么 $s(0,-x')=0-p'(-x')=q'$, 故 s 为满射.

综上便得到了 A-模短正合列:

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

♢

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

♣ 在 *2.2* 得到的短正合列中, 由 I 为内射模, 根据定义(ii), 可知该短正合列可裂, 因此有 A-模同构 $Q\oplus I'\simeq I\oplus Q'$. ♢

3 设 A 为交换环, $I_1,\ldots,I_r$ 为 A 中理想. 乘积理想 $I_1I_2\cdots I_r$ 定义为由形如 $x_1x_2\cdots x_r$ 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

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

♣ 由于 $\mathfrak{M}_i$ 互异且极大, 可知对 $i=1,\ldots,s-1$, 总有 $\mathfrak{M}_i\backslash\mathfrak{M}_s\neq\varnothing$, 因此可取 $a_i\in\mathfrak{M}_i\backslash\mathfrak{M}_s$. 由 $\mathfrak{M}_s$ 为极大理想从而为素理想, 可知 $\prod\limits_{i=1}^{s_1}a_i\notin\mathfrak{M}_s$, 故 $\prod\limits_{i=1}^{s_1}a_i\notin$

$\mathfrak{M}_1\mathfrak{M}_2\cdots\mathfrak{M}_s$(因为 $\mathfrak{M}_1\mathfrak{M}_2\cdots\mathfrak{M}_s \subset \mathfrak{M}_s$. 故 $\prod_{i=1}^{s_1} a_i \in \mathfrak{M}_1\mathfrak{M}_2\cdots\mathfrak{M}_{s-1}\backslash\mathfrak{M}_1\mathfrak{M}_2\cdots\mathfrak{M}_s$. ♢

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.

♣ 假设 A 中有无穷多个极大理想, 取其中可数个记为 $(\mathfrak{M}_i)_{i\in\mathbb{N}}$. 由 *3.1*, 我们可以构造如下理想降链:

$$\mathfrak{M}_1 \supsetneq \mathfrak{M}_1\mathfrak{M}_2 \supsetneq \ldots \supsetneq \mathfrak{M}_1\mathfrak{M}_2\cdots\mathfrak{M}_{s-1} \supsetneq \mathfrak{M}_1\mathfrak{M}_2\cdots\mathfrak{M}_s \supseteq \cdots$$

这自然与 A 的 Artin 性矛盾. 因此 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 $\mathfrak{r}^n = \mathfrak{r}^N$.

♣ 构造理想降链:

$$\mathfrak{r} \supseteq \mathfrak{r}^2 \supseteq \cdots \supseteq \mathfrak{r}^n \supseteq \cdots$$

由于 A 是 Artin 的, 该理想降链稳定, 即存在 $N \in \mathbb{N}$ 使得 $\mathfrak{r}^n = \mathfrak{r}^N$, $\forall n \geq N$. ♢

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 $\mathfrak{a} = \{0\}$.

♣ 先验证 $\mathfrak{b}$ 为 A 中理想. 若 $b_1 \in \mathfrak{b}$, $b_2 \in \mathfrak{b}$, 那么 $(b_1+b_2)a = b_1a+b_2a = 0$, $\forall a \in \mathfrak{a}$, 故 $b_1 + b_2 \in \mathfrak{b}$. 若 $b \in \mathfrak{b}$, $c \in A$, 那么 $cba = c(ba) = 0, \forall a \in \mathfrak{a}$, 故 $cb \in \mathfrak{b}$. 由 A 是交换

环, 这便说明了 b 为 A 中的理想.

假设 $\mathfrak{b} \neq A$, 那么 $A/\mathfrak{b}$ 作为 A 的商模是 Artin 模. 考虑 $A/\mathfrak{b}$ 的非零子模集合. 由假设 $A/\mathfrak{b} \neq 0$, 则该集合中的子模在包含关系下有极小元. 由于 $A/\mathfrak{b}$ 的子模一一对应到 A 中含有 $\mathfrak{b}$ 的理想, 我们可以将这个极小元记为 $\mathfrak{c}/\mathfrak{b}$, 其中 $\mathfrak{c}$ 为 A 的一个理想. 由极小性可知 $\mathfrak{c}/\mathfrak{b}$ 为单模.

记这个单模为 M, 容易验证其零化子 $Ann(M)$ 为 A 中理想 (因为 A 为交换环). 任取 M 中非零元 m, 总有 $0 \neq Am \subset M$, 由 M 的单性可知 $Am = M$, 故 $Ann(M) = Ann(Am) = Ann(m)$. 考虑满射 $\varphi\colon A \to Am$, $a \mapsto am$, 有 $M = Am \simeq A/Ann(m) = A/Ann(M)$. 若存在 A 的真理想 N 使得 $Ann(M) \subset N \subseteq A$, 有 $0 \subseteq A/N \subset A/Ann(M)$. 但 $A/Ann(M) \simeq M$ 为单模, 可知 $A/N = A/Ann(M)$, 故 $Ann(M) = N$, 即 $Ann(M)$ 为极大理想.

因此 $Ann(\mathfrak{c}/\mathfrak{b})$ 为 A 中极大理想, 故 $\exists 1 \leq i \leq t$, 使得 $Ann(\mathfrak{c}/\mathfrak{b}) = \mathfrak{M}_i$, 也即是说 $\mathfrak{M}_i \cdot \mathfrak{c} \subset \mathfrak{b}$, 因此 $\mathfrak{rc} = (\cap_{i=1}^{t}\mathfrak{M}_i \cdot \mathfrak{c} \subset \mathfrak{M}_i \cdot \mathfrak{c} \subset \mathfrak{b}$. 但 $\mathfrak{b} = \{b \in A \mid b\mathfrak{r}^N = 0\}$, 故 $\forall c \in \mathfrak{c}$, $\forall a \in \mathfrak{r}$, $\forall d \in \mathfrak{r}^N$, 总有 $c \cdot (ad) = (ca) \cdot d = 0$. 由于形如 ad 的元素生成了 $\mathfrak{r}^{N+1}$, 这表明 $\mathfrak{c} \subset Ann(\mathfrak{r}^{N+1})$. 但由 *3.3* 知 $\mathfrak{r}^{N+1} = \mathfrak{M}$, 故 $c \in Ann(\mathfrak{r}^{N+1}) = Ann(\mathfrak{r}^N)$. 但 $Ann(\mathfrak{r}^N) = \mathfrak{b}$, 故 $\mathfrak{c} \subset \mathfrak{b}$, 进而有 $\mathfrak{c} = \mathfrak{b} \Rightarrow \mathfrak{c}/\mathfrak{b} = 0$, 与 $\mathfrak{c}/\mathfrak{b}$ 的选取矛盾. 故 $b = A$, 这表明 $1_A \in Ann(\mathfrak{a})$, 即 $\mathfrak{a} = 0$. ♢

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

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

.

♣ 由假设可知集合 $\{(a - \lambda_i 1_A)^{-1} \mid i \in I\}$ 为无穷集. 由于 A 为有限维 $\mathbb{C}$-代数, 不妨设 $\dim_{\mathbb{C}} A = n$. 取 $r = n + 1$, 则 $\{a - \lambda_i 1_A)^{-1} \mid 1 \leq i \leq r\}$ 是 $\mathbb{C}$-线性相关集, 故存在不全为零的 $\mu_1, \ldots, \mu_r$, 使得 $\sum\limits_{i=1}^{r} \mu_i (a - \lambda_i 1_A)^{-1} = 0$. 删去其中 $\mu_i = 0$ 的项, 并仍将剩下的项记为 r 项, 可知 $r \geq 2$(因为每个 $(a - \lambda_i 1_A)^{-1}$ 都可逆进而不是零因子), 这便给出了需要的等式. ♢

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

♣ 在 *4.1* 所得等式 $\sum\limits_{i=1}^{r} (a - \lambda_i 1_A)^{-1} = 0$ 的两侧同乘 $\prod\limits_{i=1}^{r} (a - \lambda_i 1_A)$, 可得

$$\sum_{i=1}^{r} \mu_i \prod_{j=1, j \neq i}^{r} (a - \lambda_j 1_A) = 0$$

记 $P(X) = \sum\limits_{i=1}^{r} \mu_i \prod\limits_{j=1, j \neq i}^{r} (X - \lambda_j)$, 便给出了 $\mathbb{C}[X]$ 中的一个零化 a 的多项式. 下面证明 P 次数严格正, 即 P 不是常值多项式. 由于 $P(a) = 0$, 只需证明 $P \neq 0$. 直接考虑 $P(\lambda_1) = \mu_1 \prod\limits_{j=2}^{n} (\lambda_1 - \lambda_j) \neq 0$, 说明 $P \neq 0$. 因此 $P \in \mathbb{C}[X]$ 便给出了所需的零化 a 的正次数多项式. ♢

4.3 证明 P 的零点集与 $Spec(a)$ 的交非空.

♣ 记多项式 P 在 $\mathbb{C}$ 中的根为 $x_1,\ldots,x_k$, 则 $P(a)=\prod_{j=1}^{k}(a-x_j1_A)=0\in A$, 故一定存在 $1\le j\le k$, 使得 $a-x_j1_A\notin A^\times$, 即是说 $x_j\in Spec(a)$. ♢

注: 事实上 P 的零点集包含于 $Spec(a)$.

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)

♣ 假设 $a\neq 0$, 考虑如下两种情况:

(i) 存在无穷多个 $\lambda\in C$, 使得 $a-\lambda1_A$ 可逆. 由前三小问可知 $Spec(a)\neq\varnothing$.

(ii) 只有有限多个 $\lambda\in C$, 使得 $a-\lambda1_A$ 可逆. 由 $\mathbb{C}$ 是无限集, 有 $Spec(a)\neq\varnothing$. ♢

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

♣ 若 $\dim_{\mathbb{C}}\ge 2$, 取 $a\in A\backslash\{\lambda1_A\mid\lambda\in\mathbb{C}\}$. 由于 A 是可除 $\mathbb{C}$-代数, 对 $\forall\lambda\in\mathbb{C}$, 有 $a-\lambda1_A\in A^\times$, 也即 $Spec(A)=\varnothing$, 这与 *4.4* 的结论矛盾. 因此 $\dim_{\mathbb{C}}=1$, 也即是说 $A=\{\lambda1_A\mid\lambda\in\mathbb{C}\}=\mathbb{C}$(此时 $Spec(\lambda)=\{\lambda\}$). ♢

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 $Spec(a)=\{0\}$

♣ 取 $N\in\mathbb{N}^*$ 使得 $a^N=0$. 首先说明 $a\notin A^\times$. 如果存在 $r\in A$, 使得 $ar=1$, 由 *4.8* 可知 $ar=ra=1_A$, 故 $1=(ar)^N=a^Nr^N=0$, 矛盾. 故 $a\notin A^\times$, 即 $\{0\}\subset Spec(a)$.

任取 $\lambda\in\mathbb{C}^\times$,$=ax-\lambda1_A$ 有逆 $\lambda(1+\frac{a}{\lambda}+(\frac{a}{\lambda})^2+\ldots+(\frac{a}{\lambda})^N$. 这表明 $a-\lambda1_A\in A^\times$, $\forall\lambda\in\mathbb{C}^\times$, 即 $\lambda\notin Spec(a)$.

综上 $Spec(a)=\{0\}$. ♢

4.7 若 $Spec(a)=\{0\}$, 证明 a 为幂零的.

♣ 由于 $Spec(a)$ 为有限集, 故 a 一定满足 *4.1* 的假设, 由 *4.2* 知存在正次数的多项式 $P\in\mathbb{C}[X]$ 使得 $P(a)=0$, 记 $P(x)=(x-x_1)\cdot\ldots\cdot(x-x_n)$. 由 $P(a)=0$, 且 $(a-x_i)$

两两交换, 可知对 $1 \leq i \leq n$, 均有 $(a - x_i)$ 不可逆, 即 $x_i \in Spec(a) = \{0\}, \forall 1 \leq i \leq n$. 故 $P(a) = a^n = 0$, 即 a 为幂零元. ♢

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 $ab = 1_A$.)

♣ 若 $a \in A$ 有左逆 b, 则映射 $R_a \colon c \mapsto ac$ 为单射. 事实上, 若存在 $c \in A$, 使得 $ac = 0$, 有 $c = (ba)c = b(ac) = 0$. 由 A 为有限维 $\mathbb{C}$-代数, 可知 R_a 为同构, 故对 $1_A \in A$, 存在 $y \in A$ 使得 $ay = 1$, 则 $ab = ab(ay) = a(ba)y = ay = 1$, 即 b 也是 a 的右逆, 从而是双边逆. ♢

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 λ. 以下两问的目标是证明存在 A-单模 S 使得 $a \cdot S \neq 0$.

♣ 这不是题目, 只是一个承接. 保留这个小问是为了和法文试卷题号保持一致. ♢

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

♣ 由 $\lambda \in Spec(a)$, 知 $1_A \notin A \cdot (a - \lambda 1_A)$, 故 $N = A/A \cdot (a - \lambda 1_A) \neq 0$. 由 A 为有限维 $\mathbb{C}$-代数, 取其一组 $\mathbb{C}$-线性基 $c_1, \ldots, c_n$, 则 $c_1, \ldots, c_n$ 在映射 $\phi \colon A \mapsto A/A \cdot (a - \lambda 1_A)$ 下的像自然是 $N = A/A \cdot (a - \lambda 1_A)$ 的一组生成元. ♢

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 $a \cdot S \neq 0$.

♣ 由课堂结论, 取 S 为 N 的一个单的商模, 则 $S \simeq N/M$, 这里 M 是 N 的一个子模. 那么 $a \cdot S \simeq a \cdot N/M = a \cdot A/(a - \lambda 1_A, M) \simeq \lambda \cdot A/M$. 但 $A/N \neq 0$, 故 $A/M \neq 0$, 从而 $a \cdot S \simeq \lambda \cdot A/M \neq 0$. ♢

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 $[L:k]=[L:K][K:k]$.

♣ 设 L 作为 K 线性空间的一组基是 $l_1,\dots,l_n$, K 作为 k 的线性空间的一组基是 $e_1,\dots,e_m$, 那么可以验证 $l_ie_j, 1\le i\le n, 1\le j\le m$ 构成了 L 作为 k 线性空间的一组基. ♢

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

♣ 考虑 $\sqrt[5]{2}$ 在 Q 的极小多项式是 x^5-2, 故若记 $t=\sqrt[5]{2}$, 则 $1,t,t^2,t^3,t^4$ 是 $\mathbb{Q}(\sqrt[5]{2})$ 作为 $\mathbb{Q}$-线性空间的一组基. 故 $[\mathbb{Q}(\sqrt[5]{2}):\mathbb{Q}]=5$. ♢

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

♣ 考虑中间域 $\mathbb{Q}(\sqrt{5})$, 首先有 $[\mathbb{Q}(\sqrt{5}):\mathbb{Q}]=2$. 其次, $\sqrt[5]{2}$ 在 $\mathbb{Q}(\sqrt{5})$ 上的极小多项式应该是 x^5-2 的因式. 但

$$x^5-2=(x-\sqrt[5]{2})(x-\sqrt[5]{2}\zeta)(x-\sqrt[5]{2}\zeta^2)(x-\sqrt[5]{2}\zeta^3)(x-\sqrt[5]{2}\zeta^4),$$

这里 ζ 是五次本原单位根. 可以看出这里并不能组合出 $\mathbb{Q}(\sqrt{5})[x]$ 中的因式, 故 $\mathbb{Q}(\sqrt[5]{2})$ 在 $\mathbb{Q}(\sqrt{5})$ 上的极小多项式仍然是 x^5-2. 因此

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

♢

注: 也可以直接利用习题 1的这个关系, 说明这个扩张次数是 2 和 5 的倍数, 同时又不超过 10, 因此只能是 10.

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

♣ 仿照*2*即可. ♢

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 $K(h)\simeq K(x)$.

♣ 不妨设 h 首一. 设 $h=\dfrac{g(x)}{m(x)}$, 其中 $g(x),m(x)\in K[x]$ 互素且首一. 若存在 $0\neq f\in K[X]$, 使得 $f(h)=0$, 设 $f(x)=\sum\limits_{i=0}^{n}a_ix^i$, 将 $f(h)=f(\dfrac{g(x)}{m(x)})=0$ 通分, 即得 $\sum\limits_{i=0}^{n}a_i(g(x))^i(m(x))^{n-i}$. 如果 $\deg g\neq\deg m$, 考察左侧的最高次项系数, 可知这就是 f 的最高次项系数 (若 $\deg g>\deg m$) 或 f 的最低次项系数 (若 $\deg g<\deg m$). 由 $f(h)=0$, 知这二者之一为 0, 自然矛盾 ("最高" 或 "最低" 的预设就已经蕴含了这两个系数不为 0). 如果 $\deg g=\deg m>0$, 考察通分后的式子, 可见 $m|g$, 矛盾. 因此 $\forall\ 0\neq h\in K(x),\forall\ 0\neq f(x)\in K[x]$, 均有 $f(h)\neq 0$. 因此 $\varphi\colon K(x)\to K(h),x\mapsto h$ 是域同构 (既单且满). ♢

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

♣ 将 $K(x)$ 看作由 $K(f(x))$ 添加代数元 x 得到的域. 考虑环同态 $\varphi\colon K(f(x))[y]\to K(x),y\mapsto x$, 则 $\ker\varphi$ 是主理想, 不妨设为 (g), 其中 g 的系数在 $K(f(x))$ 中. 如果 $\deg f=1$, 那么命题显然成立. 考虑 $\deg f>1$, 则 $\deg g$ 一定大于 1, 否则 $x\in K(x)$, 矛盾. 此时若 g 的系数中没有 $f(x)$(即 g 的各项系数作为 $K(f(x))$ 中的元素落在 K 中), 则 $\varphi(g(y))=0\in K(x)$, 说明 $g(x)=0\in K[x]$, 故 $g=0\in K[y]$, 这导致 $K(x)=K(f(x))$, 矛盾. 故 g 的系数中一定出现 $f(x)$. 将 $\varphi(g(y))=0$ 通分. 考虑通分后得到的式子, 可以写成 $\sum\limits_{i=0}^{\deg g}h_i(f(x))x^i=0$, 其中 $h_i\in K[x]$. 若 $\deg g=:a<\deg f=:b$, 对 $0\leq i<j\leq a$, $h_i(f(x))x^i$ 中出现的项与 $h_j(f(x))x^j$ 中出现的项不可能次数相等, 因为 $\bmod b$ 不同余.

这表明 $h_i = 0,\ \forall 0 \le i \le a$. 但考察通分过程, 这显然不可能, 所以一定有 $\deg g \ge \deg f$. 另一方面, 取 $h(y) = f(y) - f(x)$, 有 $\deg h = \deg f, h(x) = 0$, 因此 $\ker(\varphi) = (h)$, 故 $[K(x) : K(f(x))] = \deg h = \deg f$. ♢

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 $[K(x) : K(h(x))] = max\{\deg f, \deg g\}$.

♣ 不妨设 $\deg f \ge \deg g$(否则取 $K(\dfrac{1}{h}(x)) = K(h(x))$. 同样考虑 φ: $K(h(x))[y] \to K(x),\ y \mapsto x$. 设 $\ker(\varphi) = (p)$, 类似 *2* 中讨论可知 $p \in K(h(x))[y] \backslash K[y]$. 先将 $\varphi(g(y)) = 0$ 通分, 可得: $\sum\limits_{i=0}^{\deg p} s_i(h(x))x^i$, 其中 $s_i \in K[x]$. 记 $max_{0 \le i \le \deg p}\ \{\deg s_i\} = t > 0$, 将分子同乘 $g(x)^t$ 通分. 若 $\deg p < \deg f$, 则分子中所有满足 $\deg s_i = t > 0$ 的项的次数都严格高于其余项. 取这些项中对应 i 次数最大的那项, 可见这项中 x 的次数即为通分后左侧整式关于 x 的次数, 但其前系数不为 0, 矛盾. 因此 $\deg p \ge \deg f$. 又有: 取 $p(y) = g(x)f(y) - f(x)g(y)$, 则 $\varphi(p) = 0$, 且 $\deg p = \deg f$. 因此 $\ker(\varphi) = (p)$, 故 $[K(x) : K(h(x))] = \deg p = \deg f = max\{\deg f, \deg g\}$. ♢

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 $[L:k]=[L:K][K:k]$.

♣ 见讲义 2022-04-27习题 1. ♢

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

♣ 记 $[\mathbb{Q}(\sqrt[5]{2},\sqrt{5}):\mathbb{Q}]=n$. 因为 $[\mathbb{Q}(\sqrt[5]{2}):\mathbb{Q}]=5$ 且 $[\mathbb{Q}(\sqrt{5}):\mathbb{Q}]=2$, 从而 $5|n, 2|n$, 故 $10|n$. 又由于显然 $n\leq 10$, 知 $n=10$. ♢

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 $[E:F]=\deg f$.

♣ 考虑环同态 $F[x]\to F(\alpha), x\mapsto\alpha$. 则 $\ker=(f)$, 可见 $1,\alpha,\ldots,\alpha^{\deg f-1}$ 恰好构成了 E 的一组 F-基. 因此 $[E:F]=\deg f$. ♢

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 $K(h)\simeq$

$K(x)$.

♣ 见讲义 2022-04-27 习题 3.*1*. ♢

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

♣ 见讲义 2022-04-27 习题 3.*2*. 或记 $y = f(x)$, 令 $g(T) = f(T) - y \in K(y)[T]$, 只需证明 $g(T)$ 为 $K(y)[T]$ 中不可约多项式. 为此, 注意到 $g(T)$ 在 $K[y][T] = K[y, T] = K[T][y]$ 中不可约即可 (Gauss 引理). ♢

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 $[K(x) : K(h(x))] = max\{\deg f, \deg g\}$.

♣ 见讲义 2022-04-27 习题 3.*3*. 或记 $y = h(x)$, 令 $p(T) = g(T)y - f(T) \in K(y)[T]$. 只需证明 $p(T)$ 为 $K(y)[T]$ 中不可约多项式. 为此, 注意到 $p(T)$ 在 $K[y][T] = K[y, T] = K[t][y]$ 中不可约即可 (Gauss 引理). ♢

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 $R_{P_i} \simeq K_i,\ P_i R_{P_i} = 0, \forall i = 1, \ldots, n$.

♣ 见讲义 2022-03-16习题 3. ♢

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.

♣ 由于 f 无重根, $F[x]/(f(x)) \simeq F[x]/(x - x_1) \ldots (x - x_n) \simeq \prod_{i=1}^{n} F[x]/(x - x_i) \simeq \prod_{i=1}^{n} F$. ♢

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 $P_i B_{P_i} = pB_{P_i}$ 由 p 的像生成, p 为 DVR B_{P_i} 中相伴意义下的唯一素元.

♣ 包含 (p) 的素理想对应到 B/pB 的素理想, 后者由 *1* 知恰有 n 个, 且局部环 B_{P_i} 为 DVR. 由我们在讲义 2022-03-09习题 7中所证明的局部化与商交换:$(B/(p)B)_{\bar{P}_i} \simeq B_{P_i}/(p)B_{P_i}$, 前者是域, 故后者也是域, 故 $(p)B_{P_i} \subset B_{P_i}$ 为极大理想. 故 $(p)B_{P_i} = P_i B_{P_i}$ 为 B_{P_i} 中极大理想, 且 $P_i B_{P_i}/(p) \subsetneq B_{P_i}/(p) \simeq (B/(p))_{\bar{P}_i}$, $(B/(p))_{\bar{P}_i}$ 是域, 故 $P_i B_{P_i}/(p) = 0$, 即有 $P_i B_{P_i} = (p)$ 为主理想. 由 DVR 的性质我们知道 p 的像即为 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. $K = F(\zeta_q)$.

♣ 首先有 $F(\zeta_q) \subset K$. 由于 p, q 为不同素数, 存在合适的 $a, b \in \mathbb{Z}$, 使得 $\zeta_p^a \zeta_q^b =$

ζ_{pq}(相当于 $aq+bp\equiv 1(mod\ pq)$, 可以先选择 a 使得 $aq\equiv 1(mod\ p)$, 这样 $aq=kp+1$, 再选 $b=q-k$ 即可). 因此 $K\subset F(\zeta_q)$. 故 $K=F(\zeta_q)$. ♢

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

♣ 由 *1* 知 $[K:F]=[F(\zeta_q):F]$. 考虑环 $\mathbb{Z}[\zeta_p]_P$, 其中 P 是 $\mathbb{Z}[\zeta_p]$ 中一个位于 q 上方的素理想. 那么由例 2可知 $\mathbb{Z}[\zeta_p]_P$ 是 DVR, 特别地, 是 UFD, 且 q 为其中素元, 并且满足 $Frac(\mathbb{Z}[\zeta_p]_P)=\mathbb{Q}(\zeta_p)$. 考虑 ζ_q 在环 $\mathbb{Z}[\zeta_p]_P$ 上的零化多项式 $\Phi_q(x)=\dfrac{x^q-1}{x-1}=1+x+\ldots+x^{q-1}$, 对 $\Phi_q(x+1)$ 用 Eisenstein 判别法可知其不可约, 从而 $f(x)$ 在 $\mathbb{Z}[\zeta_p]_P$ 上不可约. 又因为其本原, 由 Gauss 引理知其在 $Frac(\mathbb{Z}[\zeta_p]_P)=\mathbb{Q}(\zeta_p)$ 上不可约, 故 ζ_q 在 $\mathbb{Q}(\zeta_p)$ 上的极小多项式就是 $\Phi_q(x)$. 因此 $[K:F]=\deg f=\varphi(q)=q-1$. ♢

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

♣ 由公式直接得到 $[K:\mathbb{Q}]=[K:F][F:\mathbb{Q}]=(p-1)(q-1)=\varphi(pq)$. ♢

习题 **6.** 设 N 为正整数, $N=p^mN_1$, 其中 p 为素数, $(p,N_1)=1$. 证明:

1. $[\mathbb{Q}(\zeta_{p^m}):\mathbb{Q}]=\varphi(p^m)=p^m-p^{m-1}$.

♣ 考虑多项式 $\Phi_{p^m}(x)=\dfrac{x^{p^m}-1}{x^{p^{m-1}}-1}$. 首先 $\Phi_{p^m}(x)$ 是 ζ_{p^m} 的零化多项式. 再由我们在讲义 2022-03-16 习题 5.4中已证明 $\Phi_{p^m}(x)$ 是不可约多项式, 因此 ζ_{p^m} 在 $\mathbb{Q}$ 上的极小多项式就是 $\Phi_{p^m}(x)$. 故 $[\mathbb{Q}(\zeta_{p^m}):\mathbb{Q}]=\deg\Phi_{p^m}=\varphi(p^m)=p^m-p^{m-1}$. ♢

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

♣ 考虑环同态 $\mathbb{Z}\to\mathbb{Z}[\zeta_{N_1}]$. 令 $B=\mathbb{Z}[x]/(x^{N_1}-1)$, 则商环 $\mathbb{Z}[\zeta_{N_1}]/(p)$ 自然为 $B/(p)$ 的商环, 而 $B/(p)\simeq\mathbb{F}_p[x]/(\bar{x}^{N_1}-1)$ 为有限个域的乘积 (因为 $(N_1,p)=1$ 推导出 $x^{N_1}-1$ 在 F_p 中无重根), 从而其商环 $\mathbb{Z}[\zeta_{N_1}]/(p)$ 也为有限个域的乘积. 任取 $\mathbb{Z}[\zeta_{N_1}]$ 中位于 p 上方的素理想 P, 则 $\mathbb{Z}[\zeta_{N_1}]_P$ 为 DVR, $Frac(\mathbb{Z}[\zeta_{N_1}]_P)=\mathbb{Q}(\zeta_{N_1})$, 且 p 为其素元. 在环

$\mathbb{Z}[\zeta_{N_1}]_P$ 中对 $\Phi_{p^m}(x+1)$ 用 Eisenstein 判别法, 可知 $\Phi_{p^m}(x)$ 为 $\mathbb{Z}[\zeta_{N_1}]_P$ 中不可约多项式, 再由 Gauss 引理知其为 $\mathbb{Q}(\zeta_{N_1})$ 上的不可约多项式, 因而是 ζ_{p^m} 的极小多项式, 从而有 $[K(\zeta_{p^m}):K]=\deg\Phi_{p^m}=\varphi(p^m)=p^m-p^{m-1}$. ♢

3. $\mathbb{Q}(\zeta_N)=\mathbb{Q}(\zeta_{N_1})(\zeta_{p^m})$.

♣ 仿照习题 5.*1*即可. 注意我们在习题 5.*1* 里只是利用了 p 和 q 互素, 而没有用 p 和 q 都是素数. ♢

4. $[\mathbb{Q}(\zeta_N):\mathbb{Q}]=\varphi(N)$.

♣ $[\mathbb{Q}(\zeta_N):\mathbb{Q}]=[\mathbb{Q}(\zeta_N):\mathbb{Q}(\zeta_{N_1})][\mathbb{Q}(\zeta_{N_1}):\mathbb{Q}]=\varphi(p^m)[\mathbb{Q}(\zeta_{N_1}):\mathbb{Q}]$. 再利用 *3* 归纳, 将 N_1 继续进行素因子分解, 容易得到 $[\mathbb{Q}(\zeta_N):\mathbb{Q}]=\varphi(N)$. ♢

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

♣ 考虑中间域 $\mathbb{Q}(\sqrt{5})$. 注意其子环 $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]\simeq\mathbb{Z}[x]/(x^2+x-1)$, 那么 $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]/(2)\simeq\mathbb{F}_2[x]/(x^2+x-1)$, 是域. 故类似我们前面所做, 考虑环同态 $\mathbb{Z}\to\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ 下 (2) 上方的素理想 P. 有 $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]_P$ 为 DVR, 且 2 为其中素元. 在这个环上对 $f(x)=x^4-2$ 用 Eisenstein 判别, 可知 $f(x)$ 不可约, 进而由 Gauss 引理知 $f(x)$ 在 $Frac(\mathbb{Z}[\frac{1+\sqrt{5}}{2}]_P)=\mathbb{Q}(\sqrt{5})$ 上不可约, 所以 $f(x)$ 是 $\sqrt[4]{2}$ 在 $\mathbb{Q}(\sqrt{5})$ 上的极小多项式, 因此 $[\mathbb{Q}(\sqrt[4]{2},\sqrt{5}):\mathbb{Q}]=[\mathbb{Q}(\sqrt[4]{2}:\sqrt{5}),\mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}):\mathbb{Q}]=4\times2=8$. ♢

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

♣ 考虑中间域 $\mathbb{Q}(\sqrt{2})$, 由于 $\sqrt{2+\sqrt{2}}\notin\mathbb{Q}(\sqrt{2})$(设 $\sqrt{2+\sqrt{2}}=a+b\sqrt{2}$, 其中 $a,b\in\mathbb{Q}$, 可得 $2+\sqrt{2}=a^2+2b^2+2ab\sqrt{2}$, 故 $a^2+2b^2=2,2ab=1$, 解出 $a\notin\mathbb{Q}$, 矛盾), 立知 $[\mathbb{Q}(\sqrt{2+\sqrt{2}}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2+\sqrt{2}}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=4$ ♢

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

♣ $\sqrt[3]{2+\sqrt{3}}$ 在 $\mathbb{Q}$ 上有零化多项式 $f(x)=(x^3-2)^2-3=x^6-4x^3+1$. 对 $f(x+2)=x^6+12x^5+60x^4+156x^3+210x^2+192x+33$ 用 Eisenstein 判别, 可知 $f(x+2)$ 在 $\mathbb{Q}[x]$ 中不可约, 故 $[\mathbb{Q}(\sqrt[3]{2+\sqrt{3}}):\mathbb{Q}]=\deg f=6.$ ♢

注: 也可以考虑中间域 $\mathbb{Q}(\sqrt{3})$. 由于 $\mathbb{Z}[\sqrt{3}]$ 是 Euclide 环. 那么 $\sqrt{3}$ 是 $\mathbb{Z}[\sqrt{3}]$ 上的不可约元, 因而是素元. 由于 $\sqrt[3]{2+\sqrt{3}}$ 在 $\mathbb{Q}(\sqrt{3})$ 上有零化多项式 $g(x)=x^3-2$, 对 $g(x-1)=x^3-3x^2+3x-3-\sqrt{3}$ 用 Eisenstein 判别, 可知 $g(x)$ 是 $\mathbb{Z}[\sqrt{3}]$ 上的不可约多项式, 因此 $[\mathbb{Q}(\sqrt[3]{2+\sqrt{3}}):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2+\sqrt{3}}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2\deg g=6.$

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 $K \simeq \mathbb{Q}(\sqrt{n})$.

♣ 任取 $K\backslash\mathbb{Q}$ 中元素 u, 则 $\mathbb{Q} \subseteq \mathbb{Q}(u) \subseteq K$, 由扩张次数知只能有 $\mathbb{Q}(u)/\mathbb{Q}$ 为二次扩张, 即 $K = \mathbb{Q}(u)$. 于是 u 在 $\mathbb{Q}$ 上有极小多项式 $(x+a)^2 + \dfrac{l}{m}$, 其中 $a \in \mathbb{Q}$, $l, m \in \mathbb{Z}$ 互素. 由于 $\mathbb{Q}(u) = \mathbb{Q}(m(u+a))$, 不妨用 $mu + a$ 替换 u, 即可假定极小多项式为 $x^2 + lm$, 此时知 $u^2 = -lm \in \mathbb{Z}$, 即 $K = \mathbb{Q}(\sqrt{-lm})$. 记 $n = -ml$, 若 n 有平方因子, 即 $n = p^2 s$, 则 $\sqrt{n} = p\sqrt{s}$ 可在 $\mathbb{Q}$ 上互相生成, 故 $K = \mathbb{Q}(\sqrt{s})$, 将其约化至无平方因子即可. ♢

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

♣ 由 *1.* 知 $1, \sqrt{n}$ 构成 K 的一组 $\mathbb{Q}$-基. 故 $\forall \alpha \in K$ 有 $\alpha = \dfrac{p_1}{q_1} + \dfrac{p_2}{q_2}\sqrt{n}$(假定分数均既约). 若存在 $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ 零化 α, 则代入有 $\left(\dfrac{p_1^2}{q_1^2} + \dfrac{np_2^2}{q_2^2} + \dfrac{ap_1}{q_1} + b\right) + \left(\dfrac{2p_1p_2}{q_1q_2} + \dfrac{ap_2}{q_2}\right)\sqrt{n} = 0$, 于是两系数分别为 0, 即 $p_1^2q_2^2 + np_2^2q_1^2 + ap_1q_1q_2^2 + bq_1^2q_2^2 = 0$, $(2p_1 + aq_1)p_2 = 0$. 若 $p_2 = 0$, 即 $p_1^2 + ap_1q_1 + bq_1^2 = 0$, 由整除性立即得到 $q_1 = 1$, 即 $\alpha \in \mathbb{Z}$. 若 $p_2 \neq 0$, 第一个等式除第二项外均含 q_2^2, 又有 $(p_2, q_2) = 1$, 故 $q_2^2 | nq_1^2$. 由于 n 无平方因子, 只能有 $q_2 | q_1$. 再假定 $q_1 = kq_2$, 原等式约化为 $p_1^2 + nk^2p_2^2 + akq_2 + bk^2q_2^2 = 0$, $2p_1 + aq_1 = 0$. 两式依次给出 $k | p_1^2$ 及 $q_1 | 2$. 由于 $(p_1, q_1) = 1$, 只能有 $k = \pm 1$, 且 $q_2\alpha = kp_1 + p_2\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, 故 $\mathcal{O}_K \subseteq \mathbb{Z}\left[\dfrac{1+\sqrt{n}}{2}\right]$. 若 $n \equiv 1 \mod 4$, 则 $n = 4k + 1$, 有 $x^2 - x + k$ 为 $\dfrac{1+\sqrt{n}}{2}$ 的零化多项式, 故 $\dfrac{1+\sqrt{n}}{2} \in \mathcal{O}_K$, 即 $\mathcal{O}_K = \mathbb{Z}\left[\dfrac{1+\sqrt{n}}{2}\right]$. 若 $n \equiv 2, 3 \mod 4$, 则由前面两等式有 $0 = p_1^2 + nk^2p_2^2 + aq_1 + bk^2q_2^2 = p_1^2 + np_2^2 - 2p_1 + bq_2^2$.

若 $q_2=\pm 2$, 等式 mod 4 得到 $p_1^2+np_2^2+2p_1=0$, 且此时 p_1,p_2 需与 2 互素, 为奇数, 故 $n+1+2=0$, 矛盾, 故 $q_2=\pm 1$. 此时 $\dfrac{p_1}{q_1},\dfrac{p_2}{q_2}$ 均为整数, 故 $\mathcal{O}_K\subseteq\mathbb{Z}[\sqrt{n}]$. 另一方面,$\sqrt{n}$ 有零化多项式 x^2-n, 故 $\sqrt{n}\in\mathcal{O}_K$, 从而 $\mathcal{O}_K=\mathbb{Z}[\sqrt{n}]$. ♢

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.

♣ $\mathcal{O}_K$ 中位于 (p) 上方的素理想含有 p, 反之, 若一个素理想含有 p, 其与 $\mathbb{Z}$ 的交为 $\mathbb{Z}$ 的素理想, 且含有 p, 故只能为 (p), 因而只需分析 $\mathcal{O}_K$ 中含 p 的素理想. 记 $(p)_K=p\mathcal{O}_K$ 为 p 在 $\mathcal{O}_K$ 中生成的主理想, 则由对应定理只需分析商环 $\mathcal{O}_K/(p)_K$ 的素理想. 由前一问结论, 当 $n=4l+1$ 时, $\mathcal{O}_K=\mathbb{Z}\left[\dfrac{1+\sqrt{n}}{2}\right]\simeq\mathbb{Z}[x]/(x^2-x-l)$, 当 $n=4l+2$ 或 $4l+3$ 时, $\mathcal{O}_K=\mathbb{Z}[\sqrt{n}]\simeq\mathbb{Z}[x]/(x^2-n)$, 均形如 $\mathbb{Z}[x]/(f(x))$. 则 $\mathcal{O}_K/(p)_K\simeq\mathbb{Z}[x]/(f(x),p)\simeq(\mathbb{Z}/(p))[x]/(f(x))\simeq\mathbb{F}_p[x]/(f(x))$, 于是只需在 $\mathbb{F}_p$ 上分析 f.

首先考虑当 $p\neq 2$ 时的情况. 对 $n\equiv 1 \mod 4$ 的情形, 在 $\mathbb{F}_p$ 上有 $f(x)=x^2-x-l=x^2+2\dfrac{p-1}{2}x-l=\left(x+\dfrac{p-1}{2}\right)^2-l-\dfrac{(p-1)^2}{4}=\left(x+\dfrac{p-1}{2}\right)^2-l-\dfrac{1}{4}=\dfrac{1}{4}((2x-1)^2-n)$. 当 n 是模 p 的二次剩余时 f 在 $\mathbb{F}_p$ 中有根, 分解为一次多项式的乘积, 且 $f'(x)=2x-1$, 由 $\dfrac{1}{2}$ 不为根知 f 无重根, 故 $\mathbb{F}_p[x]/(f)\simeq\mathbb{F}_p\times\mathbb{F}_p$. 这是有限个域的乘积, 它有两个素理想, 这给出 $\mathcal{O}_K$ 中两个含 p 的素理想; 当 n 不是模 p 的二次剩余时, f 在 $\mathbb{F}_p$ 上不可约, 此时 $\mathbb{F}_p[x]/(f)$ 是域, 仅有一个素理想, 这给出 $\mathcal{O}_K$ 唯一含有 p 的素理想, 即该同态的核, 也即 $(p)_K$. 对 $n\equiv 2,3 \mod 4$ 的情形, 作类似分析, 只需考虑 $f(x)=x^2-n$ 在 $\mathbb{F}_p$ 上的根的状况, $f(x)$ 无重根, 在 $\mathbb{F}_p$ 上有根当且仅当 n 是 $\mod p$ 的二次剩余, 与前一情形结论一致.

而 $p=2$ 时, 若 $n\equiv 1 \mod 4$, 考虑 $n=4l+1$, 若 l 为奇数, 则 f 在 $\mathbb{F}_2$ 上不可约, 此时

(2) 上方有一个素理想; 若 l 为偶数, 则 $f(x)=x^2+x=x(x+1)$, $\mathbb{F}_2[x]/(f)\simeq\mathbb{F}_2\times\mathbb{F}_2$, 此时 (2) 上方有两个素理想. 若 $n\equiv 2,3 \mod 4$, 则 $f(x)=(x-n)^2$ 有重根, 此时 $\mathbb{F}_2[x]/(f)=\mathbb{F}_2[x]/(x-n)^2$ 的素理想对应到 $\mathbb{F}_2[x]$ 的包含 $(x-n)^2$ 的素理想, 由素理想定义以及 $\mathbb{F}_2[x]$ 为 PID 知这样的理想是含有 $x-n$ 的主理想, 故只有 $(x-n)$, 从而 $\mathbb{F}_2[x]/(f)$ 有唯一的素理想, 这对应到 $\mathcal{O}_K$ 中为 $(2,\sqrt{n}-n)$.

于是, $\mathcal{O}_K$ 中位于 p 上方的素理想在 $p=2$ 且 n 模 8 余 1 的时候, 或 n 是模 p 的二次剩余时有两个, 其余时候时仅有一个. 另一方面, $\mathbb{Z}\to\mathcal{O}_K$ 为整扩张, 由讲义 2022-03-14 习题 2.3., $\mathcal{O}_K$ 的非零素理想交 $\mathbb{Z}$ 均非零, 故均位于某个 (p) 上方, 于是这也给出了 $\mathcal{O}_K$ 的所有素理想. 由讲义 2022-03-16习题 3知 f 在 $\mathbb{F}_p$ 上无重根时, $\mathbb{Z}[x]/(f)$ 在 (p) 上方的任何素理想处做局部化得到离散赋值环, 相应的主理想由 p 生成. 结合以上讨论, 只需再考虑 $p=2$ 且 $n\equiv 2,3 \mod 4$ 的情况. 此时 $\mathcal{O}_K=\mathbb{Z}[\sqrt{n}]$, 且以上已经算出该素理想为 $(2,\sqrt{n}-n)$, 将其记作 $\mathfrak{P}$. 当 $n\equiv 2 \mod 4$ 时, $\mathfrak{P}=(2,\sqrt{n})$, 且 $\dfrac{n}{2}$ 为奇数. 由 $\mathfrak{P}\cap\mathbb{Z}=(2)$ 知奇数不在 $\mathfrak{P}$ 中, 这说明 $\dfrac{n}{2}$ 在 $\mathcal{O}_{K,\mathfrak{P}}$ 中为可逆元, 也即 $\dfrac{2}{n}\in\mathcal{O}_{K,\mathfrak{P}}$. 进而在 $\mathcal{O}_{K,\mathfrak{P}}$ 中有 $2=\sqrt{n}\cdot\dfrac{2\sqrt{n}}{n}$, 而原本 $\mathfrak{P}\mathcal{O}_{K,\mathfrak{P}}$ 能被 2 和 $\sqrt{n}$ 生成, 现在给出 2 能被 $\sqrt{n}$ 生成, 于是 $\mathfrak{P}\mathcal{O}_{K,\mathfrak{P}}$ 为 $\sqrt{n}$ 生成的主理想. 从而 $\mathcal{O}_{K,\mathfrak{P}}$ 为离散赋值环. 当 $n\equiv 3 \mod 4$ 时, $\mathfrak{P}=(2,\sqrt{n}+1)$. 同样考虑 $\dfrac{n-1}{2}$ 为奇数, 以及 $2=(\sqrt{n}+1)\dfrac{2(\sqrt{n}-1)}{n-1}$ 知 2 在 $\mathcal{O}_{K,\mathfrak{P}}$ 中被 $\sqrt{n}+1$ 生成, 进而也得到 $\mathcal{O}_{K,\mathfrak{P}}$ 为离散赋值环.

Noether 性和整性都是易见的, 综合以上讨论知 $\mathcal{O}_K$ 为 Dedekind 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.

♣ 由定义 Φ_N 为 ζ_N 在 $\mathbb{Q}$ 上的极小多项式, 故 $\mathbb{Q}[\zeta_N]\simeq\mathbb{Q}[x]/(\Phi_N(x))$, 进而利用

Gauss 引理交到 $\mathbb{Z}[x]$ 上即得 $\mathbb{Z}[\zeta_N] \simeq \mathbb{Z}[x]/(\Phi_N(x))$. 在讲义 2022-03-16习题 5已经证明了 $N = p^n$ 的情形. 对于一般的 N, 我们将 $X^N - 1$ 在 $\mathbb{C}$ 上分解得到 $\prod_{i=0}^{N-1}(X - \zeta_N^i)$. 而依定义 $\Phi_N(X) = \prod_{\gcd(k,N)=1}(X - \zeta_N^k)$, 且 ζ_N^i 为 $\dfrac{N}{\gcd(i,N)}$ 次本原单位根. 这给出等式 $X^N - 1 = \prod_{d|n}\Phi_d(X)$. 对给定素数 p, 我们假设 $N = mp^n$, 其中 m 与 p 互素, 则可进一步写成 $X^N - 1 = \prod_{d|m}\prod_{i=0}^{n}\Phi_{dp^i}(X)$. 以下我们对 N 归纳证明在 $\mathbb{F}_p$ 中有 $\Phi_N = (\Phi_m)^{p^n - p^{n-1}}$(当 $n = 0$ 时指数替换为 1). 当 $m = 1$ 或 $n = 0$ 时结论自然成立. 假设对所有 $s \leq N - 1$, 该结论成立, 而我们有

$$
\begin{aligned}
(X^m - 1)^{p^n} &= \left(\prod_{d|m}\Phi_d\right)^{p^n} \\
&= \Phi_m^{p^n}\prod_{d|m,d\neq m}\Phi_d^{p^n - p^{n-1}}\Phi_d^{p^{n-1} - p^{n-2}}\cdots\Phi_d^{p^1 - p^0}\Phi_d \\
&= \Phi_m^{p^n}\prod_{d|m,d\neq m}\Phi_{dp^n}\Phi_{dp^{n-1}}\cdots\Phi_{dp}\Phi_d \\
&= \Phi_m^{p^n}\prod_{d|m,d\neq m}\prod_{i=0}^{n}\Phi_{dp^i} \\
X^N - 1 &= \prod_{d|m}\prod_{i=0}^{n}\Phi_{dp^i} \\
&= \left(\prod_{i=0}^{n}\Phi_{mp^i}\right)\prod_{d|m,d\neq m}\prod_{i=0}^{n}\Phi_{dp^i}
\end{aligned}
$$

由于在 $\mathbb{F}_p$ 上我们有 $(X^m - 1)^{p^n} = X^{mp^n} - 1 = X^N - 1$, 比较以上式子我们得到

$$
\Phi_m^{p^n} = \prod_{i=0}^{n}\Phi_{mp^i}, \quad \Phi_m^{p^{n-1}} = \prod_{i=0}^{n-1}\Phi_{mp^i},
$$

其中后一式子由前一式子的 n 替换为 $n - 1$ 得到. 两式相除即得到 $\Phi_N = \Phi_{mp^n} = \Phi_m^{p^n - p^{n-1}}$. 现在由于 m 与 p 互素, 故 $\Phi_m(x)$ 在 $\mathbb{F}_p$ 上无重根 (因为 $x^m - 1$ 无重根), 我们

假设 Φ_m 在 $\mathbb{F}_p$ 上的不可约分解为 $f_1\cdots f_t$, 则 $\mathbb{F}_p[x]/(\Phi_N)\simeq\prod_{i=1}^{t}\mathbb{F}_p[x]/(f_i^{p^n-p^{n-1}})$, 每个分量均有且仅有一个素理想, 这将给出 $\mathbb{Z}[\zeta_N]/(p)$ 有 t 个素理想 (环乘积 $A_1\times\cdots\times A_t$ 的素理想均形如 $A_1\times\cdots A_{i-1}\times P_i\times A_{i+1}\times\cdots\times A_t$, 其中 P_i 为 A_i 的素理想), 且第 i 个素理想 $\mathfrak{p}_i$ 由 $(1,\cdots,f_i,\cdots,1)$ 生成, 由于各 f_i 互不相同, 故两两互素, 故也由 $(f_i,f_i,\cdots,f_i)$ 生成, 这对应回 $\mathbb{F}_p[x]/(\Phi_N)$ 中相应的素理想生成元即 $f_i(x)$. 我们记 $F_i(x)$ 为 $(f_i,\cdots,f_i)$ 在 $\mathbb{Z}[x]\to\mathbb{Z}[x]/(p,\Phi_N(x))\simeq\prod_{i=1}^{t}\mathbb{F}_p[x]/(f_i^{p^n-p^{n-1}})$ 下的一个原像, 并记 $\mathfrak{P}_i$ 为 $\mathbb{Z}[\zeta_N]$ 中与 $\mathfrak{p}_i$ 对应的素理想, 则 $F_i(\zeta_N)$ 即为 $\mathfrak{P}_i$ 的另一个生成元, 也即 $\mathfrak{P}_i=(p,F_i(\zeta_N))$. 我们有 $\mathbb{Z}[\zeta_N]/\mathfrak{P}_i=\mathbb{Z}[x]/(p,\Phi_N,F_i(x))=(\mathbb{F}_p[x]/(\Phi_N))/\mathfrak{p}_i=\mathbb{F}_p[x]/(f_i)$ 为域, 故 $\mathfrak{P}_i$ 为 $\mathbb{Z}[\zeta_N]$ 的极大理想. 另一方面,$Z[\zeta_N]$ 在 $\mathbb{Z}$ 上整, 其位于 (p) 上方的素理想均形如 $\mathfrak{P}_i$, 位于 (0) 上方的素理想只有 (0), 故 $\mathbb{Z}[\zeta_N]$ 的所有非零素理想极大. 设 $A=\mathbb{Z}[\zeta_N]_S$ 为 $\mathbb{Z}[\zeta_N]$ 的任意一个局部化, 且有 A 中两个有包含关系的素理想 $P_1\subseteq P_2$. 则 $P_1\cap\mathbb{Z}[\zeta_N]$ 和 $P_2\cap\mathbb{Z}[\zeta_N]$ 为 $\mathbb{Z}[\zeta_N]$ 的两个素理想, 且有包含关系 $P_1\cap\mathbb{Z}[\zeta_N]\subseteq P_2\cap\mathbb{Z}[\zeta_N]$. 由非零素理想极大知 $P_1\cap\mathbb{Z}[\zeta_N]=(0)$ 或 $P_1\cap\mathbb{Z}[\zeta_N]=P_2\cap\mathbb{Z}[\zeta_N]$. 由讲义 2022-03-09 习题 5.*3.* 知 $P_1=(0)$ 或 $P_1=P_2$. 取 P_1 非零, P_2 为包含其的极大理想即知 A 的非零素理想也均极大.

由于 $\mathbb{Z}[\zeta_N]$ 为 $\mathbb{Z}$ 在 $\mathbb{Q}[\zeta_N]$ 中的整闭包 (此处未证明这件事, 具体证明步骤较长, 可见 [6] 定理 1.12), 故 $\mathbb{Z}[\zeta_N]$ 是整闭的. 再考虑 $A=\mathbb{Z}[\zeta_N]_S$, A 的分式域也为 $\mathbb{Q}[\zeta_N]$. 若 $x\in\mathbb{Q}[\zeta_N]$ 在 A 上整, 则有首一零化多项式给出

$$x^k+\frac{a_{k-1}}{s_{k-1}}x^{k-1}+\cdots+\frac{a_0}{s_0}=0,$$

其中 $a_i\in\mathbb{Z}[\zeta_N]$, $s_i\in S$. 令 $s=s_0s_1\cdots s_{k-1}$, 以上等式乘以 s^k 将得到一个 sx 的 $\mathbb{Z}[\zeta_N]$ 系数的首一零化多项式, 这说明 $sx\in\mathbb{Z}[\zeta_N]$, 故 $x\in A$, 也即 A 是整闭的.

取 $\mathbb{Z}[\zeta_N]$ 的任意素理想 $\mathfrak{P}$ 并考虑局部化 $A = \mathbb{Z}[\zeta_N]_{\mathfrak{P}}$, 则上面结论给出 A 是整闭整环, 所有非零素理想极大, 且是 Noether 局部环 (由 $\mathbb{Z}[\zeta_N]$ 的 Noether 性易见 A 也是 Noether 的). 记 $\mathfrak{m}$ 为 A 的唯一极大理想, 下证 $\mathfrak{m}$ 为主理想, 从而 A 为离散赋值环, 进而证出 $\mathbb{Z}[\zeta_N]$ 为 Dedekind 整环. 若 $\mathfrak{m} = 0$ 则 A 为域, 结论成立. 否则, 取 $a \in \mathfrak{m}\backslash\{0\}$, 则 (a) 为 A 的一个非平凡理想. 考虑根式理想 $\sqrt{(a)}$ 为所有包含 (a) 的素理想之交, 由于 A 非零素理想均极大, 且仅有唯一极大理想, 只能有 $\sqrt{(a)} = \mathfrak{m}$. 由 Noether 性, $\mathfrak{m}$ 作为 A-模有限生成, 取个数最少的一组生成元 $x_1, \cdots, x_e$, 存在 $n \in \mathbb{N}$ 使得 $x_i^n \in (a)\ \forall i$, 于是 $\mathfrak{m}^n \subseteq (a)$. 不妨令 n 为最小的正整数使得 $\mathfrak{m}^n \subseteq (a)$, 即 $\mathfrak{m}^{n-1} \nsubseteq (a)$, 则取 $b \in \mathfrak{m}^{n-1}\backslash(a)$, 由定义知 $\frac{b}{a} \notin A$. 但有 $\frac{b}{a}\mathfrak{m} \subseteq A$. 这是 A 的一个理想, 若为真理想, 则有 $\frac{b}{a}\mathfrak{m} \subseteq \mathfrak{m}$, 于是 $\mathfrak{m}$ 成为 $B = A[\frac{b}{a}]$-模. 由于 $x_1, \cdots, x_e$ 为 $\mathfrak{m}$ 的生成元, 存在 $c_{ij} \in A$ 使得 $\frac{b}{a}x_i = \sum_{j=1}^{e} c_{ij}x_j$. 记 $X = (x_1, \cdots, x_e)^T, P = (c_{ij})$, 上式给出 $PX = \frac{b}{a}X$. 均看作 $A[\frac{b}{a}]$ 系数的矩阵乘法, 于是 $(P - \frac{b}{a}I_e)X = 0$. 左边再乘 $(P - \frac{b}{a}I_e)$ 的伴随矩阵得到 $\det(P - \frac{b}{a}I_e)X = 0$, 由整环将得到 $\det(P - \frac{b}{a}I_e) = 0$. 于是 $\frac{b}{a}$ 被 P 的特征多项式 $\det(P - TI_e)$ 零化, 而 P 系数均在 A 中, 其特征多项式是 A 系数首一多项式, 这说明 $\frac{b}{a}$ 在 A 上整. 由 A 整闭知 $\frac{b}{a} \in A$, 矛盾. 故 $\frac{b}{a}\mathfrak{m}$ 不是真理想, 只能有 $\frac{b}{a}\mathfrak{m} = A \Rightarrow \frac{a}{b} \in A$, $\mathfrak{m} = \frac{a}{b}A = \left(\frac{a}{b}\right)$ 为主理想, 即证所需结论. ♢

注: 事实上, 任意代数整数环 ($\mathbb{Z}$ 在 $\mathbb{Q}$ 的某个有限扩张 K 中的整闭包) 均为 Dedekind 整环. Dedekind 整环的另一等价定义为 1 维 Noether 整闭整环, 其中 1 维即指所有非零素理想极大. 以上证明已经给出了由该定义推出之前的定义的证明.

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.

♣ 设 $x \in K$, 且 x 在 A 上整, 则存在 $a_0, \ldots, a_{n-1} \in A$, 使得 $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$. 由于 A 是 UFD, 存在一组两两互素的素元 p_j, 使得每个 A 中的元素 a 可唯一分解为 $a = u\prod_j p_j^{k_j}$, $u \in A^\times$. 考虑分解 $a_i = u_i \prod_j p_j^{k_{ij}}$, 其中 $u_i \in A^\times$, 且对每个 i, 只有有限个 j 使得 $k_{ij} \neq 0$. 取 x 的一个既约分式形式 $\frac{a}{b}$, 即满足 $\mathrm{pgcd}(a, b) = 1$. 若存在素元 p, 使得 $p|b$, 由 $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ 通分可得 A 中等式:

$$a^n + a_{n-1}a^{n-1}b + \ldots + a_1 a b^{n-1} + a_0 b^n = 0$$

可见 $p|a^n$, 故 $p|a$, 这与我们的假设矛盾, 因此 $b \in A^*$, 即 $x \in A$. 故 UFD 是整闭整环.♢

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.

♣ 将 A 视作 A_m 的子环. 由讲义 Dedekind 整环的理想类群习题7.3, 可知 $A = \bigcap_{m \in Spec_A} A_m$. 因此, 对 $x \in K$, 若 x 在 A 上整, 则对 $\forall m \in Spec_A$, x 在 A_m 上整. 由 A_m 的整闭性可知 $x \in A_m$, 从而 $x \in \bigcap_{m \in Spec_A} A_m = A$, 故 A 是整闭的. ♢

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

♣ $\sqrt[n]{2}$ 在 $\mathbb{Q}$ 上的极小多项式是 x^n-2(由 Eisenstein 可知不可约性), 它有 n 个根 $\sqrt[n]{2}\zeta_n^i$, $0\leq i\leq n-1$. 对任意自同构 σ: $\mathbb{Q}(\sqrt[n]{2})\to\mathbb{Q}(\sqrt[n]{2})$, $\sigma(\sqrt[n]{2})$ 需有相同的极小多项式, 故也是 x^n-2 的根. 当 n 为奇数时, 这些根里只有 $\sqrt[n]{2}$ 为实数, 而 $\mathbb{Q}(\sqrt[n]{2})\subseteq\mathbb{R}$, 故共轭根仅有自己, 有 $\sigma(\sqrt[n]{2})=\sqrt[n]{2}$, 此时自同构仅有恒等映射, 故 $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q})=\{e\}$. 当 n 为偶数时, 共轭根有 $\sqrt[n]{2}$ 和 $-\sqrt[n]{2}$, 则诱导一个非平凡自同构满足 $\sqrt[n]{2}\mapsto-\sqrt[n]{2}$. 这给出所有自同构, 故 $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q})=\mathbb{Z}/2\mathbb{Z}$. ♢

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.

♣ 对于 $\sigma\in G=\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$, 考虑 $\sigma(\sqrt[3]{2})\in\{\sqrt[3]{2}\omega^i,0\leq i\leq 2\}$, 及 $\sigma(\omega)\in\{\omega^j,1\leq j\leq 2\}$. 故 $|G|\leq 6$. 而考虑 x^3-2 的三个根 $\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2$, 后两个不是实数, 但 $\mathbb{Q}(\sqrt[3]{2})\subseteq\mathbb{R}$, 这给出 $x^3-2=(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4})$ 为 x^3-2 在 $\mathbb{Q}(\sqrt[3]{2})$ 上的不可约分解, 于是 $[\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\omega):\mathbb{Q}(\sqrt[3]{2})]=2$. 另外有 $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\omega)=\mathbb{Q}(\sqrt[3]{2},\omega)$, 故 $[\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q}]=6$, 因而由 2022-05-30 的定义 1和习题 2, G 恰由如下 6 个元素组成:

$$\sigma_{ij}(\sqrt[3]{2})=\sqrt[3]{2}\omega^i,0\leq i\leq 2$$

$$\sigma_{ij}(\omega)=\omega^j,j=1,2$$

具体地, $G=\mathbb{Z}/3\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}\simeq D_3$, 后者是二面体群. ♢

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

♣ 考虑 $\sqrt{2+\sqrt{2}}$ 在 $\mathbb{Q}$ 上的极小多项式 x^4-4x^2+2(不可约性可由 Eisenstein 判别法证明), 其四个根为 $\sqrt{2+\sqrt{2}},-\sqrt{2+\sqrt{2}},\sqrt{2-\sqrt{2}},-\sqrt{2-\sqrt{2}}$. 如果记 $a=$

$\sqrt{2+\sqrt{2}}$, 则 $-\sqrt{2+\sqrt{2}} = -a, \sqrt{2-\sqrt{2}} = \dfrac{a^2-2}{a}, -\sqrt{2-\sqrt{2}} = -\dfrac{a^2-2}{a}$, 四个根均在 $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ 中. 为确定 G 中一个元素 σ, 只需确认 $\sigma(a)$. 注意到, 取 $\sigma \in G$, 使得 $\sigma(a) = \dfrac{a^2-2}{a} = \sqrt{2-\sqrt{2}}$, 那么 σ 在 G 中的阶数是 4(考虑 σ 在 a 上的作用,$\sigma^2(a) = -a$). 而 $|G| \leq 4$, 这说明 $|G| = 4$, 且 G 中有 4 阶元, 故 $G = \mathbb{Z}/4\mathbb{Z}$. ♢

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

♣ 由讲义 2022-03-16习题 5后的注可知 ζ_N 在 $\mathbb{Q}$ 上的极小多项式是 $\Phi_N(x)$, 这个不可约多项式的所有根为: $\zeta_N^i, 1 \leq i \leq N-1$, $pgcd(i,N) = 1$. 为确定 σ 的作用, 只需确定 $\sigma(\zeta_N)$, 而由于所有共轭根都在 $\mathbb{Q}(\zeta_N)$ 中, 这相当于选取一个 i, 使得 $1 \leq i \leq N-1$, $pgcd(i,N) = 1$, 将相应自同构记为 σ_i. 故 $\sigma_i(\sigma_j(\zeta_N)) = \sigma_i(\zeta_N^j) = \sigma_i(\zeta_N)^j = \zeta_N^{ij} = \sigma_{ij}(\zeta_N)$. 因此, 该扩张的 Galois 群同构于乘法群 $(\mathbb{Z}/N\mathbb{Z})^*$. ♢

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

♣ 记 α 为 $x^p - t$ 的一个在 $\mathbb{F}_p(t)[x]/(x^p-t)$ 中的根, 则 $x^p - t = x^p - \alpha^p = (x-\alpha)^p$, 故 G 中元素只能将 α 映至 α, 从而只有恒等映射, 即 G 为平凡群. ♢

注: 我们会看在讲义 2022-06-01习题 7中再次遇到这个例子. 这是一个典型的纯不可分扩张的例子.

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

♣ 记 α 为 $x^p - x - 1$ 在 $\mathbb{F}_p(t)[x]/(x^p - x - 1)$ 中的一个根, 可以验证 $\alpha + 1$ 也是一个根, 故 $\alpha, \alpha+1, \ldots, \alpha+p-1$ 恰为所有 p 个根, 且每个根都在 K 中. 对每个 i, 将 α 映至 $\alpha + i$ 给出一个 Galois 群中的元素, 故 Galois 群为 p 阶群, 从而为 $\mathbb{Z}/p\mathbb{Z}$. ♢

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

♣ $t^{\frac{1}{n}}$ 在 $\mathbb{C}(t)$ 上有零化多项式 $x^n - t$, 由 Eisenstein 判别法知该多项式不可约, 故为极小多项式. 它有 n 个根 $t^{\frac{1}{n}}, \zeta_n t^{\frac{1}{n}}, \cdots, \zeta_n^{n-1} t^{\frac{1}{n}}$, 而 $\zeta_n \in \mathbb{C}$, 故 Galois 群中的元素 σ 由 $\sigma(t^{\frac{1}{n}})$ 确定, 进而由某个 i, $0 \leq i \leq n-1$ 确定. 易见由 $t^{1/n}$ 确定的自同构可生成其他自同构, 故该扩张的 Galois 群为 $\mathbb{Z}/n\mathbb{Z}$. ♢

8. $K(t)/K$, 其中 K 为域.

♣ 对于 $\sigma \in G$, 考虑 $\sigma(t) = h(t) = \dfrac{f(t)}{g(t)} \in K(t)$, 其中 $f(t), g(t) \in K[t]$ 为互素多项式. 利用讲义 2022-05-09习题 3的结论可知 $max\{\deg f, \deg g\} = 1$, 否则 $[K(x) : K(h(x))] > 1$, 意味着 $K(x) \neq K(h(x))$. 不妨设 $f(t) = at + b, g(t) = ct + d, ad \neq 0$, 则 σ 由 (a,b,c,d) 完全确定, 且 f 和 g 的互素性及 $ad \neq 0$ 等价于矩阵

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL_2(K)$$

验证运算关系可知该扩张的 Galois 群就是乘法群 $PGL_2(K)$. ♢

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 α 的 $F[x]$ 中的多项式, 则称 $f(\alpha)$ 为 α 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 $f(x)|g(x)$. ♢

♣ 取 $d(x) = pgcd(f(x), g(x))$. 由 Bezout 定理可知 $d(\alpha) = 0$. 而 $\deg d \leq \deg f$, 由 f 的定义, 只能是 $\deg d = \deg f$, 故 $f(x)|g(x)$. ♢

习题 **2.**

1. 域的有限扩张为代数扩张.

♣ 设 $[E : F] = n$. 任取 $\alpha \in E$. 考虑 $1, \alpha, \alpha^2, \ldots, \alpha^n$, 可知这 $n+1$ 个元素线性相关, 这便给出了 α 的一个零化多项式. 从而 E/F 是代数扩张. ♢

2. 设 E/F, K/E 均为代数扩张, 则 K/F 为代数扩张.

♣ 设 $\alpha \in K$ 的一个零化多项式是 $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, 注意到 $F(a_{n-1}, \ldots, a_0)/F$ 是有限扩张 (这个扩张相当于 n 次扩张的复合, 每次引入一个 $a_i, 0 \leq i \leq n-1$. 由于每个 a_i 都是代数的, 故每次扩张次数都是有限的, 因而这 n 个扩张的复合是一个有限扩张), 且 $F(a_{n-1}, \ldots, a_0)(\alpha)/F(a_{n-1}, \ldots, a_0)$ 是有限扩张, 可知 $F(a_{n-1}, \ldots, a_0, \alpha)/F$ 是有限扩张, 由 *1.* 知其是代数扩张, 从而 α 在 E 上是代数的. 由 α 的任意性可知 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 α 在 F 上的极小多项式, 设 E/F 为域扩张, 则

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

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.

♣ 设 $\sigma \in \mathrm{Hom}_F(F(\alpha), E)$, 将 σ 作用在 $f(\alpha) = 0$ 上, 可知 $\sigma(\alpha)$ 要满足同样的极小多项式. 而 σ 由 $\sigma(\alpha)$ 决定, 因此

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

反之, 任给一个 E 中 f 的根 β, 考虑 E 的子域 $F(\beta)$, 由于 f 是 α 的极小多项式, 在 F 上不可约, 其也是 β 的极小多项式. 由同构 $F(\alpha) \simeq F[X]/(f) \simeq F(\beta)$ 再复合上 $F(\beta)$ 到 E 的自然嵌入即给出一个 $\mathrm{Hom}_F(F(\alpha), E)$ 中的元素. 故等号成立当且仅当 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

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

并且等号成立

$\Leftrightarrow$ 对任意 $\alpha \in E_1$, α 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 $i = 1,\cdots,n$, α_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)

♣ 设 $E_1 = F(\alpha_1,\ldots,\alpha_n)$. 对于 $\sigma \in \mathrm{Hom}_F(F(\alpha_1),E_2)$, 引定理 1, 我们可以得到 $|\mathrm{Hom}_F(F(\alpha_1),E_2)| \leq [F(\alpha_1):F]$. 再考虑 $\tau \in \mathrm{Hom}_F(F(\alpha_1,\alpha_2),E_2)$. 而 $\tau|_{F(\alpha_1)} \in \mathrm{Hom}_F(F(\alpha_1),E_2)$, 若固定 $\tau|_{F(\alpha_1)} \in \mathrm{Hom}_F(F(\alpha_1),E_2)$, τ 就完全由 $\tau(\alpha_2)$ 决定, 这表明

$$|\mathrm{Hom}_F(F(\alpha_1,\alpha_2),E_2)| \leq |\mathrm{Hom}_{F(\alpha_1)}(F(\alpha_1,\alpha_2),E_2)| \cdot |\mathrm{Hom}_F(F(\alpha_1),E_2)|$$

其中 $F(\alpha_1)$ 通过 $\tau|_{F(\alpha_1)}$ 视为 E_2 的子域. 引定理 1:

$$|\mathrm{Hom}_F(F(\alpha_1,\alpha_2),E_2)| \leq [F(\alpha_1,\alpha_2):F(\alpha_1)][F(\alpha_1):F] = [F(\alpha_1,\alpha_2):F]$$

归纳可得

$$|\mathrm{Hom}_F(E_1,E_2)| = |\mathrm{Hom}_F(F(\alpha_1,\ldots,\alpha_n),E_2)| \leq [E_1,F]$$

且考察每一步的取等条件, 可知等号成立 $\Leftrightarrow$ 对每个 $i = 1,\cdots,n$, α_i 在 $F(\alpha_1,\cdots,\alpha_{i-1})$ 上的极小多项式 $f_i(x) \in F(\alpha_1,\cdots,\alpha_{i-1})[x]$ 在 E_2 中恰有 $\deg f_i$ 个互不相同的根. 事实上, 由于以上论述对任意形如 $F(\alpha_1,\cdots,\alpha_n)$ 的扩张成立, 对任意 $\alpha \in E_1$, 我们总可以让 $\alpha_1 = \alpha$ 再得到 $E_1 = F(\alpha,\alpha_2,\cdots,\alpha_N)$, 进而得到 α 在 F 上的极小多项式 f 在 E_2 中有 $\deg f$ 个互不相同的根. 特别地, 每个 α_i 均如此. 反之, 若 $E_1 = F(\alpha_1,\cdots,\alpha_n)$, 且每个 α_i 在 F 上的极小多项式 f_i 在 E_2 中都有 $\deg f_i$ 个互不相同的根, 则 α_i 在 $F(\alpha_1,\cdots,\alpha_{i-1})$ 上的极小多项式 g_i 为 f_i 的因子, 其在 E_2 上也应当分裂, 且所有根互不相同, 这也就证明了上面的等价条件与定理中后两个等价条件互相等价, 进而证明了

结论. ♢

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).

♣ 对任意 $\alpha \in E$, 由于 α 是代数的, 取其零化多项式 $f(x) \in F(x)$. 由定义 2的注可知 $\alpha \in F$, 故 $E \subset F$. 因此嵌入 $\iota : F \to E$ 事实上是域同构. ♢

事实: 设 F 为域, 则存在域扩张 E/F, 使得 E 为代数封闭域.

以下补充一个该事实的证明:

♣ 对于任意 $f \in F[X]$ 且 $\deg f \geq 1$, 给出一个变元 X_f, 然后考虑 F 上的无穷元多项式环 $A = F[X_f, f \in F[X]\backslash F]$. 令 I 为由子集 $\{f(X_f) \mid f \in F[X]\backslash F\}$ 生成的理想, 我们先证 I 为真理想. 否则有 $1 \in I$, 于是存在 $f_1, \cdots, f_n \in F[X]\backslash F$, $g_1, \cdots, g_n \in A$ 使得

$$g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) = 1$$

将 X_{f_i} 简记作 X_i, 每个 g_i 只涉及有限个 X_f, 且只有有限个 g_i, 不妨假定每个 g_i 都在 $F[X_1, \cdots, X_N]$ 中 $(N \geq n)$, 于是以上等式成为 $F[X_1, \cdots, X_N]$. 上的等式. 令 K 为 F 的一个有限扩张, 使得各 $f_i, 1 \leq i \leq n$ 在 K 中有根, 并假定 a_i 为 f_i 的一个根. 对于 $n < i \leq N$, 令 $a_i = 0$, 于是 $(a_1, \cdots, a_N)$ 为上面等式左边的一个 K^N 中的零点, 这给出 $0 = 1$, 矛盾. 故 I 为真理想, 由 Krull 定理, 存在极大理想 $\mathfrak{m}$ 包含 I, 此时 $A/\mathfrak{m}$ 为域, 且自然为 F 的一个域扩张, 同时每个 $f(X_f)$ 在商中为 0, 于是在 $A/\mathfrak{m}$ 中, 任意 F 上的正次数多项式 f 都有根, 即 X_f 的像. 我们记 $E_1 = A/\mathfrak{m}$, 再用 E_1 替换 F 做类似操作

得到 E_2, 使得每个 E_1 上的正次数多项式在 E_2 中都有根. 重复操作得到一个域的包含列

$$E_1 \subseteq E_2 \subseteq E_3 \subseteq \cdots \subseteq E_n \subseteq \cdots$$

然后令 $E = \bigcup_{n=1}^{\infty} E_n$, 此时 E 为 F 的一个域扩张, 且对任意 E 系数的多项式, 由于只有有限个系数, 一定存在 m 使得该多项式的系数都在 E_m 中, 由构造其在 E_{m+1} 上有根, 进而在 E 上有根, 故 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 $\bar{F} := \{\alpha \in E \mid \alpha在F上整\}$, 则 $\bar{F}$ 为 E 的子域, 且为 F 的代数闭包.

♣ 我们已经在讲义 2022-03-23习题 9中用结式的技巧证明了 $\bar{F}$ 是域, 因而是 E 的子域. 而由 $\bar{F}$ 的定义, $\bar{F}$ 中的元素均在 F 上代数, 故 $\bar{F}/F$ 是代数扩张. 下面证明 $\bar{F}$ 是代数封闭域, 从而 $\bar{F}$ 是 F 的代数闭包. 设 $f(x) \in \bar{F}[x] \subset E[x]$, 由于 E 是代数封闭域, 可知存在 $\alpha \in E$, 使得 $f(\alpha) = 0$. 考虑域 $\bar{F}(\alpha)$, 其是 $\bar{F}$ 上的代数扩张, 因而也是 F 上的代数扩张, 故 α 在 F 上是代数的, 从而也是整的, 这表明 $\alpha \in \bar{F}$. 故 $\bar{F}$ 是代数封闭的, 从而是 F 的一个代数闭包. ♢

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 $\mathrm{Hom}_F(E_1, E_2) \neq \varnothing$.

♣ 考虑如下一个集合

$$S = \{(K, \varphi) | F \subset K \subset E_1, \varphi \in Hom_F(K, E_2)\}$$

其上偏序关系定义为:

$$(K_1, \varphi_1) \prec (K_2, \varphi_2) \Leftrightarrow K_1 \subset K_2, \varphi_2|_{K_1} = \varphi_1$$

由于 $(F, id) \in S$, 可知 S 非空. 任意 S 中升链 $((K_i, \varphi_i))_{i \in I}$, 取 $K = \cup_{i \in I} K_i, \varphi \in Hom_F(K, E_2)$, 使得 $\varphi|_{K_i} = \varphi_i, \forall i \in I$, 则 (K, φ) 为该全序子集的一个上界. 对 S 引 Zorn 引理, 可得 S 中一极大元 (E, ψ). 若 $E \subsetneq E_1$, 取 $a \in E_1 \backslash E$. 由于 a 在 F 上代数, 取其零化多项式 $f(x) \in F(x) \subset E_2[x]$(这里把 F 在 E_2 中的像和 F 作了等同), 由于 E_2 是代数封闭域, 存在 $\alpha \in E_2$, 使得 $f(\alpha) = 0$. 定义 $\psi_1 \in \mathrm{Hom}_F(E(a), E_2)$, 使得 $\psi_1(a) = \alpha \in E_2$, 且 $\psi|_E = \psi$. 可知 ψ 良定, 从而 $(E(a), \psi_1) \in S$, 且 $(E, \psi) \prec (E(a), \psi_1)$, 这与 (E, ψ) 是 S 中极大元矛盾. 故 $E = E_1$, 从而 $\psi \in Hom_F(E_1, E_2)$, 特别地, $\mathrm{Hom}_F(E_1, E_2) \neq \varnothing$. ♢

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

♣ 由 *1.*, 存在 $\varphi \in Hom_F(\bar{F}_1, \bar{F}_2)$. 由于 $\varphi(\bar{F}_1)$ 是代数封闭域, 且 $\bar{F}_2/\varphi(\bar{F}_1)$ 是代数扩张 ($\bar{F}_2/F$ 是代数扩张, 而 $F \subset \varphi(\bar{F}_1)$, 由习题 3. 可知 $\varphi(\bar{F}_1) \simeq \bar{F}_2$, 故 $\bar{F}_1 \simeq \bar{F}_2$. ♢

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.

♣ 首先 $\bar{E}$ 是 E 上的代数扩张, 从而是 F 上的代数扩张. 再由 $\bar{E}$ 是代数封闭域, 可知 $\bar{E}$ 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 $\tilde{\sigma}\colon E \hookrightarrow \bar{F}, \tilde{\sigma}|_F = \sigma$.

♣ 首先处理 E/F 是有限扩张的情况, 此时 E/F 一定是有限生成扩张, 我们对生成元个数进行归纳证明. 当生成元个数 $n = 1$, 也即是说 $E = F(\alpha)$ 时, 只需将 $\tilde{\sigma}(\alpha)$ 取为 α 的一个共轭根即可. 假设命题对 $n = k - 1$ 成立, 对 $n = k \geq 2$ 时, 记 $E = F(x_1, \ldots, x_k) = F(x_1, \ldots, x_{k-1})(x_k)$. 由归纳假设, 有映射 $\sigma'\colon F(x_1, \ldots, x_{k-1}) \hookrightarrow \bar{F}$, 使得 $\sigma'|_F = \sigma$. 对扩张 $E/F(x_1, \ldots, x_{k-1})$ 用 $n = 1$ 的命题即可得到 $\tilde{\sigma}\colon E \hookrightarrow \bar{F}$, 使得 $\tilde{\sigma}|_{F(x_1,\ldots,x_{k-1})} = \sigma'$, 进而有 $\tilde{\sigma}|_F = \sigma$.

对于一般的情况, 考虑偏序集:

$$\mathcal{F} := \{(M, \sigma_M), F \hookrightarrow M \hookrightarrow E, \sigma_M|_K = \sigma\}$$

其上偏序关系定义为:

$$(M, \sigma_M) \leq (M', \sigma_{M'}) \Leftrightarrow M \subset M', \sigma_{M'}|_M = \sigma_M$$

从上面我们对有限扩张的讨论可以看出 $\mathcal{F}$ 显然是非空的. 对 $\mathcal{F}$ 中升链 $(M_j, \sigma_j)_{j\in\mathcal{I}}$, 考虑 $M = \cup_{j\in\mathcal{I}} M_j$, 及映射 $\sigma_M\colon M \to \bar{F}, \sigma_M|_{M_j} = \sigma_j$, 那么 (M, σ_M) 自然是这条升链的一个上界. 由 Zorn 引理可知 $\mathcal{F}$ 中存在极大元, 我们记为 (E', σ'). 如果 $E\backslash E' \neq \varnothing$, 取 $x \in E\backslash E'$. 由于 E/F 是代数扩张,E 中每个元素在 F 上都是代数的, 从而在 E' 上都是代数的. 考虑中间域 $E'(x)$, 由上面关于有限扩张的讨论, 我们显然可以将 σ' 延拓到 $E'(x)$ 上, 这与 E' 的选取矛盾. 因而 $E = E'$, 也即给出了 σ 在 E 上的一个延拓. ♢

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. $\forall \alpha \in E$, α 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 $1 \leq i \leq n$, α_i 在 F 上的极小多项式 $f_i(x)$ 无重根, 即 $(f_i(x), f_i'(x))$.

♣ 在讲义 2022-05-16定理 2中, 取 $E_1 = E, E_2 = \bar{F}$, 即得该结论. ♢

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.

♣ 由以上定义只需证 $|\mathrm{Hom}_F(K,\bar{F})| = [K:F]$, 而 $[K:F] = [K:E][E:F] = |\mathrm{Hom}_E(K,\bar{F})| \cdot |\mathrm{Hom}_F(E,\bar{F})|$. 另一方面, 对任意 $\sigma \in \mathrm{Hom}_F(E,\bar{F})$, 这给出了 E 的一个代数闭包 $E \to \bar{F}$, 进而存在 $|\mathrm{Hom}_E(K,\bar{F})|$ 种方式将 σ 扩张到 K 上. 而 σ 的选取方式有 $|\mathrm{Hom}_F(E,\bar{F})|$ 种, 这样得到的 $\mathrm{Hom}_F(K,\bar{F})$ 中的元素两两不同, 故得到单射 $\mathrm{Hom}_E(K,\bar{F}) \times \mathrm{Hom}_F(E,\bar{F}) \to \mathrm{Hom}_F(K,\bar{F})$. 相应的限制给出反向的映射, 从而给出双射, 于是得到 $|\mathrm{Hom}_F(K,\bar{F})| = |\mathrm{Hom}_E(K,\bar{F})| \cdot |\mathrm{Hom}_F(E,\bar{F})| = [K:F]$. ♢

2. 若 K/F 为可分扩张, 则 E/F, K/E 均为可分扩张.

♣ 仍然考察 *1.* 中的等式

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

由于 K/F 为可分扩张, 上式右侧即为 $[K:F]$, 这迫使右侧的两项同时取到上界 $[K:E][E:F]$, 故而 $E/F, K/E$ 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 $f(x) = g(x^p)$.

♣ 考虑 f 的 (形式上的) 导数 f'. 若 f 有重根, 则 $d := pgcd(f, f') \neq 1$. 若 $f' \neq 0$, 总有 $\deg d \leq \deg f' < \deg f$, 这与 f 不可约矛盾. 故 $f' = 0$, 这表明域 F 的特征为某一素数 p, 且 $f(x)$ 中次数不为 p 的倍数的项前面的系数都是 0, 也即 f 可以写作 $f(x) = \sum_{k=0}^{n} a_k x^{pk}$ 的形式. 令 $g(x) = \sum_{k=0}^{n} a_k x^k$, 则 $f(x) = g(x^p)$, 即为所求. ♢

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.

♣ 设 $E = F(\alpha_1, \ldots, \alpha_n)$. 对于 α_i, 其极小多项式 f_i 当然是 $F[x]$ 中的不可约多项式. 由于 F 的特征为 0, 可知 $pgcd(f, f') = 1$(否则与不可约性矛盾), 因而无重根. 这即是说 E/F 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.

♣ 设 $\mathbb{F}_q$ 为 $\mathbb{F}_p$ 的有限扩张. 则 $\mathbb{F}_q$ 为有限维 $\mathbb{F}_p$-线性空间, 从而 $q = p^n$(这里 q 为 $\mathbb{F}_q$ 的元素个数). 记 $\bar{\mathbb{F}}_p$ 为 $\mathbb{F}_p$ 的代数闭包. 我们知道 $\mathbb{F}_q = \{x \in \bar{\mathbb{F}}_p \mid x^{q-1} = 1\} \cup \{0\}$. 注意到 $p(x) = x^{q-1} - 1$ 与 $p'(x) = (q-1)x^{q-2}$ 互素, 这表明 $p(x)$ 无重根, 从而 $\mathbb{F}_q$ 中任意

元素的极小多项式无重根. 因此 $\mathbb{F}_q/\mathbb{F}_p$ 为有限扩张. $\diamondsuit$

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

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, $\forall \varphi \in \mathrm{Hom}_{\mathbb{Q}(\alpha)}(K, \mathbb{C})$, $\varphi(\alpha) = \alpha$.

♣ 由于 $\mathbb{Q}(\alpha)$ 为特征 0 的域, 且 $K/\mathbb{Q}(\alpha)$ 为有限扩张, 可知 $K/\mathbb{Q}(\alpha)$ 为可分扩张, 从而 $|\mathrm{Hom}_{\mathbb{Q}(\alpha)}(K, \mathbb{C})| = [K : \mathbb{Q}] = m$. $\diamondsuit$

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

♣ $\sqrt{a_i}$ 的极小多项式是 $x^2 - a_i$, 从而 $\forall \varphi \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, $\varphi(\sqrt{a_i}) = \pm\sqrt{a_i}$. 因此, 如果 $\varphi \neq i$, 则 $\varphi(\alpha) \neq \alpha$ ($\varphi(\alpha) < \alpha$). 而 $\mathrm{Hom}_{\mathbb{Q}(\alpha)}(K, \mathbb{C}) \subset \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, 这表明 $|\mathrm{Hom}_{\mathbb{Q}(\alpha)}(K, \mathbb{C})| = 1$, 故 $[K : \mathbb{Q}(\alpha)]$=1, 即 $K = \mathbb{Q}(\alpha)$. $\diamondsuit$

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 φ 不等于包含同态 i, 就有 $\varphi(\alpha) \neq \alpha$.

♣ 由于 E/F 为有限可分扩张, $E/F(\alpha)$ 也为有限可分扩张, 从而 $[E : F(\alpha)] = |\mathrm{Hom}_{F(\alpha)}(E, \bar{F})|$. 因此, $E = F(\alpha) \Leftrightarrow [E : F(\alpha)] = |\mathrm{Hom}_{F(\alpha)}(E, \bar{F})| = 1 \Leftrightarrow \forall \varphi \in \mathrm{Hom}_F(E, \bar{F})$, 只要 φ 不等于包含同态 i, 就有 $\varphi(\alpha) \neq \alpha$. $\diamondsuit$

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 $E = F(\alpha)$.

♣ 当 F 为有限域时, E 也为有限域, 从而乘法群 $E^* = \langle \alpha \rangle$ 为循环群, 这样 $E = F(\alpha)$. 从而可以假设 F 为无限域, 并且通过对生成元的个数归纳, 可以进一步假设 $E = F(\beta, \gamma)$. 记 $f(x)$ 和 $g(x)$ 分别为 β 和 γ 在 F 上的极小多项式设 $\{\beta_1 = \beta, \beta_2, \cdots, \beta_n\}$ 为 $f(x)$ 在 $\bar{F}$ 上所有的不同根, $\{\gamma_1 = \gamma, \gamma_2, \cdots, \gamma_m\}$ 为 $g(x)$ 在 $\bar{F}$ 上所有的不同根. 则 $\forall \varphi \in \mathrm{Hom}_F(E, \bar{F})$, 均存在 i, j, 使得 $\varphi(\beta) = \beta_i$, $\varphi(\gamma) = \gamma_j$. 由 F 为无限域, 可以找到 $c \in F$, 使得只要 $(i, j) \neq (1, 1)$, 就有 $\beta_1 + c\gamma_1 \neq \beta_i + c\gamma_j$, 令 $\alpha = \beta + c\gamma = \beta_1 + c\gamma_1$, 再利用上面的引理 1即可看出 $E = F(\alpha)$. ♢

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: $|1| = |-1| = 1$.

♣ 注意范数具有正则性. 我们有: $|1| = |1^2| = |1|^2 \Rightarrow |1| = 1$. $|-1|^2 = |(-1)^2| = 1 \Rightarrow |-1| = 1$. ♢

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.

♣ 容易验证 $|\cdot|_p$ 是一个域范数. 而 $\mathbb{Q}_p$ 正是 $\mathbb{Q}$ 在此范数下拓扑完备化得到的等价类, 因而自然在该范数下完备. ♢

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

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

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 $|x+y| = |y|$.

♣ 由强三角不等式, $|x+y| \le max\{|x|, |y|\} = |y|$. 另一方面, $|y| = |(x+y)+(-x)| \le max\{|x+y|, |x|\}$. 由 $|y| > |x|$, 可知 $|y| \le |x+y|$, 从而 $|x+y| = |y|$. ♢

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 $C_1|x|_2 \le |x|_1 \le C_2|x|_2$.

♣ 对 $x = (x_1, \cdots, x_n) \in \mathbb{Q}_p^n$, 定义范数 $|\cdot|_0$ 为 $|x|_0 = \max\{|x_1|_p, \cdots, |x_n|_p\}$. 取典范基有 $x = x_1e_1 + \cdots + x_ne_n$, 于是 $|x|_1 \le \sum\limits_{i=1}^{n} |x_i|_p|e_i|_0 \le C_2|x|_0$, 其中 $C_2 = \sum\limits_{i=1}^{n} |e_i|_0$. 进一步, 有 $|x|_1 - |y|_1 \le |x-y|_1 \le C_2|x-y|_0$. 考虑 V 上乘积拓扑, 而 $|\cdot|_0$ 恰诱导乘积拓扑, 故前面的式子说明 $|\cdot|_1$ 是连续的. 而 $B = \mathbb{Z}_p^n \subseteq V$ 为 $|\cdot|_0$ 单位球, 由 $\mathbb{Z}_p$ 紧知 B 紧, 进而 B 在 $|\cdot|_1$ 下的像紧, 于是有正的下确界 C_1. 也即是说, 对任意 x 满足 $|x|_0 \le 1$, 有 $|x|_1 \ge C_1$. 对一般的 $x \in V\backslash\{0\}$, 若 $|x|_0 = p^N$, 考虑 $p^Nx \in B$, 即知 $|x|_1 \ge C_1|x|_0$. 由于所有范数均与 $|\cdot|_0$ 等价, 故互相也均等价. ♢

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 $C_1|x|_2 \le |x|_1 \le C_2|x|_2$, 那么 $|\cdot|_1 = |\cdot|_2$

♣ 即证明 $C_2 = C_1 = 1$. 假设存在 x, 使得 $\frac{|x|_1}{|x|_2} \neq 1$, 不妨设 $\frac{|x|_1}{|x|_2} > 1$, 那么 $\frac{|x^n|_1}{|x^n|_2} = (\frac{|x|_1}{|x|_2})^n \to \infty$, 显然不可能被上界 C_2 控制. 因此 $\forall x, \frac{|x|_1}{|x|_2} = 1$, 即 $|\cdot|_1 = |\cdot|_2$. ♢

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 $|\sigma(x)| = |x|$.

♣ 对 $\sigma \in \mathrm{Hom}_{\mathbb{Q}_p}(E, \bar{\mathbb{Q}}_p)$, 定义新的范数 $|\cdot|'$

$$\forall x \in E,\ |x|' := |\sigma(x)|$$

逐条验证可知这是 E 上的一个范数. 由习题 8和习题 9可知 $|\cdot| = |\cdot|'$, 也即对任意 $x \in E$, 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 α 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:$\mathbb{Q}_p(\alpha) \subset \mathbb{Q}_p(\beta)$.

♣ 即证 $\alpha \in \mathbb{Q}_p(\beta)$, 只需证明 $\mathbb{Q}_p(\alpha, \beta) = \mathbb{Q}_p(\beta)$. 考虑 $\varphi \in \mathrm{Hom}_{\mathbb{Q}_p(\beta)}(\mathbb{Q}_p(\alpha, \beta), \bar{\mathbb{Q}}_p)$, 则 $\exists 1 \leq i \leq n$, 使得 $\varphi(\alpha) = \alpha_i$, 从而 $\varphi(\alpha - \beta) = \alpha_i - \beta$. 由习题 10可知 $|\alpha - \beta| = |\varphi(\alpha - \beta)| = |\alpha_i - \beta|$. 据条件, 只能是 $i = 1$, 从而 $\varphi = id$. 由讲义 2022-05-18引理 1可知 $\mathbb{Q}_p(\alpha, \beta) = \mathbb{Q}_p(\beta)$, 从而 $\mathbb{Q}_p(\alpha) \subset \mathbb{Q}_p(\beta)$. ♢

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 $F(f_1, f_2) = 0$.

♣ 若 $f_1 \in K$, 取 $F(x,y) = x - f_1$ 即可. 否则, 考虑域 $K(f_1)$, 下证 f_2 在上面代数. 事实上, 只需证 x 在上面代数, 于是 $K(x)/K(f_1)$ 为代数扩张, 从而由 $f_2 \in K(x)$ 即知 f_2 在 $K(f_1)$ 上代数. 若 $f_1(x) = \dfrac{g(x)}{h(x)}$, 考虑 $K(f_1)[t]$ 中的多项式 $f_1(x)h(t) - g(t)$ 为 x 的一个零化多项式, 且由于 $f_1 \notin K$ 知该多项式非零. 故令 $G(t) \in K(f_1)[t]$ 为 f_2 在 $K(f_1)$ 上的极小多项式, 于是有等式

$$G(f_2) = f_2^n + \frac{g_{n-1}(f_1)}{h_{n-1}(f_1)} f_2^{n-1} + \cdots + \frac{g_0(f_1)}{h_0(f_1)} = 0,$$

其中 $g_i, h_i \in K[t]$, 通分取分子即得到一个二元多项式零化 (f_1, f_2). ♢

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 $F(f_1, \cdots, f_{n+1}) = 0$.

♣ 如果存在非零的 n 元多项式 $F(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, 使得 $F(f_1, \ldots, f_n) = 0$, 则命题已经成立. 下设不存在这样的非零 n 元多项式. 特别地, 此时各 f_i 均在 K 上超越. 由于 $E/K(x_1, \ldots, x_n)$ 是代数扩张, 存在非零的 $f \in K[x_1, \ldots, x_n][x_{n+1}] = K[x_1, \cdots, x_{n+1}]$, 使得 $f(f_1, x_1, \ldots, x_n) = 0$ (将 f_1 在 $K(x_1, \ldots, x_n)$ 上的极小多项式通分得到). 由假设, 存在某个 x_i, $1 \leq i \leq n$ 使得 f 关于 x_i 的 deg 大于零 (即

$f \notin K[x_{n+1}]$), 不妨设为 x_1, 我们证明 $E/K(f_1, x_2, \ldots, x_n)$ 是代数扩张, 且不存在非零的 $g \in K[x_1, \ldots, x_n]$, 使得 $g(f_1, x_2, \ldots, x_n) = 0$. 由于 $E/K(f_1, x_1, \ldots, x_n)$ 和 $K(f_1, x_1, \ldots, x_2)/K(f_1, x_2, \ldots, x_n)$ 都是代数扩张, 所以它们的复合 $E/K(f_1, x_2, \ldots, x_n)$ 也是代数扩张. 其次, 假如存在非零的 $g \in K[x_1, \ldots, x_n]$, 使得 $g(f_1, x_2, \ldots, x_n) = 0$, 那么 $g \notin K[x_2, \cdots, x_n]$, 即 g 关于第一个分量的 deg 大于 0, 且这给出 f_1 在 $K(x_2, \cdots, x_n)$ 上的零化多项式, 于是 $K(f_1, x_2, \ldots, x_n)/K(x_2, \ldots, x_n)$ 是代数扩张, 故 $E/(x_2, \ldots, x_n)$ 是代数扩张, 这说明 x_1 在 $K(x_2, \ldots, x_n)$ 上代数, 矛盾. 故 $E/K(f_1, x_2, \ldots, x_n)$ 是代数扩张, 且不存在非零的多项式 $g \in K[x_1, \ldots, x_n]$, 使得 $g(f_1, x_2, \ldots, x_n) = 0$.

对 $f_2, \ldots, f_n$ 重复这样的操作, 可以证明 $E/K(f_1, \ldots, f_n)$ 是代数扩张, 且不存在非零的 $g \in K[x_1, \ldots, x_n]$, 使得 $g(f_1, \ldots, f_n) = 0$. 由于 $f_{n+1} \in E$, 这说明存在非零的多项式 $F \in K[f_1, \ldots, f_n][x_{n+1}] = K[f_1, \cdots, f_n, x_{n+1}]$, 使得 $F(f_1, \ldots, f_{n+1}) = 0$, 即证. $\diamondsuit$

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).

♣ 若 E/K 为代数扩张, 则结论平凡. 设 E/K 为超越扩张. 考虑集合:

$$S = \{X | X \subset E, X\text{中元素在 } K \text{ 上代数无关}\}$$

由于 E 中有超越元, 可知 S 非空. 易于验证 S 配备上偏序关系 (集合的包含) 后满足升链条件, 故由 Zorn 引理知 S 中有极大元 A. 设 $E = K(a_1, \ldots, a_n)$, 先验地, $|A| \leq n$. 于是 A 即为一个 E 中的 K 上极大代数无关组. 事实上, 考虑映射

$$\varphi\colon K(x_1, \ldots, x_n) \to K(a_1, \ldots, a_n), x_1 \mapsto a_1, \ldots, x_n \mapsto a_n$$

如果 $|A| \geq n+1$, 取 $f_1, \ldots, f_{n+1} \in K(x_1, \ldots, x_n)$, 使得 $f_i(a_1, \ldots, a_n) \in A, \forall 1 \leq i \leq n$. 在习题 2中, 取 $E = K(x_1, \ldots, x_n)$, 即知 E 中最大 K 上代数无关组的个数不能超过 n, 故 $f_1, \ldots, f_{n+1}$ 在 K 上代数相关, 即存在非零的 $F(x_1, \ldots, x_{n+1}) \in K[x_1, \ldots, x_{n+1}]$, 使得 $F(f_1, \ldots, f_{n+1}) = 0$. 将 φ 作用在这个式子上, 即得到 A 中的这 $n+1$ 个元素的一个 K 上的代数相关关系, 这与 A 的选取矛盾. 故 $|A| \leq n$. ♢

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 $n = m$.

♣ 不妨设 $n \leq m$. $n = 1$ 的情况借由习题 1 容易说明. 下设 $m \geq n \geq 2$. 首先,$b_1, a_1, \ldots, a_n$ 代数相关, 故存在非零的 $f \in K[x_1, \ldots, x_{n+1}]$, 使得 $f(b_1, a_1, \ldots, a_n) = 0$. 注意到 f 关于某个 x_i 的 deg 大于 0, 否则与 b_1 为超越元相矛盾. 不妨设其为 x_1, 我们证明 $\{b_1, a_2, \ldots, a_n\}$ 是一个极大代数无关组. 考虑 $K(b_1, a_1, \ldots, a_n)/K(b_1, a_2, \ldots, a_n)$ 和 $E/(b_1, a_1, \ldots, a_n)$ 都是代数扩张, 故它们的复合 $E/K(b_1, a_1, \ldots, a_n)$ 是代数扩张. 只需再证明 $b_1, a_2, \ldots, a_n$ 代数无关. 若存在非零的 $g \in K[x_1, \ldots, x_n]$, 使得 $g(b_1, a_2, \ldots, a_n) =$

0, 那么 g 的表达式中一定出现 x_1, 否则 $a_2,\ldots,a_n$ 代数相关. 故 $K(b_1,a_2,\ldots,a_n)$ 是 $K(a_2,\ldots,a_n)$ 上的代数扩张, 因此 $E/K(a_2,\ldots,a_n)$ 是代数扩张, 这导致 $a_1,a_2,\ldots,a_n$ 代数相关, 显然矛盾. 故 $b_1,a_2,\ldots,a_n$ 确实是一个极大代数无关组.

类似地, 对 $b_2,\ldots,b_m$ 进行同样的操作后, 我们可以证明 $b_1,\ldots,b_n$(将 a_i 全部替换为 b_i) 是极大代数无关组. 又 $b_1,\ldots,b_m$ 代数无关, 这只能是 $m=n$. ♢

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

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

♣ 设 F 在 K 上的超越次数是 n, E 在 F 上的超越次数是 m. 设 F 中一个 K 上极大代数无关组是 $a_1,\ldots,a_n$, E 中一个 F 上极大代数无关组是 $b_1,\ldots,b_m$. 我们证明 $a_1,\ldots,a_n,b_1,\ldots,b_m$ 是 E 中一个 K 上极大代数无关组.

首先这 $n+m$ 个元素在 K 上代数无关: 如果存在非零的 $f\in K[x_1,\ldots,x_{n+m}]$ 使得 $f(a_1,\ldots,a_n,b_1,\ldots,b_m)=0$, 那么 f 的额表达式中一定出现某个 b_i, 否则与 $a_1,\ldots,a_n$ 是 K 上代数无关的矛盾. 因此 $f(a_1,\ldots,a_n,b_1,\ldots,b_m)=0$ 事实上给出了 $b_1,\ldots,b_m$ 在 F 上的代数相关关系, 这与 $b_1,\ldots,b_m$ 在 F 上代数无关矛盾. 故 $a_1,\ldots,a_n,b_1,\ldots,b_m$ 在 K 上代数无关. 其次, 我们证明 E 中任何一个元素均在 $K(a_1,\ldots,a_n,b_1,\ldots,b_m)$ 上代数. 对任意 $x\in E$, 由于 $x,b_1,\ldots,b_m$ 在 F 上代数相关, 存在非零 $g\in F(x_1,\ldots,x_{m+1})$,

使得 $F(x,b_1,\ldots,b_m)=0$. 将这个表达式中出现的所有 F 中的元素取出:$c_1,\ldots,c_l$, 由于这 l 个元素均在 $K(a_1,\ldots,a_n)$ 上代数, 可知

$$K(a_1,\ldots,a_n,b_1,\ldots,b_m,c_1,\ldots,c_l)/K(a_1,\ldots,a_n,b_1,\ldots,b_m)$$

是代数扩张. 而代数扩张的复合是代数扩张, 由 x 在 $K(a_1,\ldots,a_n,b_1,\ldots,b_m,c_1,\ldots,c_l)$ 上代数, 知其在 $K(a_1,\ldots,a_n,b_1,\ldots,b_m)$ 上代数.

以上便说明了 $a_1,\ldots,a_n,b_1,\ldots,b_m$ 是 E 在 K 上的一个极大线性无关组, 故 E 在 K 上的超越次数是 $m+n$. ♢

• 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 $\mathrm{Gal}(E/K):=\{\sigma\mid \sigma\colon E\xrightarrow{\sim}E$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 $|\mathrm{Gal}(E/K)|\leq[E:K]$.

♣ 由于 E/K 为有限扩张, 则为代数扩张. 取 $\bar{K}$ 为 K 的代数闭包, 则 $\mathrm{Gal}(E/K)\subset\mathrm{Hom}_K(E,\bar{K})$(通过复合自然包含 $j\colon E\to\bar{K}$ 视为子集). 由讲义 2022-05-16定理 2可知 $|\mathrm{Hom}_K(E,\bar{K})|\leq[E:K]$, 从而有 $|\mathrm{Gal}(E/K)|\leq|\mathrm{Hom}_K(E,\bar{K})|\leq[E:K]$. ♢

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 $1\le m\le n$, 定义初等对称多项式

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

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 $[E:K]\le n!$, 从而为代数扩张.

♣ 由 $\sigma_1,\ldots,\sigma_n$ 的构造可以看出 $\sigma_i\in F,\forall 1\le i\le n$, 故 $K\subset F$. 其次, 考虑多项式 $f(x)=\sum_{i=0}^{n}(-1)^i\sigma_{n-i}x^i=\prod_{i=1}^{n}(x-x_i)$(由根与系数关系), f 是 $x_1,\ldots,x_n$ 在 K 上的一个零化多项式. 考虑 $K_1=K(x_1)$, 可知 $[K_1:K]\le n$. 在 K_1 上, 多项式 $f(x)/(x-x_1)\in K_1[x]$(作 Euclid 除法), 且零化了 x_2. 记 $K_2=K_1(x_2)$, 则 $[K_2:K_1]\le n-1$. 类似地可以定义 $K_i, 1\le i\le n$, 其中 $K_n=E$. 记 $K_0=K$, 便得到 $[E:K]\le\prod[K_{i+1}:K_i]\le n!$. 因此 E/K 为有限扩张, 从而为代数扩张. ♢

注: 对于一般的域 K, 考虑 $f\in K[x]$. 若 $\deg f=n$, 则对于 f 的分裂域 E, 总有 $[E:K]\mid n!$. 归纳证明该结论. $n=1$ 情形平凡. 一般地, 若 f 本身在 K 上已经不可约, 考虑域 $K(x_1)$, 其中 $f(x_1)=0$. 则 $[K(x_1):K]=n$, 再对 $K(x_1)$ 和 $f/(x-x_1)\in K_1[x]$ 用归纳即可. 若 f 在 K 上分解成 $f=gh$, 其中 g 与 h 互素, 且有 $\deg g=m$, $\deg h=m-n$. 由归纳假设考虑 g 的分解域 K', 有 $[K':K]\mid m!$. 考虑 $h\in K'[x]$ 的分裂域 K'', 有 $[K'':K']\mid(n-m)!$. 注意到 K'' 即是 f 的分裂域 (因为 g 和 h 互素), 故有 $[K'':K]=[K'':K'][K':K]$, 后者整除 $m!(n-m)!$, 因而整除 $n!$.

2. $\mathrm{tr.deg}\,E/\mathbb{Q}=n$.

♣ 由于 $x_1,\ldots,x_n$ 在 $\mathbb{Q}$ 上代数无关, 自然地, 它们是 E 在 $\mathbb{Q}$ 上的一个极大代数无关组, 因此 $\mathrm{tr.deg}\, E/\mathbb{Q}=n$. ♢

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

♣ 由 *1.* 知 E/K 是代数扩张, 即 $\mathrm{tr.deg}\, E/K=0$. 由习题 4可知, $n=\mathrm{tr.deg}\, E/\mathbb{Q}=\mathrm{tr.deg}\, E/K+\mathrm{tr.deg}\, K/\mathbb{Q}$, 故 $\mathrm{tr.deg}\, K/\mathbb{Q}=n$. 如果 $\sigma_1,\cdots,\sigma_n$ 在 $\mathbb{Q}$ 上代数相关, 则有 $\mathrm{tr.deg}\, K/\mathbb{Q}<n$, 矛盾. 故 $\sigma_1,\cdots,\sigma_n$ 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.

♣ 考虑 $f(x)=\sum\limits_{i=0}^{n}(-1)^i\sigma_{n-i}x^i=\prod\limits_{i=1}^{n}(x-x_i)$, 知 $x_1,\ldots,x_n$ 均在 $\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$ 上整, 故 $\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}$ 在 $\mathbb{Z}[\sigma_1,\ldots,\sigma_n]$ 上整, 从而 $\mathbb{Z}[\sigma_1,\cdots,\sigma_n]\subseteq\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}$ 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.

♣ $\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$ 的分式域自然为 K, 且 $\mathrm{Frac}(\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n})\subset F$. 取 $\dfrac{f}{g}\in F=\mathbb{Q}(x_1,\cdots,x_n)^{\mathfrak{S}_n}$, 其中 f 与 g 互素, 对 $\tau\in\mathfrak{S}_n$, 由 $\tau(\dfrac{f}{g})=\dfrac{\tau(f)}{\tau(g)}$, 有 $f\tau(g)=g\tau(f)$. 由 f 与 g 互素, 说明 $\tau(g)\mid g$, 而 $\deg\tau(g)=\deg g$, 且最高次项系数相同, 说明 $g=\tau(g)$, 故 $f=\tau(f)$, 从而 $\dfrac{f}{g}\in\mathrm{Frac}(\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n})$. 这表明 $\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}$ 的分式域为 F.♢

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

♣ 由 $F=\mathbb{Q}(x_1,\cdots,x_n)^{\mathfrak{S}_n}$, $E=\mathbb{Q}(x_1,\cdots,x_n)$, 自然有 $\mathfrak{S}_n\subseteq\mathrm{Gal}(E/F)$, 从而由习题 5可知 $[E:K]\geq|\mathrm{Gal}(E/K)|\geq n!$. ♢

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

♣ 由 *1* 知 $[E:K]\leq n!$, 故由 $[E:F]\mid[E:K]$ 知 $[E:F]\leq n!$. 又由*6*知 $[E:F]\geq n!$,

从而 $[E:F]=n!$, 致使 $[F:K]=1$, 也即 $F=K$. 同时 $|\mathrm{Gal}(E/K)|\leq[E:K]=n!$, 说明 $|\mathrm{Gal}(E/K)|=n!$, 故 $\mathrm{Gal}(E/K)$ 中恰是 $\mathfrak{S}_n$ 中的全体元素, 即 $\mathrm{Gal}(E/K)=\mathfrak{S}_n$. ♢

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 $x\in R$.

♣ 由于 $\sigma_1,\ldots,\sigma_n$ 代数无关, 可知 $\mathbb{Z}[\sigma_1,\ldots,\sigma_n]$ 与 $\mathbb{Z}[x_1,\ldots,x_n]$ 之间存在环同构, 后者为 UFD, 故 $\mathbb{Z}[\sigma_1,\ldots,\sigma_n]$ 为 UFD. 由第三轮口试题目习题 1.3.*1*(所有 UFD 都是整闭整环), 知 $R=\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$ 为整闭整环. ♢

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

♣ 只需要证明 $\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}\subset\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$. 任取多项式 $h\in\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}$. 那么由*5*,$h$ 自然可视作 $\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}$ 分式域 K 中的元素. 由*7*, $F=K$, 故 $h\in F$, 即 h 是 $\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$ 分式域中的元素. 而由*4*知 h 在 $\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$ 上整, 故由*8*即 $\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$ 是整闭整环, 可知 $h\in\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$, 即 $\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}\subset\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$. 故 $\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n}=\mathbb{Z}[\sigma_1,\cdots,\sigma_n]$. ♢

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

♣ 有 $R\otimes_{\mathbb{Z}}\mathbb{Z}[\sigma_1,\cdots,\sigma_n]\simeq R[\sigma_1,\cdots,\sigma_n]$ 及 $R\otimes_{\mathbb{Z}}\mathbb{Z}[x_1,\cdots,x_n]\simeq R[x_1,\cdots,x_n]$. 令 $\mathfrak{S}_n$ 在 R 上平凡作用, 则给出 $\mathfrak{S}_n$ 在 $R\otimes\mathbb{Z}[x_1,\cdots,x_n]$ 上的作用 $\sigma\cdot(r\otimes f)=r\otimes(\sigma\cdot f)$, 也即给出作用 $F(x_1,\cdots,x_n)\in R[x_1,\cdots,x_n]$, $\sigma\cdot F=F(x_{\sigma(1)},\cdots,x_{\sigma(n)})$, 与所需的作用一致. 而由习题 6知 $R[\sigma_1,\cdots,\sigma_n]=R\otimes_{\mathbb{Z}}\mathbb{Z}[\sigma_1,\cdots,\sigma_n]=R\otimes_{\mathbb{Z}}(\mathbb{Z}[x_1,\cdots,x_n]^{\mathfrak{S}_n})\subseteq(R\otimes_{\mathbb{Z}}\mathbb{Z}[x_1,\cdots,x_n])^{\mathfrak{S}_n}=R[x_1,\cdots,x_n]^{\mathfrak{S}_n}$. 令一方面, 若给出 $F\in(R\otimes_{\mathbb{Z}}\mathbb{Z}[x_1,\cdots,x_n])^{\mathfrak{S}_n}$, 则有 $F=\sum\limits_{i=1}^{m}r_i\otimes f_i$, 且 $\sum\limits_{i=1}^{m}r_i\otimes f_i=\dfrac{1}{|\mathfrak{S}_n|}\sum\limits_{\sigma\in\mathfrak{S}_n}\sigma\left(\sum\limits_{i=1}^{m}r_i\otimes f_i\right)=\dfrac{1}{|\mathfrak{S}_n|}\sum\limits_{\sigma\in\mathfrak{S}_n}\sum\limits_{i=1}^{m}r_i\otimes$

$(\sigma f_i) = \sum_{i=1}^{m} r_i \otimes \left(\frac{1}{|\mathfrak{S}_n|} \sum_{\sigma \in \mathfrak{S}_n} \sigma f_i \right) \in R \otimes_{\mathbb{Z}} (\mathbb{Z}[x_1, \cdots, x_n]^{\mathfrak{S}_n})$, 故反向包含也成立, 进而得到 $R[x_1, \cdots, x_n]^{\mathfrak{S}_n} = R[\sigma_1, \cdots, \sigma_n]$. ♢

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

4. 对任意 $\alpha \in E$, α 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 $\forall 1 \leq j \leq n$, α_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 $\forall 1 \leq j \leq n$, α_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.

♣ 利用讲义 2022-05-23习题 5, 可知 *1.* 中 E/F 为正规扩张 $\Leftrightarrow |\mathrm{Gal}(E/F)| = |\mathrm{Hom}_F(E, \bar{F})|$, 后者即为 *2.* 对于 $\alpha \in E, \alpha$ 的共轭根均在某个 $\sigma(\alpha)$ 中, $\sigma \in \mathrm{Hom}_F(E, \bar{F})$, 故 $\mathrm{Hom}_F(E, \bar{F}) \subset \mathrm{Gal}(E/F) \Leftrightarrow$*3.* 进一步地, *3* 与 *4* 自然等价, 故前四条等价. 另外 *5* 与 *6* 等价, 且 *3* 蕴含 *5.* 下证 *5* $\Rightarrow$ *1.* 任给 $\sigma \in \mathrm{Hom}_F(E, \bar{F})$, 由于 $\sigma(\alpha_j)$ 仍为 f_j 的多项式, 故仍在 E 中, 也即 $\sigma(E) = F(\sigma(\alpha_1), \cdots, \sigma(\alpha_n)) \subseteq F(\alpha_1, \cdots, \alpha_n) = E$, 即正规.♢

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

♣ 是正规扩张. 因为 $\sqrt{2}$ 在 $\mathbb{Q}$ 上的极小多项式 x^2-2 在 $\mathbb{Q}(\sqrt{2})[x]$ 上分裂. ♢

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

♣ 不是正规扩张, 因为 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的极小多项式在 $\mathbb{Q}(\sqrt[3]{2})[x]$ 中分解为 $(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}+\sqrt[3]{4})$, 其余两根为 $\sqrt[3]{2}\omega$ 和 $\sqrt[3]{2}\omega^2$, 而 $\mathbb{Q}[\sqrt[3]{2}]\subseteq\mathbb{R}$, 故极小多项式不能分裂为一次因子的乘积. ♢

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

♣ 是正规扩张. 因为 $\mathbb{Q}(\zeta_N)$ 作为有限生成扩张, 其生成元 ζ_N 的所有共轭根 $\zeta_N^i, 1\leq i\leq N-1, pgcd(N,i)=1$ 均在 $\mathbb{Q}(\zeta_N)$ 中. ♢

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

♣ 是正规扩张. 因为 $t^{\frac{1}{p}}$ 在 F 上的的极小多项式 x^p-t 在 $E[x]$ 上分裂为 $(x-t^{\frac{1}{p}})^p$, 为一次因子的乘积. ♢

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.

♣ 若 K/F 为正规扩张, 则 K 中任意元素 α 在 F 上的极小多项式在 $K[x]$ 中分裂. 由于 α 在 E 上的极小多项式一定是其在 F 上极小多项式的因子, 因而也在 $K[x]$ 中分裂. 故 K/E 一定是正规扩张.

K/F 是正规扩张而 E/F 不是正规扩张的例子: $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$. ♢

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.

♣ 考虑 $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$, 此时 $\sqrt[4]{2}$ 的极小多项式为 $x^4 - 2$, 其有四个根 $\sqrt[4]{2}i^n$, $0 \leq n \leq 3$, 其中 $n = 1, 3$ 时非实数, 但 $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$, 这说明 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 不是正规扩张. ♢

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 α_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 $\tilde{E} := F(\alpha_{ji},\ 1 \leq j \leq n,\ 1 \leq i \leq k_j)$. 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.

♣ 取 $\bar{F}$ 为 F 的代数闭包, 设 f 在 $\bar{F}$ 中的所有根为 $\alpha_1, \ldots, \alpha_n$, 则 $E = F(\alpha_1, \ldots, \alpha_n)$. 对任意 $1 \leq i \leq n$, 均有 α_i 在 F 上的极小多项式均是 f 的因子, 从而无重根且在 $E[x]$ 中分裂, 这说明 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. $|\mathrm{Gal}(E/F)| \leq |\mathrm{Hom}_F(E, \bar{F})|$, 并且等号成立 $\Leftrightarrow$ E/F 为正规扩张.

♣ 由定义, 显然有 $\mathrm{Gal}(E/F) \subset \mathrm{Hom}_F(E, \bar{F})$, 故 $|\mathrm{Gal}(E/F)| \leq |\mathrm{Hom}_F(E, \bar{F})|$. 等号成立表明 $\mathrm{Hom}_F(E, \bar{F}) \subset \mathrm{Gal}(E/F)$, 即 E/F 为正规扩张. ♢

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

♣ 见讲义 2022-05-18习题 1. ♢

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

♣ 由*1*和*2*立刻得到此结论. ♢

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.

♣ 由习题 1可看出 *1* 与 *2* 等价. 若 *3* 成立, 则 $E \simeq F(\alpha_1, \ldots, \alpha_n)$, 其中 $\alpha_1, \ldots, \alpha_n$ 是 $f(x)$ 在 $\bar{F}$ 中的所有根. 对每个 α_i, 均有 α_i 的极小多项式无重根, 且在 E 中分裂, 因而 E/F 为既正规又可分的扩张, 即 *3* 蕴含 *2*. 另一方面, 如果 *2* 成立, 设 $E = F(\alpha_1, \ldots, \alpha_n)$, 则每个 α_i 的极小多项式 f_i 都在 E 上分裂且无重根, 不妨假设 $f_1, \cdots, f_m$

两两不同, 而 $f_{m+j},\ 1\leq j\leq n-m$ 均等于前 m 个中的某个 f_i, 考虑 $f=\prod\limits_{i=1}^{m}f_i$, 则 f 在 E 上分裂且无重根 (因为每个 f_i 在 $F[x]$ 中都是不可约的, 彼此一定互素, 也即无公共根), 且每个 α_i 均为 f 的根, 故 E 为 f 在 F 上的分裂域. 这即推出了 *3.* ♢

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 $f(\alpha)=0,\ \deg f\leq n$, 并且 f 无重根.

♣ 设 α 在 G 作用下的轨道为: $G\cdot\alpha=\{\alpha_1,\ldots,\alpha_m\}$, 令 $f(x)=(x-\alpha_1)\cdots(x-\alpha_m)$. 注意 G 作用在 f 上相当于置换一次因式 $x-\alpha_i$, 也即是说不会改变 f 的因式分解, 因此将 f 展开后, 其每项系数在 G 的作用下也不会改变, 这说明 $f(x)\in F[x]$. 容易看出 $f(\alpha)=0$, 且无重根. 另一方面, 轨道长自然不超过群的阶, 故 $m\leq n$. ♢

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 $[E_1:F]\leq n$.

♣ 由 *1*, 每个 E 中元素在 F 上都是代数的, 且次数不超过 $n=|G|$. 考虑中间域 E_1, 则 E_1 中任意元素在 F 上有无重根的零化多项式, 因而极小多项式也无重根. 由于 E_1/F 是有限扩张, 由讲义 2022-05-18定理 1(即单扩张定理), 存在 $\beta\in E_1$, 使得 $E_1=F(\beta)$. 而 β 在 F 上的次数不超过 n, 着说明 $[E_1:F]\leq n$. ♢

3. E/F 为有限扩张, 且 $[E:F]\leq n$.

♣ 取 $x\in E$, 使得 x 在 F 上的次数 (即 $[F(x):F]$) 是所有 E 中元素中最大的 (因为这个次数不超过 n, 所以这样的 x 总可以取到). 我们证明 $E=F(x)$. 对任意 $y\in E$, 考虑域 $E'=F(x,y)$, 则由单扩张定理, 存在 $z\in F(x,y)\subset E$, 使得 $E'=F(z)$. 于是 $F(x)\subset F(z)$. 但是 $[F(x):F]\geq[F(z):F]=[F(z):F(x)][F(x):F]\geq[F(x):F]$,

这表明 $[F(z):F(x)]=1$, 从而 $F(x)=F(z)$, 也即 $y\in F(x)$. 由 y 的任意性, 可知 $E\subset F(x)$, 故 $E=F(x)$, 从而 E/F 为有限扩张, 且 $[E:F]\leq n$. ♢

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

♣ 由*3*可以知道 $E=F(x)$, 而 x 在 F 上的极小多项式是在 E 里分裂且无重根的, 从而 E/F 为 Galois 扩张, 故 $n=|G|\leq|\mathrm{Gal}(E/F)|\leq[E:F]\leq n$, 可知 $|\mathrm{Gal}(E/F)|=n$, 也即 $\mathrm{Gal}(E/F)=G$. ♢

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 $F=E^G$.

♣ 若 *1* 成立, 考虑 $Aut(E)$ 的子群 $G=\mathrm{Gal}(E/F)$, 则由习题 3, E/E^G 为 Galois 扩张, 且 $[E:E^G]=|G|=[E:F]$. 而 $F\subset E^G\subset E$, 这给出 $E^G=F$, 即 *2* 成立. *2* 平凡地蕴含 *3*. 若 *3* 成立, 由习题 3, 可知 $E/F=E/E^G$ 为 Galois 扩张, 即为 *1*. 故这三条互相等价. ♢

注: Artin 引理事实上从自同构群的固定域的角度给出了 Galois 扩张的一种刻画.

• 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.

♣ 事实上, E 为 $f(x) = x^{q^n} - x \in F[x]$ 在 F 上的分裂域. 对 f 求导, 有 $f' = -1$, 故 f 无重根. 因此 E/F 为 Galois 扩张. 计数可知 E 为 F 上的 n 维向量空间, 故 $[E : F] = n$. 考虑 $\mathrm{Gal}(E/F)$. 由于 $Fr|_F = id_F$, 故 $Fr \in Gal(E/F)$. 另一方面, E^* 为循环群, 从而存在 $x \in E^*$, 使得 $\langle x\rangle = E^*$. 因此 $Fr^m(x) = x^{p^m} \neq x, \forall m \leq n-1$. 因此 Fr 在 $\mathrm{Gal}(E/F)$ 中的阶数至少是 n, 而 $|\mathrm{Gal}(E/F)| = [E : F] = n$, 知 $\mathrm{Gal}(E/F)$ 就是由 Fr 生成的 n 阶循环群, 即 $\mathrm{Gal}(E/F) = \langle Fr\rangle \simeq \mathbb{Z}/n\mathbb{Z}$. ♢

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 $f(x) = x^n + t_1x^{n-1} + t_2x^{n-2} + \cdots + t_n \in F[x]$. 设 E 为 f 在 F 上的分裂域. 则 E/F 为 Galois 扩张, 且 $\mathrm{Gal}(E/F) \simeq \mathfrak{S}_n$.

♣ 先证明 $f(x) \in F[x]$ 不可约, 再由特征 0 可知 $f(x)$ 无重根. 令 $A = \mathbb{Q}[t_1, \cdots, t_n]$ 为多项式环, 进而是 UFD, 且 F 为 A 的分式域. 考虑 $\mathbb{Q}$-代数之间的同态:

$$\varphi\colon A \to \mathbb{Q}, t_i \mapsto p,$$

其中 p 为一素数. φ 通过在系数上的作用诱导了 $A[x]$ 到 $\mathbb{Q}[x]$ 的映射. 如果 $f(x)$ 在 $A[x]$ 中可约, 则 $\varphi(f(x)) \in \mathbb{Q}[x]$ 可约. 但是 $\varphi(f(x)) = x^n + px^{n-1} + \ldots + p$, 由 Einsenstein 判别法可知 $\varphi(f(x))$ 是 $\mathbb{Q}[x]$ 中的不可约多项式. 因此 $f(x)$ 是 $A[X]$ 中的不可约无重根多项式, 进而在 F 上不可约. 其在 F 上的分裂域 E 满足 E/F 是 Galois 扩张. 记 $f(x)$ 在 E 中的 n 个根为 $\alpha_1, \ldots, \alpha_n$, 则对于 $\sigma \in \mathrm{Gal}(E/F), \sigma$ 的作用由 $\sigma(\alpha_i), 1 \leq i \leq n$ 所

决定. 注意到 $f(x)\in F[x]$, 其系数在 σ 的作用下保持不变, 故有

$$f(x)=\sigma(f(x))=(x-\sigma(\alpha_1))\cdots(x-\sigma(\alpha_n))$$

可知 σ 在这 n 个互异根上的作用是置换, 因而在相差一个同构的情况下 $\mathrm{Gal}(E/F)\subset\mathfrak{S}_n$.

另一方面, 若 f 的 n 个根在 $\mathbb{Q}$ 上代数相关, 即存在 $p(X_1,\cdots,X_n)\in\mathbb{Q}[X_1,\cdots,X_n]\backslash\{0\}$, 使得 $p(\alpha_1,\cdots,\alpha_n)=0$, 则考虑 $P(X_1,\cdots,X_n)=\prod\limits_{\sigma\in\mathfrak{S}_n}p(X_{\sigma(1)},\cdots,X_{\sigma(n)})$, 于是将有 $P(X_1,\cdots,X_n)=P(X_{\sigma(1)},\cdots,X_{\sigma(n)})\forall\sigma\in\mathfrak{S}_n$. 由对称多项式基本定理, 存在 $Q\in\mathbb{Q}[X_1,\cdots,X_n]$ 使得 $Q(\tau_1,\cdots,\tau_n)=P(X_1,\cdots,X_n)$, 其中 τ_i 为 $X_1,\cdots,X_n$ 的 i 次初等对称多项式. 于是有 $Q((-1)t_1,\cdots,(-1)^nt_n)=P(\alpha_1,\cdots,\alpha_n)=0$. 但另一方面,$P\neq0$, 于是 $Q\neq0$, 给出各 t_i 间代数相关, 矛盾. 故 $\mathbb{Q}[\alpha_1,\cdots\alpha_n]\simeq\mathbb{Q}[X_1,\cdots,X_n]$, 上面带有 $\mathfrak{S}_n$ 的自然作用, 进而按以下诱导 $\mathfrak{S}_n$ 在 $\mathbb{Q}(\alpha_1,\cdots,\alpha_n)$ 上的作用 $\tilde{\sigma}$

$$\begin{array}{ccc}\mathbb{Q}[\alpha_1,\cdots,\alpha_n] & \xrightarrow{\ i\ } & \mathbb{Q}(\alpha_1,\cdots,\alpha_n)\\ \downarrow{\scriptstyle\sigma} & & \downarrow{\scriptstyle\exists\tilde{\sigma}}\\ \mathbb{Q}[\alpha_{\sigma(1)},\cdots,\alpha_{\sigma(n)}] & \xrightarrow{\ i\ } & \mathbb{Q}(\alpha_{\sigma(1)},\cdots,\alpha_{\sigma(n)})\end{array}$$

且易见 $\mathbb{Q}(t_1,\cdots,t_n)$ 在 $\tilde{\sigma}$ 的作用下不动, 各 $\tilde{\sigma}$ 的作用不同, 于是给出 $\mathfrak{S}_n\subseteq\mathrm{Gal}(E/F)$, 故给出 $\mathrm{Gal}(E/F)=\mathfrak{S}_n$. ♢

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

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

♣ 由讲义 2022-03-16习题 5后的注可知 ζ_N 在 $\mathbb{Q}$ 上的极小多项式是 $\Phi_N(x)$, 这个不可约多项式的所有根为: $\zeta_N^i, 1 \leq i \leq N-1$, $pgcd(i,N)=1$, 因此 ζ_N 在 $\mathbb{Q}$ 上的极小多项式无重根, 且在 $\mathbb{Q}(\zeta_N)$ 中分裂. 故 $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ 为 Galois 扩张. 取 $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N/)\mathbb{Q})$. 为确定 σ 的作用, 只需确定 $\sigma(\zeta_N)$, 而由于所有共轭根都在 $\mathbb{Q}(\zeta_N)$ 中, 这相当于选取一个 i, 使得 $1 \leq i \leq N-1$, $pgch(i,N)=1$, 将相应自同构记为 σ_i. 故 $\sigma_i(\sigma_j(\zeta_N)) = \sigma_i(\zeta_N^j) = \sigma_i(\zeta_N)^j = \zeta_N^{ij} = \sigma_{ij}(\zeta_N)$. 因此, 该扩张的 Galois 群同构于乘法群 $(\mathbb{Z}/N\mathbb{Z})^*$. ♢

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 ζ_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

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

♣ 由条件, $\sqrt[n]{a}$ 在 F 上的极小多项式无重根, 且在 E 中分裂. 故 E/F 为 Galois 扩张. 任取 $\sigma \in \mathrm{Gal}(E/F)$, σ 由 $\sqrt[n]{a}$ 决定. 由于 $\sigma(\sqrt[n]{a})$ 是 $\sqrt[n]{a}$ 的共轭根, 因而一定存在 $1 \leq i \leq n$, 使得 $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n^i$, 将这个自同构记为 σ_i, 则 $\sigma_i(\sigma_j(\sqrt[n]{a})) = \sigma_i(\sqrt[n]{a}\zeta_n^i) = \sqrt[n]{a}\zeta_n^{i+j} = \sigma_{i+j}$. 因此, 该扩张的 Galois 群同构于加法群 $\mathbb{Z}/n\mathbb{Z}$. ♢

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:

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

♣ 设 $f(x)$ 在 $F[x]$ 中分解为 $f = g_1 \cdots g_r$, 其中 $g_1, \ldots, g_r$ 均不可约, 故 h 和 g. 取 $g_1(x)$ 在 F 的代数闭包 $\bar{F}$ 中的一个根 α, 则 $F(\alpha)$ 是 F 上的域扩张. 考虑 $f(\alpha+1) = (\alpha+1)^p - (\alpha+1) - a = (\alpha^p+1) - (\alpha+1) - a = f(\alpha) = 0$, 可知 $\alpha+1$ 也是 f 的一个根, 进而 $\alpha+i, 1 \leq i \leq p-1$ 均是 f 的根. 因此 $F(\alpha)$ 是 f 的分裂域. 故 $\deg g_1 = [F(\alpha) : F]$. 但是 $[F(\alpha) : F]$ 为一定值 n, 故 $\deg g_1 = \ldots = \deg g_r = n$, 这给出 $p = \deg f = \deg g_1 + \ldots \deg g_r = rn$. 由于 $f(x)$ 在 F 上无根, 可知 $\deg g_i \geq 2$, 这只能推出 $r = 1, n = p$. 故 $f(x)$ 在 $F[X]$ 中不可约. 从上面的过程中, 我们看到, 若记 $E = F(\alpha)$, 有 α 在 F 上的极小多项式 $f(x) = x^p - x - a$ 无重根, 且在 $E[x]$ 中分裂, 故 E/F 为 Galois 扩张. 取 $\sigma \in \mathrm{Gal}(E/F)$, 则存在 i, $0 \leq i \leq p-1$, 使得 $\sigma(\alpha) = \alpha + i$, 将这个自同构记为 σ_i, 则 $\sigma_i(\sigma_j(\alpha)) = \sigma_i(\alpha + j) = \alpha + i + j$. 故该扩张的 Galois 群同构于加法群 $\mathbb{Z}/p\mathbb{Z}$. ♢

• 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 φ, ψ 为互逆映射.

♣ 对 $K \in M$, $H \in S$ 由定义可知: $K \subset \varphi(\psi(K)) = E^{\mathrm{Gal}(E/K)}, H \subset \psi(\varphi(H)) = \mathrm{Gal}(E/E^H)$. 为说明 $K = E^{\mathrm{Gal}(E/K)}$, 我们援引习题 4.2即可. 为说明 $H = \mathrm{Gal}(E/E^H)$, 我们援引习题 3.4即可. 这就说明 φ, ψ 为互逆映射. ♢

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

♣$H_1 \subset H_2$ 自然可以推出 $E^{H_2} \subset E^{H_1}$. 另一方面, 如果 $E^{H_2} \subset E^{H_1}$, 则 $H_1 = \mathrm{Gal}(E/E^{H_1}) \subset Gal(E/E^{H_2}) = H_2$. 故 $H_1 \subseteq H_2 \Leftrightarrow E^{H_2} \subset E^{H_1}$. ♢

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: $\sigma \mapsto \sigma|_{E^H}$.

♣ 首先 E^H/F 为可分扩张, 这是因为 E/F 为有限可分扩张, 关键在于判定 E^H/F 是否为正规扩张. 由于 E/F 为正规扩张, 我们先证明: E^H/F 为正规扩张 $\Leftrightarrow \forall \sigma \in Aut_F(E), \sigma(E^H) = E^H$.

$\Leftarrow$: 任取 $\sigma \in \mathrm{Hom}_F(E^H, \bar{F})$. 由讲义 2022-05-16习题 7, 域同态 $\sigma : E^H \hookrightarrow \bar{F}$ 可以延拓到 E 上: $\tilde{\sigma}\colon E \hookrightarrow \bar{F}$. 由于 E/F 为正规扩张, $\mathrm{Im}\tilde{\sigma} = M$. 故 $\tilde{\sigma} \in Aut_F(E)$, 由条件, 其在

E^H 上的限制 $\tilde{\sigma}|_{E^H}$, 即 σ, 满足 $\sigma(E^H) = E^H$. 故 $\mathrm{Hom}_F(E^H, \bar{F}) \subset \mathrm{Gal}(E^H/F)$, 这就说明了 E^H/F 是正规扩张.

$\Rightarrow$ 对 $\sigma \in Aut_F(E)$, 总有 $\sigma|_{E^H} : E^H \hookrightarrow E \subset \bar{F}$. 由于 E/E^H 是正规扩张, 有 $\sigma|_{E^H} \subset \mathrm{Hom}_F E^H, \bar{F} = \mathrm{Gal}(E^H/F)$, 即给出 $\sigma|_{E^H}(E^H) = E^H$.

借此, 注意到 $\sigma(E^H) = E^{\sigma H \sigma^{-1}}$(因为 $h(x) = x \Leftrightarrow \sigma h \sigma^{-1}(\sigma(x)) = \sigma h(x) = x, \forall \sigma \in Gal(E/F), \forall x \in F$. 故 $x \in E^H \Leftrightarrow \sigma(x) \in E^{\sigma H \sigma^{-1}}$), 可知 E^H/F 为正规扩张等价于 $\forall \sigma \in \mathrm{Gal}(E/F), E^{\sigma H \sigma^{-1}} = E^H$. 由 *2* 知这等价于 $H = \sigma H \sigma^{-1}, \forall \sigma \in \mathrm{Gal}(E/F)$, 即 H 为 G 的正规子群. 此时, E^H/F 为正规扩张, $\sigma(E^H) = E^H$ 表明 $\mathrm{Gal}(E/F)$ 中的元素均稳定 E^H, 于是有映射:

$$\rho : \mathrm{Gal}(E/F) \to Gal(E^H/F), \sigma \mapsto \sigma|_{E^H}$$

容易验证, ρ 是一个群同态. 进一步地, ρ 是满射. 事实上, 对正规扩张 E/E^H, 考虑映射 $j : E^H \hookrightarrow E$, 对 $h \in \mathrm{Gal}(E^H/F)$, 由讲义 2002-05-16习题 7, 有延拓 $\tilde{h} \in Aut(E)$, 使得 $\tilde{h}|_{E^H} = h$. 记 $\iota : F \to E^H$, 由延拓定义可知 $\tilde{h} \circ j = j \circ h$, 因此 $\tilde{h} \circ j \circ \iota = j \circ h \circ \iota = j \circ \iota$, 也即 $\tilde{h}|_F = Id|_F$. 于是 $\tilde{h} \in \mathrm{Gal}(E/F)$.

考虑 $\ker \rho$:

$$\ker \rho = \{\sigma \in \mathrm{Gal}(E/F), \sigma|_{E^H} = Id|_{E^H} = Aut_{E^H}(E) = \mathrm{Gal}(E/E^H)\}$$

也即是说:

$$\mathrm{Gal}(E/F)/H = \mathrm{Gal}(E/F)/\ker \rho \simeq \mathrm{Im}\rho = \mathrm{Gal}(E^H/F)$$

这也就给出了正合列

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

♢

思考: 如果 $H \leq G$ 为子群, 不一定是正规子群, 那么对于 $\sigma \in G$, H 对应的中间域 E^H 和 $H' := \sigma H \sigma^{-1}$ 对应的中间域 $E^{H'}$ 有什么关系?

♣ 从上面的证明中我们可以看到:$E^{H'} = E^{\sigma H \sigma^{-1}} = \sigma(E^H)$. ♢

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 α 的迹 (trace) 为 $Tr_{E/F}(\alpha) := \mathrm{tr}\varphi_\alpha$, 定义 α 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.

♣ $Tr_{E/F}(\alpha+\beta) = \mathrm{tr}\varphi_{\alpha+\beta} = \mathrm{tr}(\varphi_\alpha + \varphi_\beta) = \mathrm{tr}\varphi_\alpha + \mathrm{tr}\varphi_\beta = Tr_{E/F}(\alpha) + Tr_{E/F}(\beta)$.

$N_{E/F}(\alpha\beta) = \det \varphi_{\alpha\beta} = \det(\varphi_\alpha \circ \varphi_\beta) = \det \varphi_\alpha \cdot \det \varphi_\beta = N_{E/F}(\alpha)N_{E/F}(\beta)$. ♢

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

♣ 设 $[E:F] = n$. 取 E 作为 $F-$ 线性空间的一组基 $x_1, \ldots, x_n$, 则 φ_α 在这组基下的矩阵为 αI_n, 故 $Tr_{E/F}(\alpha) = n\alpha = [E:F]\alpha,\ N_{E/F}(\alpha) = \alpha^n = \alpha^{[E:F]}$. ♢

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 α 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 $f(x)$.

♣ 可以取 E 作为 F-线性空间的一组基为 $1, \alpha, \ldots, \alpha^{n-1}$, 则 φ_α 在这组基下的矩阵为

$$C_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

也即是说, E 为 φ_α-循环空间. 注意到 $1, \varphi_\alpha(1) = \alpha, \ldots, \varphi_\alpha^{n-1}(1) = \alpha^{n-1}$ 线性无关, 知 α 的极小多项式一定是 n 次的, 即为其特征多项式 $f(x)$. ♢

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 α 在 F 上的极小多项式. 证明: $Tr_{E/F}(\alpha) = -[E : F(\alpha)]a_{n-1}, N_{E/F}(\alpha) = ((-1)^n a_0)^{[E:F(\alpha)]}$.

♣ 设 $[E : F] = m$, E 作为 $F(\alpha)$-线性空间的一组基为 $e_1, \ldots, e_m$, 则 $E = \oplus_{i=1}^m F(\alpha)e_i$ 为 φ_α-不变 (循环) 子空间分解. 具体而言, 若取 $1, \alpha, \ldots, \alpha^{n-1}$ 作为 $F(\alpha)$ 的一组 F-线性空间的基, 则 $e_i\alpha^j, 1 \le i \le m, 0 \le j \le n-1$ 成为 E 作为 F-线性空间的一组基, 且 φ_α 在这组基下的矩阵为 $C_f \otimes I_m$, 其中 C_f 即为习题 2中出现的 $f(x)$ 的伴随矩阵. 故 $Tr_{E/F}(\alpha) = m \cdot \mathrm{tr} C_f = -[E : F(\alpha)]a_{n-1}, N_{E/F}(\alpha) = (\det C_f)^m = ((-1)^n a_0)^{[E:F(\alpha)]}$. ♢

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: $Tr_{E/F}(x) = \sum_{i=1}^n \sigma_i(x)$, $N_{E/F}(x) = \prod_{i=1}^n \sigma_i(x)$.

♣ 由讲义 2022-05-18定理 1(单扩张定理) 可知, 存在 $\alpha \in E$, 使得 $E = F(\alpha)$, 而 α 在 F 上的极小多项式就是 $f(x) = \prod_{i=1}^n (x - \sigma_i(\alpha))$, 这个多项式无重根. 任取一组基, 则 φ_α 在这组基下的矩阵被 $f(x)$ 零化, 因而该矩阵可对角化, 其特征值正是 $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$, 也即是说 φ_α 在某组基下的矩阵是 $D = \mathrm{diag}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$.

一般情况下, 设 $x \in E = F(\alpha)$, 则存在多项式 $P \in \mathbb{F}[x]$, 使得 $x = P(\alpha)$. 任取一组基, 如果 φ_α 在这组基下对应的矩阵是 A, 则 φ_x 在这组基下对应的矩阵就是 $W = P(A)$,

故使得 φ_α 对应矩阵为对角阵的基也同时使 φ_x 对应的矩阵成为对角阵. 特别地, 这个对角阵的对角元就是 $P(\sigma(\alpha))=\sigma(P(\alpha))=\sigma(x)$, 故有 $Tr_{E/F}(x)=\sum\limits_{i=1}^{n}\sigma_i(x)$, $N_{E/F}(x)=\prod\limits_{i=1}^{n}\sigma_i(x)$. ♢

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 $\alpha\in E$, $Tr_{E/F}(\alpha)=\sum\limits_{i=0}^{n-1}\alpha^{q^i}$, $N_{E/F}(\alpha)=\alpha^{\sum_{i=0}^{n-1}q^i}$.

♣ 由讲义 2022-05-30例 1可知, $\mathrm{Gal}(E/F)$ 为由 Frobenius 自同态 $Fr\colon x\mapsto x^q$ 生成的 n 阶循环加法群. 引用习题 4的结果即可得到 $Tr_{E/F}(\alpha)=\sum\limits_{i=0}^{n-1}Fr^i(\alpha)=\sum\limits_{i=0}^{n-1}\alpha^{q^i}$, $N_{E/F}(\alpha)=\prod\limits_{i=0}^{n-1}Fr^i(\alpha)=\prod\limits_{i=0}^{n-1}\alpha^{q^i}=\alpha^{\sum_{i=0}^{n-1}q^i}$. ♢

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

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

♣ 由于 $N_{E/F}$ 是乘法群同态, 且 $\det(\psi_1\circ\psi_2)=\det\psi_1\cdot\det\psi_2\in E$, 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: $N_{E/F}(\det\psi)=\det\psi_F$.

♣ 由 ψ 可对角化, 不妨设 ψ 在 K 作为 E-线性空间的一组基 $k_1,\dots,k_m$ 下成为对角阵 $D=\mathrm{diag}(d_1,\dots,d_m)$, 则 $\det\psi=\prod\limits_{i=1}^{m}d_i$. 固定 E 作为 F-线性空间的一组基 $e_1,\dots,e_n$, 并记 φ_{d_i} 在这组基下的矩阵为 D_i, 则 $N_{E/F}(\det\psi)=N_{E/F}(\prod\limits_{i=1}^{m}d_i)=\prod\limits_{i=1}^{m}N_{E/F}(d_i)=$

$\prod_{i=1}^{m} \det D_i$. 另一方面, 把 ψ 看作 K-上的 F-线性变换时, $(e_i k_j, 1 \le i \le n, 1 \le j \le m)$ 成为 K 作为 F-线性空间的一组基, 且在这组基下的矩阵为分块对角阵 $\mathrm{diag}(D_1, \ldots, D_n)$. 故 $\det \psi_F = \prod_{i=1}^{n} \det D_i$. 比较两式即有 $N_{E/F}(\det \psi) = \det \psi_F$. ♢

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

♣ 类似于*2*的思路, 设 ψ 在 K 作为 E-线性空间的一组基 $k_1, \ldots, k_m$ 下成为上三角阵, 对角元为 $d_1, \ldots, d_m$, 则 $\det \psi = \prod_{i=1}^{m} d_i$. 固定 E 作为 F-线性空间的一组基 $e_1, \ldots, e_n$, 并记 φ_{d_i} 在这组基下的矩阵为 D_i, 则 $N_{E/F}(\det \psi) = N_{E/F}(\prod_{i=1}^{m} d_i) = \prod_{i=1}^{m} N_{E/F}(d_i) = \prod_{i=1}^{m} \det D_i$. 另一方面, 把 ψ 看作 K-上的 F-线性变换时, $(e_i f_j, 1 \le i \le n, 1 \le j \le m)$ 成为 K 作为 F-线性空间的一组基, 且在这组基下的矩阵为分块上三角阵阵, 对角部分为 $D_1, \ldots, D_n$. 故 $\det \psi_F = \prod_{i=1}^{n} \det D_i$. 比较两式即有 $N_{E/F}(\det \psi) = \det \psi_F$. ♢

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

♣ 类似*2*和*3*, 可以证明如果 ψ 在 K 作为 E-的线性空间的某组基下是下三角矩阵或置换矩阵, 那么同样的结果也成立. 而每个矩阵总可以写成一些初等矩阵和对角阵的乘积 (Gauss 消元), 进而是一些上三角矩阵、下三角矩阵和置换矩阵的乘积, 于是利用*1*的结果, 可知对任意 $\psi \in End_E(K)$, 总有 $N_{E/F}(\det \psi) = \det \psi_F$. ♢

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

♣ 对任意 $\alpha \in K$, 在*4*取 $\psi = \varphi_\alpha$, 则有 $N_{E/F} \circ N_{K/E}(\alpha) = N_{E/F}(\det \varphi_\alpha) = \det(\varphi_{\alpha,F}) = N_{K/F}(\alpha)$. ♢

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 $Tr_{E/F} \circ Tr_{K/E} = Tr_{K/F}$.

♣ 模仿前五小问, 首先说明对于 $\psi_1, \psi_2 \in End_E(K)$, 有 $Tr_{E/F}(\mathrm{tr}(\psi_1 + \psi_2)) =$

$Tr_{E/F}(\mathrm{tr}\psi_1) + Tr_{E/F}(\mathrm{tr}\psi_2)$. 再对 $\psi \in End_E(K)$ 为可对角化或可上 (下) 三角化的情况, 证明 $Tr_{E/F}(\mathrm{tr}\psi) = \mathrm{tr}\psi_F$. 注意到每个矩阵总可以写成上三角矩阵和下三角矩阵的和, 即可证明对任意 $\psi \in End_E(K)$, $Tr_{E/F}(tr\psi) = tr\psi_F$. 特别地, 对 $\alpha \in K$, 我们将 ψ 取作 φ_α, 即可证明 $Tr_{E/F} \circ Tr_{K/E} = Tr_{K/F}$. ♢

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.

♣ 验证定义即可. 记 $a = t^{\frac{1}{p}}$, 有 $a^p = t \in F$. 一般地, E 中的元素可以写作 $h = \sum_{i=0}^{p-1} c_i a^i$, 其中 $c_i \in F, 0 \le i \le p-1$. 考虑在特征 p 下, 有

$$h^p = (\sum_{i=0}^{p-1} c_i a^i)^p = \sum_{i=0}^{p-1} c_i^p a^{ip}$$

上式右端每一项均在 F 中, 故 $h^p \in F$. 这就说明了 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. $|\mathrm{Hom}_F(E, \bar{F})| = 1$.

♣ 对 $\forall a \in E$, 存在正整数 n, 使得 $a^{p^n} = b \in F$. 因此,$f(x) = x^{p^n} - b = (x-a)^{p^n}$ 是 a 的一个零化多项式. 可见 $f(x)$ 只有一个根, 故 a 的极小多项式也只有 a 这一个根, 也即是说 a 的共轭元只有 a 自己, 所以 $|\mathrm{Hom}_F(E, \bar{F})| = 1$. ♢

2. $[E : F]$ 为 p 的幂次.

♣ 由于 E/F 是有限扩张, 自然是有限生成扩张, 我们将其写成一些单扩张的复合. 由定义, 这些单扩张都是纯不可分扩张, 故只需证明: 对纯不可分扩张 $F(\alpha)/F$, 有 $[F(\alpha):F]$ 为 p 的幂次. 考虑 α 在 F 上的极小多项式 $g(x)$. 由于存在正整数 n 和 $b\in F$, 使得 $f(x)=x^{p^n}-b=(x-a)^{p^n}$ 为 a 的一个零化多项式, 所以 $g(x)$ 一定只有一个根 a. 由于 $g(x)$ 是不可约多项式, 且 $char\ F=p$, 其导数 $g'(x)$ 必须为 0, 也即是说存在 $g_1(x)\in F[x]$, 使得 $g(x)=g_1(x^p)$. 注意到 $g_1(x)$ 也不可约 (否则 $g(x)=g_1(x^p)$ 可约), 如果 $g_1(x)$ 有重根 (由于 $g_1(x)$ 也只有一个根: 这个根是 $\bar{F}$ 中唯一满足 x^p-a 的元素, 故 $g_1(x)$ 有重根当且仅当 $\deg g_1>1$), 则一定存在 $g_2(x)\in F[x]$, 使得 $g_1(x)=g_2(x^p)$. 注意到这个过程中多项式的次数在严格递减, 因此一定存在整数 $\mu\geq 0$, 使得 $g_p(x)$ 的 deg 为 1. 不妨记 $g_\mu(x)=x-t\in F[x]$, 则 $g(x)=g_p(x^{p^\mu})=x^{p^\mu}-t$. 故 $[E:F]=\deg g=p^\mu$, 为 p 的幂次. ♢

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

♣ 由于 E/F 为纯不可分扩张, 由2.可知, 存在整数 μ 使得 $f(x)=x^{p^\mu}-t=(x-a)^{p^\mu}$ 为 a 的零化多项式. 任取一组 E 作为 F-线性空间的基, 考虑 φ_a 的矩阵, 有零化多项式为 $(X-a)^{p^\mu}$, 因而 φ_a-aI 是幂零阵, 故 $0=\mathrm{tr}(\varphi_a-aI)=\mathrm{tr}\varphi_a-\mathrm{tr}aI=Tr_{E/F}(a)-p^\mu a=Tr_{E/F}(a)$. 即 $\forall a\in E,\ Tr_{E/F}(a)=0$. ♢

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 $E_s:=\{a\in E\mid a \text{ 在 } F \text{ 上的极小多项式无重根 (即 } a \text{ 在 } F \text{ 上可分)}\}$. 证明:

1. E_s 为 E 的子域, 称为 F 在 E 中的可分闭包.

♣ 取 $(a,b)\in E_s^2$, 则 $F(a,b)$ 为可分扩张, 因而 $a+b,ab,a^{-1},b^{-1}$ 均在 $E(a,b)$ 中, 从而为可分元素, 故这些元素都在 E_s 中, 也即是说 E_s 为域. ♢

2. E_s/F 为可分扩张, E/E_s 为纯不可分扩张.

♣ 由于 E_s 中任意元素均在 F 上可分, 则 E_s/F 为可分扩张. 设域 F 的特征为 p, 考虑扩张 E/E_s. 取 $a \in E$, 若 a 在 E_s 上的极小多项式 f 无重根, 则 $E(a)/E_s$ 为可分扩张. 由可分扩张的复合还是可分扩张, 知 $E(a)/F$ 为可分扩张, 从而 a 在 F 上可分, 有 $a \in E_s$. 于是 $(f, f') \neq 1$, 又由 f 不可约知 $f|f' \Rightarrow f' = 0$. 故 f 形如 $\sum_{i=1}^{m} a_i x^{pi}$. 令 $g(x) = \sum_{i=1}^{m} a_i x^i$, 于是 a^p 是 g 的根, 由 f 不可约将给出 g 不可约. 若 g 有重根, 重复此操作, 由于次数严格下降且项数保持不变, 操作于有限步内终止, 将得到 $\exists n$ 使得 a^{p^n} 的极小多项式无重根, 也即在 F 上可分, 故 $a^{p^n} \in E_s$, 即 $\bar{E}/E_s$ 纯不可分. ♢

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

♣ 如果 E/F 不是可分扩张, 则 $E_s \nsubseteq E$. 对任意 $a \in E$, 有

$$Tr_{E/F}(a) = Tr_{E/E_s}(Tr_{E_s/F}(a)) = 0$$

因为 Tr_{E/E_s} 为零映射.(习题 8.*3*) ♢

注: 关于纯不可分扩张的内容可以参考 [3] 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. φ 在这组基下对应得方阵记为 M, 则 $M(i, j) = Tr_{E/F}(\alpha^{i+j-2}) =$

$\sum_{k=1}^{n} \sigma_k(\alpha^{i+j-2})$.

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

♣ 记 $A(i,j) = \sigma_j(\alpha^{i-1})$, 则 $M = AA^t$. 注意到 $\det A$ 为 Vandermon 行列式, 故有 $\det M = (\det A)^2 = \prod_{1\le i<j\le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$. ♢

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

♣ 记 $n = [K : \mathbb{Q}]$. 首先可以取出一组基 $d_1, \dots, d_n \in K$, 使得 $d_1, \dots, d_n$ 为 K 的一组 $\mathbb{Q}$-线性基. 考虑 d_i 的极小多项式 $f_i(x) = \sum_{k=0}^{n} a_{ik}x^k$, 其中 $a_{ik} \in \mathbb{Q}$. 通分后有 $\sum_{k=0}^{n} \tilde{a}_{ik}{d_i}^k = 0$, 其中 $\tilde{a}_{ik} \in \mathbb{Z}$. 在该等式两边同乘 $\tilde{a}_{ik}^{n-1}$, 即得 $\sum_{k=0}^{n} \tilde{a}_{in}^{n-1-k}\tilde{a}_{ik}(\tilde{a}_{in}d_i)^k = 0$ 这是关于 $\tilde{a}_{in}d_i$ 的首一整系数零化多项式, 也即是说 $\tilde{a}_{in}d_i \in \mathcal{O}_K$. 将这组基记为 $e_1, \dots, e_n$, 即为一组在 $\mathcal{O}_K$ 中的 K 的一组 $\mathbb{Q}$-线性基. ♢

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

♣ 取 $a \in \mathcal{O}_K$, 则有首一多项式 $f(x) \in \mathbb{Z}[x]$ 零化 a. 考虑 $\forall \sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ 作用在 $f(a) = 0$ 上, 有 $f(\sigma(x)) = 0$. 故 $\sigma \in \mathcal{O}_K$. 由于 K/Q 为可分扩张 (特征零), 由习题 4可知 $Tr_{E/F}(a) = \sum_{i=1}^{n} \sigma_i(x) \in \mathcal{O}_K$. 另一方面, 由 $Tr_{K/\mathbb{Q}}$ 的定义可知 $Tr_{K/\mathbb{Q}}(a) \in \mathbb{Q}$, 故 $Tr_{K/\mathbb{Q}}(a) \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$. 由 a 的任意性, 可知 $Tr_{K/\mathbb{Q}}(\mathcal{O}_K) \subset \mathbb{Z}$. ♢

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

♣ 由1、2立知 M 为整系数方阵. 另一方面, 若令 $A(i,j)=\sigma_i(e_j)$, 则 $M=AA^t$, 只需证明 $\det A\neq 0$. 若有 $\det A=0$, 则存在不全为零的 $\lambda_1,\dots,\lambda_n\in\mathbb{C}$, 使得 $\sum\limits_{i=1}^{n}\lambda_i\sigma_i(e_j)=0,\forall 1\leq j\leq n$. 由于 $e_1,\dots,e_n$ 是 K 的一组基, 可知 $\sum\limits_{i=1}^{n}\lambda_i\sigma_i=0\in\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$, 但是 $\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$ 中的任意 n 个不同的非零映射一定线性无关. 因此 $\det A\neq 0$, 进而 $\det M\neq 0$. ♢

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

♣ 对 $a\in\mathcal{O}_K\subset K$, 存在 $c_1,\dots,c_n\in\mathbb{Q}$, 使得 $a=\sum\limits_{i=1}^{n}c_ie_i$. 用 σ_j 作用在这个式子上, 可得 $\sigma_j(a)=\sum\limits_{i=1}^{n}c_i\sigma_j(e_i)$, 其中 $1\leq j\leq n$. 将这 n 个等式看作关于 $c_1,\dots,c_n$ 的线性方程组, 由 Cramer 法则可解出 $c_i=\dfrac{\det A}{A_i}$, 其中 A 即为习题 10中定义的矩阵, A_i 为将 A 的第 i 列换作 $(\sigma_1(a),\dots,\sigma_n(a))^t$ 得到的矩阵. 也即有 $\det A_i=c_i\det A$, 因此 $\det Mc_i=(\det A)^2c_i=\det A_i\det A$. 由于 $\sigma_j(e_i),\sigma_j(a)\in\mathcal{O}_K,\forall 1\leq i,j\leq n$, 可知 $\det A_i\in\mathcal{O}_K,\det A\in\mathcal{O}_K$, 故 $\det A\det A_i\in\mathcal{O}_K$, 于是 $\det Mc_i=\det A\det A_i\in\mathcal{O}_K$. 再由 $\det M\in\mathcal{O}_K\cap\mathbb{Q}=\mathbb{Z}$, 且 $c_i\in\mathbb{Q}$, 知 $\det Mc_i\in\mathbb{Q}$, 故 $\det Mc_i\in\mathbb{Q}\cap\mathcal{O}_K=\mathbb{Z}$. 这就表明 $\det M\cdot\mathcal{O}_K\subset\mathbb{Z}e_1+\cdots+\mathbb{Z}e_n$.(事实上为直和) ♢

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

♣ 由 *4* 立得 $O_K\subset\mathbb{Z}\dfrac{e_1}{\det M}\oplus\cdots\oplus\mathbb{Z}\dfrac{e_n}{\det M}$. 但是右边是秩为 n 的自由 Abel 群, 从而其子群 O_K 为秩不超过 n(事实上就是 n, 因为 $e_1,\dots,e_n$ 这 n 个元素 $\mathbb{Z}$-线性无关)的自由 Abel 群, 当然为有限生成 $\mathbb{Z}$-模, 因此可以写成某个 $\mathbb{Z}[X_1,\dots,X_n]$ 的商模, 当然为 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 φ 同上.

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

♣ 由单扩张定理, 可设 $E = F(\alpha)$, 令 $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n$ 为 α 在 F 上的所有共轭根, 则 α 有极小多项式 $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$, 且 $E \simeq F[x]/(f)$. 于是 $E \otimes_F \bar{F} \simeq (F[x]/(f)) \otimes_F \bar{F} \simeq \bar{F}[x]/(f) \simeq \prod_{i=1}^{n} \bar{F}[x]/(x-\alpha_i) \simeq \bar{F}^n$ 为代数同构. ♢

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

♣ 视 $E \otimes_F \bar{F}$ 为 $\bar{F}$-线性空间, 定义 $\mathrm{tr}_{\bar{F}}(x \otimes a)$ 为左乘 $x \otimes a$ 得到的 $\bar{F}$-线性映射的迹. 由 *1* 中的 F-代数同构, 给出 $\bar{F}^n$ 上的双线性型 $\tilde{\varphi}(u,v) = \mathrm{tr}_{\bar{F}}(uv)$. 取 $\bar{F}^n$ 的典范基 $e_1 = (1,0,\cdots,0), \cdots, e_n = (0,\cdots,0,1)$, 则由 $e_i^2 = e_i,\ e_i e_j = 0\ \forall i \neq j$ 以及 $\tilde{\varphi}$ 的定义知 $\tilde{\varphi}(e_i, e_j) = \delta_{ij}\mathrm{tr}_{\bar{F}}(e_i) = \delta_{ij}$. 故 $\tilde{\varphi}$ 在这组基下的矩阵即为单位阵, 从而非退化. ♢

3. φ 为 E 上的非退化对称 F-双线性型.

♣ 取 E 的一组 F-基 $(x_1, \cdots, x_n)$, 于是 $(x_1 \otimes 1, \cdots, x_n \otimes 1)$ 给出 $E \otimes_F \bar{F}$ 的一组 $\bar{F}$-基. 另一方面, 按定义容易验证 $\mathrm{tr}_{\bar{F}}(x_i x_j \otimes 1) = \mathrm{tr}(x_i x_j)$, 故在这组基下 φ 和 $\tilde{\varphi}$ 有相同的矩阵, 系数均在 F 中. 由*2*知该矩阵在 $\bar{F}$ 上是非退化的, 进而有非零的行列式, 而行列式自然取值于 F, 于是矩阵在 F 上也非退化, 故 φ 非退化. ♢

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. φ 为非退化双线性型.

♣(部分证明来自 [5]) 我们依次证明 *1*⇔*2*⇒*3*⇒*4*⇒*2*.

1⇔2: 由于自然映射 $A\otimes_F K\hookrightarrow A\otimes_F \bar{F}$ 是单射, 进而 $A\otimes_F K$ 中的幂零元都在 $A\otimes_F \bar{F}$ 中. 反之, 任一 $A\otimes_F \bar{F}$ 中的元素仅涉及有限个 $\bar{F}$ 中的元素, 于是存在一个 K 使得该元素落在 $A\otimes_F K$ 中, 进而 $A\otimes_F \bar{F}$ 中的幂零元也都落在某个 $A\otimes_F K$ 中, 从而易见 *1⇔2*.

2⇒3: 若 R 为 k-代数, 且存在 k-代数 B_1, B_2 使得 $R\simeq B_1\times B_2$, 则称 R 是可分解的 k-代数, 反之则称为不可分解的. 由于 $A\otimes_F \bar{F}$ 是有限维 $\bar{F}$-代数, 故由维数下降 (即分解后的代数维数严格小于原来的代数) 可确保存在 $M_1,\cdots,M_m$ 为不可分解的 $\bar{F}$-代数使得 $A\otimes_F \bar{F}\simeq M_1\times\cdots\times M_m$. 由于乘积没有非零幂零元, 可以给出各 M_i 均没有非零幂零元 (否则若有幂零元 a, 则 $(0,\cdots,a,\cdots,0)$ 给出乘积的非零幂零元). 另一方面, 若 k-代数 R 中含有除 0 和 1 以外的幂等元 (即 e 满足 $e^2=e$), 考虑 R 的两个理想 eR 和 $(1-e)R$. 此时 $(1-e)^2=1-e$ 也为幂等元, 且 eR 成为环 (以 e 为环幺元, 保持原本的加法和乘法, 但不是 R 的子环). 而若 $a\in eR\cap(1-e)R$, 则 $a=ex_1=(1-e)x_2$. 两边同乘 e 得到 $e^2x_1=e(1-e)x_2$, 但 $e(1-e)=0$ 给出 $a=ex_1=e^2x_1=e(1-e)x_2=0$, 于是 $eR\cap(1-e)R=0$, 这给出环同构 $R\to eR\times(1-e)R$, $r\mapsto(er,(1-e)r)$, 进而 R 是可分解的 k-代数. 这说明 M_i 中没有 0 和 1 以外的幂等元. 考虑 M_i 中任一非零元 x, 则有理想降链 $(x)\supseteq(x^2)\supseteq\cdots$. 同样由维数下降可知存在 $l\in\mathbb{N}^*$ 使得从 l 起降链全取等号. 于是有 $(x^l)=(x^{l+1})$, 这说明存在 $y\in M_i$ 使得 $x^l=x^{l+1}y=x^l(xy)$. 反复迭代得到 $x^l=x^l(xy)=x^l(xy)^2=\cdots=x^l(xy)^l$. 两边再同乘 y^l 即得 $x^ly^l=(x^ly^l)^2$, 给出一个幂等元 x^ly^l. 故其等于 0 或 1. 但由于 M_i 无非零幂零元, 有 $x^ly^l=0\Rightarrow xy=0\Rightarrow x^n=x^n(xy)=0\Rightarrow x=0$, 与 x 非零矛盾, 从而 $x^ly^l=1$, 这说明 x 有逆 $x^{l-1}y^l$. 由 x 的任意性知 M_i 的所有非零元可逆, 故为域. 而 M_i 本身为 $\bar{F}$-代数, 维数有限, 故是 $\bar{F}$ 的有限扩张, 再根据代数闭即得 $M_i=\bar{F}\ \forall i$. 于是知 $A\otimes_F\bar{F}\simeq\bar{F}^m$, 比较维数得到 $m=n$.

3⇒4: 习题 12 的*2*和*3*并未用到 E 为域的条件, 将 E 替换为 A 即得到此处的证明.

4⇒2: A 上的迹形式 (即题干中定义的双线性型) 仿照习题 12 扩张到 $A\otimes_F \bar{F}$ 上恰为上面的 $\bar{F}$-线性空间的迹形式, 且有相同的矩阵表达, 进而得到 $A\otimes_F \bar{F}$ 上的迹形式非退化. 假设 $x\in A\otimes_F \bar{F}$ 为一个非零幂零元, 将 $\{x\}$ 扩张为一组基 $(e_1 = x, e_2\cdots, e_n)$. 则在这组基下迹形式的矩阵为 $(\mathrm{tr}(e_ie_j))$. 由于 e_1 幂零, 进而 e_1e_j 均幂零. 而幂零元对应作用的矩阵为幂零阵, 所有特征值均为 0, 故迹也是 0, 这给出 $\mathrm{tr}(e_1e_j) = 0$, 即迹形式矩阵第一行为 0, 与非退化矛盾. 故 $A\otimes_F \bar{F}$ 没有非零幂零元. ♢

注: 如果上述等价命题成立, 则称 F-代数 A 为可分的或平展的 (étale). 这是域的可分扩张的推广. 事实上, 将 $4\Rightarrow 2$ 的证明方法应用到 A 上可得 A 没有非零幂零元, 再将 $2\Rightarrow 3$ 的证明方法应用在 A 上, 对于非代数闭的情形, 给出 A 是有限个域的乘积, 每个乘积分量是 F 的一个有限扩张. 事实上这些有限扩张均为可分扩张:

$A\otimes_F \bar{F}\simeq \bar{F}^n$, 且 A 有乘积分量 L, 易知 $L\otimes_F \bar{F}\simeq \bar{F}^{[L:F]}$. 另一方面, 给定 $f\in \mathrm{Hom}_F(L,\bar{F})$, 则给出 $\bar{F}-$ 代数同态 $L\otimes_F \bar{F}\to \bar{F}\otimes_f \bar{F}\to \bar{F}$, 即有 $\mathrm{Hom}_F(L,\bar{F})\to \mathrm{Hom}_{\bar{F}}(L\otimes_F \bar{F},\bar{F})$; 反之, 复合上 $L\to L\otimes_F \bar{F}$ 将给出反向映射. 可验证这两个映射互逆, 从而 $\mathrm{Hom}_F(A,\bar{F})\simeq \mathrm{Hom}_{\bar{F}}(A\otimes_F \bar{F},\bar{F})\simeq \mathrm{Hom}_{\bar{F}}(\bar{F}^{[L:F]}\bar{F})\Rightarrow |\mathrm{Hom}_F(L,\bar{F})| = |\mathrm{Hom}_{\bar{F}}(\bar{F}^{[L:F]},\bar{F})| = [L:F]\Rightarrow L/F$ 可分.

于是上述命题还有一个等价刻画, 即 A 是有限个 F 的有限可分扩张的乘积.

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 α_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 $\mathrm{Gal}(K/\mathbb{Q})$.

♣ 根据定义, $K = \mathbb{Q}(\sqrt[8]{5}\zeta^i,\ 0 \le i \le 7)$, 其中 ζ 为 8 次本原单位根. 显然 $K = \mathbb{Q}(\sqrt[8]{5}, \zeta)$. 这样 K 的容易计算的共轭根的生成元从 8 个缩减到两个. 对于 $\sigma \in G = \mathrm{Gal}(K/\mathbb{Q})$,

$$\sigma(\sqrt[8]{5}) \in \{\sqrt[8]{5}\zeta^i,\ 0 \le i \le 7\},$$

$$\sigma(\zeta) \in \{\zeta^i,\ 0 \le i \le 7, (i,8) = 1\}.$$

这样得到 $|G| \le 32$. 另一方面, 通过验证 $x^8 - 5$ 在 $\mathbb{Q}(\zeta)$ 上不可约, 可以得到 $[K : \mathbb{Q}(\zeta)] = 8$, 从而 $[K:\mathbb{Q}] = 32$. 这样知道 G 恰由如下的 32 个变换组成:

$$\sigma(\sqrt[8]{5}) = \sqrt[8]{5}\zeta^i,\ 0 \le i \le 7,$$

$$\sigma(\zeta) = \zeta^j,\ 0 \le j \le 7, (j,8) = 1.$$

再往下容易写出 G 的形式 (为一个半直积). ♢

注: 以上解答的思路由许金兴老师提供, 但其中 $x^8 - 5$ 在 $\mathbb{Q}[\zeta]$ 上不可约并不容易直接验证, 主要源于 5 在 $\mathbb{Z}[\zeta]$ 上并不是素元以及 $\mathbb{Z}[\zeta]$ 是 UFD 这一事实并不平

凡. 为使用 Eisenstein 判别法, 我们需要找一个素元整除 5, 但它的平方不整除 5. 考虑 $\mathbb{Z}[\zeta] \simeq \mathbb{Z}[X]/(X^4+1)$ 位于 5 上方的素理想, 即考虑 $\mathbb{Z}[X](X^4+1,5) \simeq \mathbb{F}_5[X]/(X^4+1) \simeq \mathbb{F}_5[X](X^2+2) \times \mathbb{F}_5[X]/(X^2-2)$. 而 x^2+2 和 x^2-2 在 $\mathbb{F}_5$ 上无根, 故不可约, 这给出 $\mathbb{Z}[\zeta]$ 包含 5 的素理想只有 $(5,\zeta^2+2)$ 和 $(5,\zeta^2-2)$. 注意到 $\zeta^2=i$, 而 $5=(2+i)(2-i)$, 于是这两个理想都是主理想, 生成元为 $2+i$ 和 $2-i$. 关于 $\mathbb{Z}[\zeta]$ 是 UFD, 我们对 $x=a+b\zeta+c\zeta^2+d\zeta^3 \in \mathbb{Z}[\zeta]$, 令 $N(x)=(a^2+c^2)^2+(b^2+d^2)^2+4(ab+cd)(ad-bc)$, 可验证其成为欧几里得函数, 进而 $\mathbb{Z}[\zeta]$ 是 ED, 从而是 UFD. 由唯一分解性, 5 没有平方因子, 从而可对 $i+2$ 用 Eisenstein 判别法知 x^8-5 在 $\mathbb{Z}[\zeta]$ 上不可约, 进而在 $\mathbb{Q}[\zeta]$ 上不可约.

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.

♣ 有 x^4-2 的所有根为 $\pm\sqrt[4]{2}$ 和 $\pm i\sqrt[4]{2}$, 于是 $K=\mathbb{Q}[\sqrt[4]{2},i]$. 而易见 $[K:\mathbb{Q}]=8$, 且作用完全被 $\sqrt[4]{2}$ 和 i 的像确定, 进而 $\mathrm{Gal}(K/\mathbb{Q})$ 在 K 上的作用可将 $\sqrt[4]{2}$ 映至 $i^k\sqrt[4]{2}$, 将 i 映至 $(-1)^j i$, 将如此定义的作用记作 $\sigma_{k,j}$, $0 \leq k \leq 3$, $0 \leq j \leq 1$. 于是有 $\sigma_{0,1}^2 = \mathrm{id}$, $\sigma_{1,0}^4 = \mathrm{id}$, $\sigma_{0,1}\sigma_{1,0}\sigma_{0,1} = \sigma_{1,0}$. 由以上关系可给出 $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_4$. ♢

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

♣ 令 $\mu=\dfrac{1+\sqrt{5}}{2}$, 且 $a=\sqrt{\mu}$, 则 x^4-x^2-1 有四个根 $a,-a,ia^{-1},-ia^{-1}$, 故 $K=\mathbb{Q}[a,i]$. 同上一题, 这是一个 8 次扩张, 进而 $\mathrm{Gal}(K/\mathbb{Q})$ 恰有 8 个元素, 分别将 a 与 i 任意映到共轭根. 考虑 $\sigma_1\colon a\mapsto a, i\mapsto -i$, $\sigma_2\colon a\mapsto ia^{-1}, i\mapsto -i$, 则 $\sigma_1^2=\sigma_2^4=\mathrm{id}$, 易见 σ_1 与 σ_2 交换且生成的循环群交平凡, 这给出 $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. ♢

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

♣ 考虑 $\sqrt{2+\sqrt{2}}$ 在 $\mathbb{Q}$ 上的极小多项式 x^4-4x^2+2(不可约性可由 Eisenstein 判别法证明), 其四个根为 $\sqrt{2+\sqrt{2}}, -\sqrt{2+\sqrt{2}}, \sqrt{2-\sqrt{2}}, -\sqrt{2-\sqrt{2}}$. 如果记 $a=\sqrt{2+\sqrt{2}}$, 则 $-\sqrt{2+\sqrt{2}}=-a, \sqrt{2-\sqrt{2}}=\dfrac{a^2-2}{a}, -\sqrt{2-\sqrt{2}}=-\dfrac{a^2-2}{a}$, 四个根均在 $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ 中. 为确定 G 中一个元素 σ, 只需确认 $\sigma(a)$. 注意到, 取 $\sigma\in G$, 使得 $\sigma(a)=\dfrac{a^2-2}{a}=\sqrt{2-\sqrt{2}}$, 那么 σ 在 G 中的阶数是 4(考虑 σ 在 a 上的作用,$\sigma^2(a)=-a$). 而 $|G|\leq 4$, 这说明 $|G|=4$, 且 G 中有 4 阶元, 故 $G=\mathbb{Z}/4\mathbb{Z}$. ♢

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.

♣ 由于 $\mathbb{F}_p[T]$ 为 UFD, 且 T 是素元, 对 T 用 Eisenstein 判别法即知 f 和 g 在 $\mathbb{F}_p[T][X]$ 上不可约, 从而在 $K[X]$ 上不可约. 易见 f 和 g 导数均非零, 从而无重根. ♢

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

♣ 若 $\alpha\in M$ 为 g 的一个根, 即 $\alpha^{p-1}=T$, 则 $\forall a\in F_p^*$, $a\alpha$ 也满足 $(a\alpha)^{p-1}=T$, 故这给出 g 的所有根, 且 $M=K[\alpha]$. 这给出 $[M:K]=p-1$, 由 *1* 知 g 无重根, 进而 M/K 可分且正规, 故 $|\mathrm{Gal}(M/K)|=p-1$. 令一方面, 每个 $\sigma\in\mathrm{Gal}(M/K)$ 由 $\sigma(\alpha)$ 决定. 记 $\alpha\mapsto a\alpha$ 为 σ_a, 则有 $\sigma_a\circ\sigma_b=\sigma_{ab}$, 于是给出 $\mathrm{Gal}(M/K)\simeq\mathbb{F}_p^*$. ♢

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.

♣ 若 $\beta_1,\beta_2\in L$ 为 f 的两个不同根, 即满足 $\beta^p=\beta T+T$, 则 $(\beta_1-\beta_2)^p=\beta_1^p-\beta_2^p=$

$(\beta_1 T+T)-(\beta_2 T+T)=(\beta_1-\beta_2)T$ 消去 $\beta_1-\beta_2$ 得到 $g(\beta_1-\beta_2)=0$. 又由2知乘 $\mathbb{F}_p^*$ 中的元素得到 g 的所有根, 故 g 在 L 中分裂. 另一方面, 固定 β 为 f 的根, 令 $\alpha_1=\alpha,\cdots,\alpha_{p-1}$ 为 g 的根, 则 $\beta+\alpha_1,\cdots,\beta+\alpha_{p-1}$ 也都是 f 的根, 于是给出 β 的所有共轭根, 且 $L=K[\beta,\alpha]$. 由于 $[M:K]<\deg f$, 故 $\beta\notin M$, 若 f 在 M 上可约, 不妨假设有首一因子 $h(x)$, 且在 L 中分解为 $(x-\beta_1)\cdots(x-\beta_m)$, $0<m<p$. 考虑 $m-1$ 次项系数为 $a_{m-1}=-(\beta_1+\cdots+\beta_m)$. 令 $\varphi\colon L\to L$, $a\mapsto a^p-aT$, 则易见 φ 为 $\mathbb{F}_p$-线性映射且 $\varphi(\beta_i)=T$. 令 n 是 $-m$ 模 p 的乘法逆, 则 $\varphi(na_{m-1})=-nmT=T$, 这说明 $na_{m-1}\in M$ 是 f 在 M 上的根, 与 f 无根矛盾. 故 f 在 M 上不可约, 从而可算出扩张次数 $[L:K]=p(p-1)$, 得到 $\mathrm{Gal}(L/K)$ 的阶, 且 Galois 群的作用由在 β 和 α 上的作用决定. 对 $0\le i\le p-1$, $1\le j\le p-1$ 记 $\sigma_{i,j}$ 为 $\beta\mapsto\beta+i\alpha$, $\alpha\mapsto j\alpha$ 决定的自同构, 则计算 α 和 β 的像可得到 $\sigma_{i_1,j_1}\circ\sigma_{i_2,j_2}=\sigma_{i_1+i_2j_1,j_ij_2}$(下标为模 p 意义下). 给出 $\mathbb{F}_p^*$ 在 $\mathbb{F}_p$ 上自然数乘的作用 η, 这正好是半直积 $\mathbb{F}_p\rtimes_\eta\mathbb{F}_p^*$ 上的乘法, 对应到下标即给出同构 $\mathrm{Gal}(L/K)\simeq\mathbb{F}_p\rtimes\mathbb{F}_p^*$. ♢

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.

♣ 若 f 在 F 上不可约, 考虑 α_1 的轨道, 不妨假设即为 $\{\alpha_1,\cdots,\alpha_m\}$, 则 $g(x)=(x-\alpha_1)\cdots(x-\alpha_m)$ 在 G 作用下不动. 由于 f 无重根, 故分裂域为 F 的 Galois 扩张, 在 G 作用不动知 $g(x)\in F[x]$, 而另一方面在 $K[x]$ 中有 $g|f$, 做带余除法可得 $F[x]$ 上

也有该整除关系, 从而由 f 的不可约性知 $m=n$, 即 G 作用传递. 反之, 若 G 作用在根上传递, 令 $h(x)$ 为 α_1 在 F 上的极小多项式, 则 $(x-\alpha_1)|h$, 且 h 在 G 作用下不动. 由于作用传递, 存在 $\sigma_i\in G$ 使得 $\sigma_i(\alpha_1)=\alpha_i$, 于是有 $(x-\alpha_i)|h\Rightarrow f|h$. 由于 f 零化 h, 故 $h|f$, 再由首一即推出 $f=h$, 从而不可约. 由于轨道长整除群的阶, 故 f 不可约时有 $n||G|$. ♢

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.

♣ G 在根上的置换作用给出群同态 $\rho\colon G\to\mathfrak{S}_p$, 而 Galois 群的作用由在生成元上的作用唯一确定, 故 G 的作用是忠实的, 从而 ρ 给出 G 到 $\mathfrak{S}_p$ 的嵌入, 将 G 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)

♣ 令 $\tau\colon\mathbb{C}\to\mathbb{C}$, $z\mapsto\bar{z}$ 为复共轭, 由于 $K/\mathbb{Q}$ 为 Galois 扩张, 将 τ 限制在 K 上可得到 $K/\mathbb{Q}$ 的自同构, 即 G 中的元素. 由于 $\mathbb{R}=\mathbb{C}^{\langle\tau\rangle}$ 下不动, 故该自同构固定 $p-2$ 个实根, 置换剩下的两个虚根, 于是为对换. ♢

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

♣ 由习题 5知 $p=\deg f||G|$, 故 G 存在 Sylow-p 子群, 从而有 p 阶元. 将 G 中元素 g 拆成不交循环的乘积, 可知元素的阶即为各循环长度的最小公倍数. 又由于循环长度之和为 p, 故 g 的阶为 p 当且仅当 g 为 p-循环. ♢

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

♣ 记2中的对换为 σ, 3中的 p-循环为 η, 我们证明 G 包含所有对换. 不妨假定

$\sigma = (i\ j)$, $\eta = (1\ 2\ \cdots\ p)$, 于是 $\eta \circ \tau \circ \eta^{-1} = (\eta(i)\ \eta(j)) = (i+1\ j+1)$(指标均在模 p 意义下). 于是迭代 $j-i$ 次得到 $(j\ i+2(j-i))$, 此时可由 $(i\ j)$ 和 $(j\ 2j-i)$ 生成 $(i\ i+2(j-i)$. 最终可得到所有的 $(i\ i+k(j-i))$, $0 \leq k \leq p-1$, 由于 $j-i$ 与 p 互素, 这将给出所有的 $(i\ k)$, 再利用 $(1\ k)$ 和 $(1\ l)$ 可以得到 $(k\ l)$, 即给出所有对换. 故 $G = \mathfrak{S}_p$. ♢

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

♣ f 为 3-Eisenstein 多项式, 故在 $\mathbb{Q}$ 上不可约. $f'(x) = 5x^4 - 6$ 在 $\mathbb{R}$ 上有零点 $\pm\sqrt[4]{\frac{6}{5}}$. 而 $f(-\sqrt[4]{6/5}) > 0$, $f(\sqrt[4]{6/5}) < 0$, 根据介值性与 f 的单调性易知 f 有 3 个实根, 两个虚根. 直接由习题 6的结论即知 $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathfrak{S}_5$. ♢

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 $2|[K:\mathbb{Q}]$.

♣ $\Delta(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{-1}\mathrm{Res}(f, f') = -81$. 由于 $\Delta(f) = a_n^{2n-2} \prod\limits_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2$, 有平方根 $a_n^{n-1} \prod\limits_{1\leq i<j\leq n} (\alpha_i - \alpha_j) \in K$, 故 $\mathbb{Q}[\sqrt{\Delta(f)}] \subseteq K$. 而 $[\mathbb{Q}[\sqrt{\Delta(f)}] : \mathbb{Q}] = 2$, 故有 $2|[K:\mathbb{Q}]$. ♢

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

♣ $3 = \deg f | [K:\mathbb{Q}]$, 再由 *1* 知 $6|[K:\mathbb{Q}]$. 令一方面, $K/\mathbb{Q}$ 为 Galois 扩张, 由习题 7知 $G = \mathrm{Gal}(K/\mathbb{Q})$ 为 $\mathfrak{S}_3$ 的子群, 故 $[K:\mathbb{Q}] = |G||6$, 故只能有 $G \simeq \mathfrak{S}_3$. ♢

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 $\sigma\colon L\to\bar{K}$.

♣ 由于 i 为单射, 易知 $\sigma\mapsto i\circ\sigma$ 单. 又由有限正规扩张定义知 $|\mathrm{Gal}(L/K)|=|\mathrm{Hom}_K(L,\bar{K})|<\infty$, 故以上映射给出双射. ♢

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).

♣ 由乘法 $\bar{K}\times L\to\bar{K}$ 的双线性性知 $x\otimes y\mapsto xy$ 为 K-线性映射, 再由 $\mathrm{id}_{\bar{K}}\otimes\sigma\colon x\otimes y\mapsto x\otimes\sigma(y)$ 是 K-线性的即得 $\varphi_\sigma=\varphi_i\circ(\mathrm{id}\otimes\sigma)$ 为 K-线性映射. 事实上, φ_i 和 $\mathrm{id}_{\bar{K}}\otimes\sigma$ 都为 $\bar{K}$-代数同态即知 φ_a 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).

♣ 由讲义 2022-05-18定理 1(单扩张定理) 知存在 $\alpha\in L$ 使得 $L=K(\alpha)$, 于是 $\bar{K}\otimes_K L$ 有一组 $\bar{K}$-基 $(1\otimes\alpha^k)_{0\le k\le n-1}$(记 $n=[L:K]$). 若 $x=\sum\limits_{i=0}^{n-1}x_i\otimes\alpha^i\in\ker\left(\prod\limits_{\sigma\in\mathrm{Gal}(L/K)}\varphi_\sigma\right)$, 即对任意 σ 有 $0=\varphi_\sigma(x)=\sum\limits_{i=0}^{n-1}x_i\sigma(\alpha)^i$, 于是有 $\sigma(\alpha)$ 为多项式 $\sum\limits_{i=0}^{n-1}x_iT^i\in\bar{K}[T]$ 的根. 但该多项式次数不超过 $n-1$, 有 n 个根, 故只能有 $x=0$, 即 $\prod\limits_{\sigma\in\mathrm{Gal}(L/K)}\varphi_\sigma$ 是单射. 由于这是有限维 $\bar{K}$-线性空间之间的线性单射, 故为线性同构 (进而也是 $\bar{K}$-代数同构). ♢

4. $\forall\sigma\in\mathrm{Gal}(L/K)$, 记 e_σ 为 $\prod\limits_{\sigma\in\mathrm{Gal}(L/K)}\bar{K}$ 中 σ 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.

♣ 这正是 $\bar{K}^n$ 的一组典范基. ♢

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:

$$\begin{array}{ccc} \bar{K}\otimes_K L & \xrightarrow{\prod\limits_{\sigma\in\mathrm{Gal}(L/K)}\varphi_\sigma} & \prod\limits_{\sigma\in\mathrm{Gal}(L/K)} \bar{K} \\ \downarrow{\scriptstyle 1\otimes\tau} & & \downarrow{\scriptstyle \tilde{\tau}} \\ \bar{K}\otimes_K L & \xrightarrow{\prod\limits_{\sigma\in\mathrm{Gal}(L/K)}\varphi_\sigma} & \prod\limits_{\sigma\in\mathrm{Gal}(L/K)} \bar{K} \end{array}$$

♣ 记*3*中的乘积映射为 φ, $G = \mathrm{Gal}(L/K)$, 则对 $x = \sum\limits_{i=0}^{n-1} x_i\otimes\alpha^i$, 有 $\varphi(x) = \sum\limits_{\sigma\in G}\varphi_\sigma(x)e_\sigma$, 故 $\varphi\circ(1\otimes\tau)(x) = \varphi\left(\sum\limits_{i=0}^{n-1} x_i\otimes\tau(\alpha)^i\right) = \sum\limits_{\sigma\in G}\left(\sum\limits_{i=0}^{n-1} x_i(\sigma\cdot\tau)(\alpha)^i\right)e_\sigma$. 而 $\tilde{\tau}\circ\varphi(x) = \tilde{\tau}\left(\sum\limits_{\sigma\in G}\sum\limits_{i=0}^{n-1} x_i\sigma(\alpha)^i e_\sigma\right) = \sum\limits_{\sigma\in G}\sum\limits_{i=0}^{n-1} x_i\sigma(\alpha)^i e_{\sigma\cdot\tau^{-1}} = \sum\limits_{\sigma\in G}\left(\sum\limits_{i=0}^{n-1} x_i(\sigma\cdot\tau)(\alpha)^i\right)e_\sigma$. 故以上图表交换. ♢

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 τ 的 $\bar{K}$-线性变换.

♣ 依定义 e_σ 和 σ^{-1} 分别为两边的基, 故以上映射给出线性同构. 另一方面有 $\tilde{\tau}(e_\sigma) = e_{\sigma\cdot\tau^{-1}} \mapsto \tau\cdot\sigma^{-1}$ 为左乘作用. ♢

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:

$$\begin{array}{ccc} \bar{K}\otimes_K L & \xrightarrow{\sim} & \bar{K}[G] \\ \downarrow{\scriptstyle 1\otimes\tau} & & \downarrow{\scriptstyle \tau\cdot} \\ \bar{K}\otimes_K L & \xrightarrow{\sim} & \bar{K}[G] \end{array}$$

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 $\sum\limits_{\tau\in G}\tau$.

♣ 综合5和6的结论即得图表, 且 $1 \in \bar{K}\otimes_K L$ 对应 $(1,\cdots,1) = \sum\limits_{\sigma\in G} e_\sigma$, 进而对应到 $\sum\limits_{\sigma\in G}\sigma^{-1} = \sum\limits_{\tau\in G}\tau$. ♢

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 $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$.

♣ 若 $\lambda_1,\ldots,\lambda_n \in L$, 使得 $\lambda_1\sigma_1(x)+\ldots+\lambda_n\sigma_n(x) = 0$, $\forall x \in L$, 则作为 $\bar{K}\otimes_K L$ 中的 $\bar{K}$-线性变换, 有

$$\lambda_1(1\otimes\sigma_1)+\ldots+\lambda_n(1\otimes\sigma_n) = 0$$

再由习题 1.7, 此即 $\lambda_1\sigma_1+\ldots+\lambda_n\sigma_n$ 看作 $\bar{K}[G]$ 上的左乘变换为 0, 而显然通过观察该变换在 G 的单位元取值得到 $\lambda_1\sigma_1+\ldots+\lambda_n\sigma_n$ 看作 $\bar{K}[G]$ 中元为 0, 从而 $\lambda_1=\ldots,=\lambda_n=0$. ♢

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 ζ_n 为本原 n 次单位根, 则存在 $a\in K$, 使得 $L=K(\sqrt[n]{a})$.

♣ 记 σ 为 G 的一个生成元, 则

$$G=\{1,\sigma,\sigma^2,\ldots,\sigma^{n-1}\}$$

易见只需证明存在 $\beta\in L,\ \beta\neq 0$, 使得 $\sigma(\beta)=\zeta_n\cdot\beta$ 即可, 即只需证明 ζ_n 为 L 上的 K-线性变换 σ 的一个特征值. 而由习题 1 的7, 只需证明 $\bar{K}[G]$ 上左乘 σ 的 $\bar{K}$-线性变换有特征值 ζ_n, 而直接考虑 $\sum\limits_{k=0}^{n-1}\zeta_n^{-k}\sigma^k$, 则左乘 σ 后得到 $\sum\limits_{k=0}^{n-1}\zeta_n^{-k+1}\sigma^k=\zeta_n\sum\limits_{k=0}^{n-1}\zeta_n^{-k}\sigma^k$, 故给出 ζ_n-特征向量. ♢

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 α 为 K 上多项式 $f(x)=x^p-x-a$ 的根.

♣ 记 $G=\mathrm{Gal}(L/K)\simeq\mathbb{Z}/p\mathbb{Z}$. 记 σ 为 G 的一个生成元, 那么只需要证明存在 $\alpha\in L$, 使得 $\sigma(\alpha)=\alpha+1$, 从而只需要证明存在 $\alpha'\in\bar{K}\otimes_K L$ 使得 $1\otimes\sigma(\alpha')=\alpha'+1$. 再

由习题 1.7, 即证明在 $\bar{K}[G]$ 中, 存在 $\alpha'' \in \bar{K}[G]$, 使得 $\sigma\cdot\alpha'' = \alpha'' + \sum_{\tau\in G}\tau = \alpha'' + \sum\limits_{k=0}^{p-1}\sigma^k$. 则考虑 $\alpha'' = -\sum\limits_{k=0}^{p-1} k\sigma^k$, 左乘 σ 后得到 $-\sum\limits_{k=0}^{p-1}(k-1)\sigma^k = \alpha'' + \sum\limits_{k=0}^{p-1}\sigma^k$, 即证. ♢

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.

♣ 我们分 K 为无限域和有限域两种情况讨论.

1. 当 K 为无限域时, 我们需要证明 $\exists\alpha \in L$, 使得 $\{\sigma(\alpha) \mid \alpha \in \mathrm{Gal}(L/K)\}$ 为 K-线性无关集. 取 $e_1, \ldots, e_n$ 为 L 的一组 K-基, 并设 $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$, 则 $\forall\alpha = x_1e_1 + \ldots + x_ne_n$, 存在唯一的 $A \in M_n(K)$, 使得

$$(\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)) = (e_1, \ldots, e_n)\cdot A$$

令 $f = \det A$, 则 f 为 $x_1, \ldots, x_n$ 的一个 K-系数多项式, 只需证明 $f \neq 0$ 即可. 由于 $\sigma_1\cdot 1, \ldots, \sigma_n\cdot 1$ 在 $\bar{K}[G]$ 中是 $\bar{K}$-线性无关的, 根据习题 1.7, 在 $\bar{K}$-线性空间 $\bar{K}\otimes_K L$ 中, $\exists\beta \in \bar{K}\otimes_K L$(这里 β 就是 $\bar{K}[G]$ 中单位元在 1.7中同构下的原像), 使得 $(1\otimes\sigma_1)\beta, \ldots, (1\otimes\sigma_n)\beta$ 为 $\bar{K}\otimes_K L$ 的一组 $\bar{K}$-基. 记 $A = (a_{ij})_{1\le i,j\le n}$, 则有 $\sum\limits_{i=1}^{n} a_{ij}e_i = \sigma_j(\alpha)$. 将两边系数扩张到 $\bar{K}$ 中得到 $\sum\limits_{i=1}^{n} a_{ij}(1\otimes e_i) = (1\otimes\sigma_j)(1\otimes\alpha)$. 另一方面, 对 $\beta = \bar{x}_1(1\otimes e_1) + \cdots + \bar{x}_n(1\otimes e_n) \in \bar{K}\otimes_K L$, 存在唯一的 $\tilde{A} \in M_n(\bar{K})$ 使得

$$((1\otimes\sigma_1)(\beta), (1\otimes\sigma_2)(\beta), \ldots, (1\otimes\sigma_n)(\beta)) = (1\otimes e_1, \ldots, 1\otimes e_n)\cdot\tilde{A}$$

由唯一性, 上面的系数扩张给出当 $\beta \in 1\otimes L$ 时 (进而看作 L 中的元素) 有 $\tilde{A} = A$, 给

出 $\det A = \det \tilde{A}$, 故二者作为 x_i 的多项式相同. 从而取上面找到的 β 可以说明: 存在 $\bar{x}_1, \ldots, \bar{x}_n \in \bar{K}$, 使得 $f(\bar{x}_1, \cdots, \bar{x}_n) \neq 0$. 于是 f 为非零多项式, 从而由 K 为无限域可知: 存在 $x_1, \ldots, x_n \in K$, 使得 $f(x_1, \cdots, x_n) \neq 0$.

2. 当 K 为有限域时, $G = \mathrm{Gal}(L/K)$ 为循环群, 只需证明 L 作为 K-线性空间为循环 σ-空间. 注意到 σ 为 G 的生成元, 而 $\bar{K}[G]$ 显然为循环 σ-空间. 再由习题 1.7以及一个线性空间是否循环不依赖系数扩张即可证明. ♢

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 α 的 K-线性变换. 验证在习题 1.7 的同构下, 有如下交换图表:

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

♣ 记右侧映射为 ψ_α, 只需在一组基下验证图表的交换性. 取 $e_1, \cdots, e_n$ 为 L 的 K-基, 则 $1 \otimes e_1, \cdots, 1 \otimes e_n$ 为 $\bar{K} \otimes_K L$ 的一组基, 由习题 1.7, 它们通过同构对应到右边为 $\sum\limits_{\sigma\in G} \sigma(e_1)\sigma^{-1}, \cdots, \sum\limits_{\sigma\in G} \sigma(e_n)\sigma^{-1}$, 而左乘 α 只需将 e_i 替换为 αe_i, 故对应到 $\bar{K}[G]$ 上会将 $\sum\limits_{\sigma\in G} \sigma(e_i)\sigma^{-1}$ 映为 $\sum\limits_{\sigma\in G} \sigma(\alpha e_i)\sigma^{-1}$. 另一方面, 有 $\psi_\alpha\left(\sum\limits_{\sigma\in G} \sigma(e_i)\sigma^{-1}\right) = \sum\limits_{\sigma\in G} \sigma(e_i)\psi_\alpha(\sigma^{-1}) = \sum\limits_{\sigma\in G} \sigma(e_i)\sigma(\alpha)\sigma^{-1}$, 故上面的图表交换. ♢

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 $N_{L/K}(\beta) = 1 \Leftrightarrow \exists \alpha \in L^*,\ s.t.\ \beta = \dfrac{\sigma\alpha}{\alpha}$.

♣ $\Leftarrow$ 部分是显然的, 只需证明 $\Rightarrow$ 部分. 这等价于说 $N_{L/K}(\beta) = 1$ 时, 存在 α

为 L 上的 K-线性方程 $\sigma(\alpha)-\varphi_\beta(\alpha)=0$ 的非零解. 记 $\alpha=x_1e_1+\cdots+x_ne_n$, 其中 (e_i) 为一组基, 令 $X=(x_1\ \cdots x_n)^T$, 上面的方程可写成 $AX=0$, 此时 $\det A$ 是关于 $\beta=a_1e_1+\cdots+a_ne_n$ 的系数 a_i 的多项式, 方程有非零解等价于 $\det A=0$. 我们将系数扩张到 $\bar{K}$ 上, 并通过习题 1.7中的同构在 $\bar{K}[G]$ 中解方程 $\sigma\cdot\gamma-\psi_\beta(\gamma)=0$($\psi_\beta$ 为上一题中定义的映射), 类似地, 取对应的基后这相当于解 $\bar{K}$ 系数的方程 $A\tilde{X}=0$, 故只需证存在非零的 γ 满足方程. 令 $\gamma=\sum\limits_{i=0}^{k}c_k\sigma^k$, 其中 $c_k=\prod\limits_{i=0}^{k}\sigma^i(\beta)$, 则可直接验证这给出一个解 (由 $N_{L/K}(\beta)=c_{n-1}=1$ 保证). ♢

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 $Tr_{L/K}(\beta)=0\Leftrightarrow\exists\alpha\in L,\ s.t.\ \beta=\sigma(\alpha)-\alpha$.

♣ 我们同样只需证 $\Rightarrow$ 部分. 沿用前一问的记号, 这等价于说在 $Tr_{N/K}(\beta)=0$ 时存在 α 为 L 的非齐次 K-线性方程 $\sigma(\alpha)-\alpha=\beta$ 的解. 类似前一题的说明, 此时在 L 中有解等价于做系数扩张后再 $\bar{K}[G]$ 中有解, 也即 $(\sigma-1)\gamma=\sum\limits_{k=0}^{n-1}\sigma^k(\beta)\cdot\sigma$ 有解. 令 $\gamma=\sum\limits_{k=0}^{n-1}c_k\sigma^k$, 其中 $c_k=-\sum\limits_{i=0}^{k}\sigma^i(\beta)$, 可验证这给出一个解 (由 $Tr_{L/K}(\beta)=-c_{n-1}=0$ 保证). ♢

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:

$$\varphi_\sigma\colon \bar{K}[G]\to\bar{K}[G]$$

$$\tau\mapsto\tau^{-1}(f(\sigma))\cdot\tau$$

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 $f(\sigma_1\sigma_2)=f(\sigma_1)\cdot\sigma_1(f(\sigma_2)),\ \forall\sigma_1,\sigma_2\in G$.

♣ 将 *1* 的两边写为求和式得到 $\sum\limits_{h\in G}c_hh^{-1}(f(\sigma))h=\sum\limits_{h\in G}c_h(\sigma\cdot h)$, 比较系数得到 $c_hh^{-1}(f(\sigma))=c_{\sigma^{-1}.h}\ \forall\sigma,h\in G$.

1⇒*2* : 令上式 h 取 1, σ 取 h^{-1} 即得 $c_1\cdot f(h^{-1})=c_h$. 取 $h{=}\sigma_1^{-1}$, $\sigma=\sigma_2$ 有 $c_{\sigma_1^{-1}}\sigma_1(f(\sigma_2))=c_{\sigma_2^{-1}\sigma_1^{-1}}$, 再用前一式子代换得到 $c_1\cdot f(\sigma_1)\cdot\sigma_1(f(\sigma_2))=c_1\cdot f(\sigma_1\sigma_2)$, 若 $c_1=0$ 将有任意的 $c_h=0$, 与 $a\neq0$ 矛盾, 故两边消去 c_1 即证.

2⇒*1* : $c_{\sigma^{-1}.h}=c_1\cdot f(h^{-1}\sigma)=c_1\cdot f(h^{-1})\cdot h^{-1}(f(\sigma))=c_h\cdot h^{-1}(f(\sigma))$. ♢

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 $H^1(G,L^*)=\{1\}$.

♣ ⇐ 部分直接代入验证即可, 只需证 ⇒. 注意到 $\exists a\in L^*,\ s.t.\ f(\sigma)=\dfrac{\sigma(a)}{a},\ \forall\sigma\in G\Leftrightarrow$ 关于 a 的 L 中的 K-线性方程组 $\varphi_{f(\sigma)}(a)-\sigma(a)=0,\ \forall\sigma\in G$ 存在非零解. 与前面相同, 做系数扩张后, 利用习题 1.7 , $\varphi_{f(\sigma)}$ 将对应到 φ_σ, 故对应方程恰为习题 3的 *1.* 因此取 $c_1=1,\ c_h=f(h^{-1})$, 由习题 3即知此时方程有解. ♢

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 $H^1(G,L)=\{0\}$.

♣ 与乘法情形同理, 考虑方程 $\sigma(a)-a=\varphi_{f(\sigma)}(1)$ 的解. 由习题 1.7, 可将 $\bar{K}_KL$ 的单

位元对应至 $\beta=\sum_{\tau\in G}\tau$, 进而扩张系数后只需考虑方程 $(\sigma-1)a=\varphi_\sigma(\beta)=\sum_{\tau\in G}\tau^{-1}(f(\sigma))\tau$.

完全仿照习题 3可给出加法情形, 即 $c_1=0,\ c_h=f(h^{-1})$ 给出方程的一个解. ♢

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.

♣ 由于 x 在 K 上代数, 设 $P_{x,K}$ 为 x 在 K 上的极小多项式, 那么 $[K(x) : K] = \deg P_{x,K} < \infty$. 故 $[K(y) : K] = [K(x) : K] = \deg P_{x,K} < \infty$, 因此 y 在 K 上代数, 且 $\deg P_{y,K} = [K(y) : K] = [K(x) : K] = \deg P_{x,K}$. ♢

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

♣ 据域的特征是否为 2 讨论.

若 $Car(K) \neq 2$, 任取 $x \in L\backslash K$, 则 x 的极小多项式次数为 2 次, 不妨设为 $f(x) = ax^2 + bx + c$, 其中 $a \neq 0$. 令 $z = ax + \dfrac{b}{2}$, 则 $z^2 = \dfrac{b^2}{4} - ac \in K$, 且 $L = K(z)$. 此时 $\mathrm{Gal}(L/K) = \{id, \sigma\}$, 其中 $\sigma\colon z \mapsto -z \in L$. 故 L/K 为 Galois 扩张. 特别地, 是正规扩张.

若 $Car(K) = 2$, 任取 $x \in L\backslash K$, 设 x 的极小多项式为 $f(x) = x^2 + ax + b = 0$, 其中 $a, b \in K$. 若 $a^-4b = a^2 = 0$, 则 f 只有二重根 x. 若 $a^2 \neq 0$, 则 f 的另一个根为 $x' = -a - x \in L$. 因此总有 L 是 f 的分裂域, 因而 L/K 为正规扩张. ♢

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 Λ 在 K 上生成的 L 的子环, 它是否一定等于 Λ 在 K 上生成的子域 $K(\Lambda)$?

♣ 首先 $K[\Lambda] \subset K(\Lambda)$. 接下来只需证明 $K[\Lambda]$ 中非零元均可逆. 注意到 $K[\Lambda]$ 中元素在 K 上均代数, 任取非零元 $a \in K[\Lambda]\backslash\{0\}$, 取其极小多项式 $P_{a,K}$, 使得 $P_{a,K}(a) = a^n + c_{n-1}a^{n-1} + \ldots + c_1 a + c_0 = 0$(由 $a \neq 0$ 知 $c_0 \neq 0$), 故 $-\dfrac{a^{n-1} + c_{n-1}a^{n-2} + \ldots + c_1}{c_0}$

即为 a 在 $K[\Lambda]$ 中的一个逆. 这就说明了 $K[\Lambda] = K(\Lambda)$. ♢

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 Σ 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 Σ.)

♣ 自然有 $[K_n : K] = 2^n > 1$. 若 K 是无限集, 则 $K_n \backslash K$ 是无限集, 从而不能是在 K 上可建造的. 因此这样的 K 必须是 R 的有限子域, 也即 K 不存在. ♢

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?

♣ 设 $P(x) = \sum_{k=0}^{n} a_k x^k$, $Q(x) = \sum_{j=0}^{m} b_j x^j$, 其中 $a_n \neq 0$, $b_m \neq 0$. 记 $K[X]_d$ 为 $K[X]$ 中次数不超过 d 的多项式集合, 则对任意 $A(x) = \sum_{k=0}^{m-1} c_k x^k \in K[X]_{m-1}$, $B(x) = \sum_{j=0}^{n-1} d_j x^j \in K[X]_{n-1}$, 可记 $P(x)A(x) + Q(x)B(x) = \sum_{i=0}^{m+n-1} z_i x^i \in K[X]_{m+n-1}$. 比较这个式子两侧各项系数, 可得:

$$\begin{pmatrix} a_0 & & & b_0 & & \\ & \ddots & & \vdots & \ddots & \\ \vdots & & a_0 & & & b_0 \\ a_n & & & b_m & & \\ & \ddots & & & \ddots & \\ & & a_n & & & b_m \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{m_1} \\ d_0 \\ \vdots \\ d_{n-1} \end{pmatrix} = \begin{pmatrix} z_0 \\ \vdots \\ z_{m_1} \\ z_m \\ \vdots \\ z_{m+n-1} \end{pmatrix}$$

将这个映射记为 φ: $K^{m+n-1} \to K^{m+n-1}$, 则 φ 为线性空间之间的线性映射, 且在标准基下的矩阵表示即为

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

如果 $P(x)$ 与 $Q(x)$ 互素, 由 Bézout 引理, 对任意 $T(x) \in K[X]_{m+n-1}$, 总可找到 $A(x) \in K[X]_{m-1}$ 和 $B(x) \in K[X]_{n-1}$, 使得 $P(x)A(x) + Q(x)B(x) = T(x)$. 换言之, 此时 φ 是满射, 进而是线性空间之间的同构, 那么 $Res(P, Q) = \det M \neq 0$.

反过来, 如果 $Res(P, Q) \neq 0$, 则有 φ 是满射, 那么存在 $F(x) \in K[X]_{m-1}$ 和 $G(x) \in K[X]_{n-1}$, 使得 $P(x)F(x) + Q(x)G(x) = 1$. 这自然得到 $(P(x), Q(X))|1$, 只能是 $P(x)$ 与 $Q(x)$ 互素. $\diamondsuit$

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.

♣ 首先, 如果 K 是有限域或可数域, 那么 $K(X)$ 中元素个数可数. 事实上, 对 $f \in K(X)$, 总可写成 $f = \dfrac{g}{h}$, 其中 $g, h \in K[X]$. 但由于 K 有限或可数, 知 $K[X]$ 中只有可数多个多项式, 从而 $K(X)$ 也是可数集, 因此其作为 K 上的线性空间不可能是不可数维的, 即 $[K(X) : K]$ 是可数的.

另一方面, 若 K 不可数, 我们证明集合 $\{\dfrac{1}{X-k} \mid k \in K\}$ 是 K 上的线性无关集. 若存在有限个 $k_1, \ldots, k_n \in K$, 及不全为零的 $\lambda_1, \ldots, \lambda_n \in K$, 使得 $\sum\limits_{i=1}^{n} \lambda_i \dfrac{1}{X-k_i} = 0$, 将之通分可得 $\sum\limits_{i=1}^{n} \lambda_i \prod\limits_{j=1, j\neq i}^{n} (X-k_j) = 0$. 不妨设 $\lambda_1 \neq 0$, 则由 $X - k_1$ 整除其余各项, 可知 $(X-k_1) | \lambda_1 \prod\limits_{j=2}^{n} (X-k_j)$, 这显然矛盾. 故我们找到了 $K(X)$ 中一个在 K 上线性无关的不可数集, 从而 $[K(X) : K]$ 不可能是可数的. ♢

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

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

♣ 我们证明以下结论: 若 $x \in \mathcal{L}$, 那么 $x + \dfrac{a}{b} \in \mathcal{L}$, $\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}$. 若该结论成立, 由 $\mathbb{Q}$ 的稠密性立刻得到 $\mathcal{L}$ 的稠密性.

取定 $x \in \mathcal{L}$ 及 $(a,b) \in \mathbb{Z} \times \mathbb{Z}$. 对固定的 $n \in \mathbb{N}$, 取 m 使得 $|b|^n < 2^{m-n}$. 由 $x \in \mathcal{L}$, 存在无穷多组 $(c,d) \in \mathbb{Z} \times (\mathbb{Z} \backslash \{\pm 1\})$, 使得 $|x - \dfrac{c}{d}| < \dfrac{1}{d^m}$. 因此可做如下计算:

$$|(x + \frac{a}{b}) - (\frac{a}{b} + \frac{c}{d})| = |x - \frac{c}{d}| < \frac{1}{|d|^m} \leq \frac{1}{|bd|^n}$$

因为 $|b|^n < 2^{m-n} \leq |d|^{m-n}$. 故 $x + \dfrac{a}{b} \in \mathcal{L}$. 再由开头的论述可知 $\mathcal{L}$ 在 $\mathbb{R}$ 中稠密. ♢

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

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

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

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

♣ 由于 $\dfrac{1}{(1-T^n)^{f(n)}} = \sum\limits_{k=0}^{\infty} \binom{k+f(n)-1}{f(n)-1} T^{nk}$, 只需证明

$$\sum_{n\in\mathbb{N}} p^n T^n = \prod_{n\in\mathbb{N}^*} \sum_{k=0}^{\infty} \binom{k+f(n)-1}{f(n)-1} T^{nk}$$

我们证明: 上式两侧 T^n 前系数都是 $\mathbb{F}_p[X]$ 中 n 次首一多项式的个数. 一方面, 除去最高次项, 每项系数有 p 种选择, 因此这个个数即是 p^n, 等于左侧 T^n 前系数. 另一方面, 对每个首一 n 次多项式做不可约因式分解, 并设分解出的诸不可约因子的次数满足次数为 k 的 i 共有 s_k 个, 则这类 n 次首一多项式个数为

$$\prod_{k\in N^*} \binom{f(k)+s_k-1}{f(k)-1}$$

这是因为, 这个选取的过程相当于对每个 $k \in N^*$, 在所有 $f(k)$ 个 k 次不可约多项式中可重复且不排序地选出 s_k 个, 每种选法与

$$\{(x_1, \ldots, x_{f(k)} \in \mathbb{N}^{f(k)} | x_1 + \ldots + x_{f(k)} = s_k\}$$

的一个元素对应. 由组合知识可知这个个数是 $\binom{f(k)+s_k-1}{f(k)-1}$. 因此,$n$ 次首一多项式的总数

也可以表示为

$$\sum_{\substack{\sum\limits_{k\in\mathbb{N}} ks_k=n \\ s_k\in\mathbb{N},\ \forall k\in\mathbb{N}}} \prod_{k\in N^*} \binom{f(k)+s_k-1}{f(k)-1}$$

而这恰好就是 $\prod\limits_{k\in\mathbb{N}^*}\sum\limits_{s_k=0}^{\infty}\binom{s_k+f(k)-1}{f(k)-1}T^{ks_k}$ 的 T^n 前系数. 事实上, 为了在这个乘积中得到 T^n, 需要对每个 k, 在 k 对应的求和项中选定 s_k, 使得 $\sum\limits_{k\in\mathbb{N}} ks_k = n$. 每固定一次 $(s_k)_{k\in\mathbb{N}}$, 得到的 T^n 前系数便是 $\prod\limits_{k\in\mathbb{N}^*}\binom{f(k)+s_k-1}{f(k)-1}$, 因此对所有取法求和后给出的 T^n 前系数恰为以上得出的 $\mathbb{F}_p[X]$ 中 n 次首一多项式的个数. 对 $\prod\limits_{k\in\mathbb{N}^*}\sum\limits_{s_k=0}^{\infty}\binom{s_k+f(k)-1}{f(k)-1}T^{ks_k}$ 替换求和指标后, 即给出了最开始的右式. 进而我们得到了左右两式 T^n 前的系数相等, 因此原恒等式成立. ♢

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, $\varepsilon(k)\in\{\pm1\}$ 为可显式写出的符号函数.

♣ 在*8.1*所得的恒等式中, 利用 $\sum\limits_{n\in\mathbb{N}} p^nT^n = \dfrac{1}{1-pT}$ 可得

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

对上式求导 (这个步骤的合理性将在注中给出), 即有

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

再利用 $\dfrac{1}{1-T^n} = \sum\limits_{k\in\mathbb{N}} T^{kn}$ 及 $\sum\limits_{n\in\mathbb{N}} p^nT^n = \dfrac{1}{1-pT}$, 有

$$\sum_{n\in\mathbb{N}^*} nf(n)T^{n-1}\sum_{k\in N}T^{kn} = p\sum_{n\in N}p^nT^n$$

对 $n \geq 1$, 比较上式两侧 T^{n-1} 前系数, 可得

$$\sum_{\substack{d|n \\ d\in N^*}} df(d) = p^n$$

对此式做 Möbius 反演, 可得

$$nf(n) = \sum_{d|n} \mu(d) p^{\frac{n}{d}}$$

其中 μ 为 Möbius 函数. 这即给出了 $nf(n)$ 的一个显式表达. $\diamondsuit$

注: 求导步骤的问题在于:

(i) 有限乘积的求导法则是否可以推广到无穷乘积上.

(ii) 如果可以, 依此法则求导后得到的式子是否还落在形式幂级数环内.(注意 $\mathbb{Z}$ 系数的形式幂级数环的定义是 $\mathbb{Z}[[X]] = \{\sum_{n\in\mathbb{N}} a_n x^n \mid a_n \in \mathbb{Z}, \forall n \in N\}$, 所以一般的无穷乘积并不一定是 $\mathbb{Z}[[X]]$ 中良定的元素, 因为其展开后的系数不一定有限, 比如 $\prod_{n\in\mathbb{N}}(1-X)^n \notin \mathbb{Z}[[X]]$)

无妨在 $\mathbb{C}[[X]]$ 中考虑本题. 一般地, 对于域 K 及形式幂级数环 $K[[X]]$, 我们对 $\alpha = \sum_{n\in\mathbb{N}} \in K[[X]]$ 定义 $\inf(\alpha) = \inf\{n \in \mathbb{N} \mid a_n \neq 0\}$, 则我们可以在 $K[[X]]$ 上定义范数

$$\|\alpha\| = 2^{-\inf(\alpha)},\ \alpha \neq 0,\ \|0\| = -\infty$$

可以验证, 这个范数让 $K[[X]]$ 成为一个 Banach 空间.

进一步地, 我们有如下结果: 若 $\alpha_1, \alpha 2, \ldots \in \mathbb{C}[[X]]$, 且 $\|\alpha_k\| \to 0$, 则有如下无穷乘

积的求导法则成立:

$$\left(\prod_{k\in\mathbb{N}}(1+\alpha_k)\right)'=\prod_{k\in\mathbb{N}}(1+\alpha_k)\sum_{k\in\mathbb{N}}\frac{\alpha_k'}{1+\alpha_k}$$

在 *8.2* 中, 令 $\alpha_k=1-(1-T^k)^{f(k)}$, 则有 $\|\alpha_k\|\leq 2^{-k}$, 故 $\|\alpha_k\|\to 0$, 由上述求导法则即得所需等式.

注中细节及更多关于形式幂级数的内容可参考文章 [4].

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.

♣ 由 $nf(n)=\sum\limits_{d|n}\mu(d)p^{\frac{n}{d}}$, 做估计

$$nf(n)=\sum_{d|n}\mu(d)p^{\frac{n}{d}}\geq p^n-\sum_{k=1}^{n-1}p^k\geq p^n-\frac{p^n-1}{p-1}>0$$

故 $f(n)>0$, 因此对任意 $n\in\mathbb{N}^*$, 存在 $\mathbb{F}_p[X]$ 中的 n 次首一不可约多项式 g_n. 考虑域 $\mathbb{F}_p[X]/(g_n)$, 即得一 p^n 元域. ♢

注: 也可以直接用 $p^n=\sum\limits_{d|n}df(d)$ 得出本题结论. 由

$$p^n=\sum_{d|n}df(d)$$

可得到 $p^d=df(d)+\sum\limits_{d'|d,\ d'<d}d'f(d')$. 特别地, 有 $df(d)\leq p^d$. 为此有

$$p^n\leq nf(n)+\sum_{d|n,\ d<n}p^d\leq nf(n)+\sum_{k=0}^{n-1}p^k=nf(n)+\frac{p^n-1}{p-1}<nf(n)+p^n$$

故 $f(n)>0$

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.

♣ $X^{p^n}-X$ 在 $\mathbb{F}_p[X]$ 上的分裂域正是 $\mathbb{F}_{p^n}$. ♢

注: 事实上, 考虑 $X^{p^n}-X$ 后, 可以用更简洁的观点来计算 $f(n)$. 首先有熟知事实: n 次扩域 $\mathbb{F}^{p^n}$ 的全体元素恰好是 $\mathbb{F}_p$ 上的方程 $X^{p^n}-X$ 的全体 p^n 个根. 若 f 是一个 $\mathbb{F}_p[X]$ 中的 d 次首一不可约多项式, 且 $f|X^{p^n}-X$, 则 $\mathbb{F}_p[X]/(f)\simeq\mathbb{F}_{p^d}$ 作为 f 的分裂域 (这是一个 Galois 扩张) 是 $\mathbb{F}_{p^n}$ 的一个子域, 其扩张次数 d 满足 $d|n$. 反过来, 若 $d|n$, 则 $\mathbb{F}_p[X]/(f)\simeq\mathbb{F}_{p^d}$ 是 $\mathbb{F}_{p^n}$ 的子域, 从而 f 的所有根都是 $X^{p^n}-X$ 的根, 也就是说 $f|X^{p^n}-X$ 等价于 $d|n$. 由此, 我们可以把 $X^{p^n}-X$ 分解为这些首一不可约多项式的乘积:

$$X^{p^n}-X=\prod_{d|n}\prod_{\substack{\deg f=d\\ f\text{ 首一不可约}}}f(X)$$

比较两边 X 的最高次项次数可得 $p^n=\sum\limits_{d|n}df(d)$.

需要注意的是, 不能用这个途径去证明 *8.3*, 因为我们在计算 $f(n)$ 的过程中已经使用了存在 p^n 元域的事实.

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 ζ_n 为这个根, 即需要给出 $K_n=\mathbb{Q}(\zeta_n)$.

♣ P_n 的所有根为 ζ_n^j, 其中 $\zeta_n=e^{\frac{2\pi i}{n}}$, $0\leq j\leq n-1$. 取出这个 ζ_n, 即有 $\mathbb{Q}(\zeta_n)\subset K_n=\mathbb{Q}(\zeta_n,\ldots,\zeta_n^{n-1})\subset\mathbb{Q}(\zeta_n)$. 故 $K_n=\mathbb{Q}(\zeta_n)$. ♢

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

♣ 此时 $\dfrac{X^n-1}{X-1}$ 零化 ζ_n, 且由 Einsenstein 判别法可知 $\dfrac{X^n-1}{X-1}$ 不可约. 所以有 $[\mathbb{Q}(\zeta-n):\mathbb{Q}]=n-1$. ♢

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 $\phi_n(X) = \prod_{\zeta\in\tilde{\mu}_n(K_n)} (X-\zeta)$;

♣ 此处不是题目, 只是一个承接. 保留这个小问是为了和法文试卷题号保持一致.♢

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

♣ 由于 $K_n = \mathbb{Q}(\zeta_n)$, 可知对 $\forall d \in N^*$, $d|n$, K_n 都包含了所有的 d 次本原单位根. 而 d 次本原单位根的个数为 $\varphi(d)$. 考虑 $P_n(X) = \prod_{j=0}^{n-1}(X-\zeta_n^j) = \prod_{d|n}\prod_{\zeta\in\tilde{\mu}_d(K_n)} (X-\zeta) = \prod_{d|n}\phi_d$. 比较这个等式两边关于 X 的次数, 可知 $\deg P_n = n = \deg\prod_{d|n}\phi_d = \sum_{d|n}\varphi(d)$. ♢

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

♣ 任取 $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ 及 $\zeta \in \tilde{\mu}_n(K_n)$, 考虑 σ 作用在 $\tilde{\mu}_n$ 的极小多项式上, 可知 $\zeta \in \tilde{\mu}_n(K_n) \Leftrightarrow \sigma(\zeta) \in \tilde{\mu}_n(K_n)$. 因此

$$\sigma(\phi_n(X)) = \sigma(\prod_{\zeta\in\tilde{\mu}_n(K_n)} (X-\zeta)) = \prod_{\zeta\in\tilde{\mu}_n(K_n)} (X-\sigma(\zeta)) = \prod_{\zeta\in\tilde{\mu}_n(K_n)} (X-\zeta)$$

也即 $\sigma(\phi_n(X)) = \phi_n(X)$, 故 $\phi_n(X)$ 的各项系数均在 $\mathbb{Q}$ 中, 也即是说 $\phi_n(X) \in \mathbb{Q}(X)$. 而 $\phi_n(X)|P_n(X)$, 后者是 $\mathbb{Q}(X)$ 中的本原多项式, 又 $\phi_n(X)$ 首一, 由 Gauss 引理可知 $\phi_n \in \mathbb{Z}[X]$. ♢

9.6 在什么条件下我们有 $X^n - 1 \in K[X]$ 是可分的?

♣ 分域 K 的特征讨论.

i) 若 $Car\ K = 0$, 那么 $X^n - 1$ 当然可分.

ii) 若 $Car\ K = p$, 其中 p 为素数, 考虑代数导数, 可知 $X^n - 1$ 不可分当且仅当 $X^n - 1 \in K[X^p] \Leftrightarrow p|n$. 所以, 如果 $p \nmid n$, 有 $X^n - 1$ 可分.

综上, 若 $Car\ K=0$ 或 $Car\ K=p$ 且 $p\nmid n$, 那么 X^n-1 可分. ♢

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 ϕ_n 的一个不可约因子. 证明若 ζ 是 Q 的根, 那么 ζ^p 也是.

♣ 由假设, 可知 Q 为 ζ 在 $\mathbb{Q}$ 上的极小多项式.

先证明 $K_n/\mathbb{Q}$ 是 Galois 扩张, 即 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 是正规且可分的扩张. 由*9.1*知 $\mathbb{Q}(\zeta_n)$ 是 $P(X)=X^n-1$ 在 $\mathbb{Q}$ 上的分裂域, 因此该扩张正规. 由特征 0 即知该扩张可分, 因此该扩张为 Galois 扩张. 由 $(p,n)=1$, 可知 ζ^p 也为 n 次本原单位根, 这是因为集合 $\{d\mid 1\leq d\leq n,\ (d,n)=1\}$ 和集合 $\{pd\mid 1\leq d\leq n,\ (d,n)=1\}$ 在模 n 意义下相等.

考虑映射

$$\sigma_p\colon \mathbb{Q}(\zeta_n)\to\mathbb{Q}(\zeta_n)),\ \zeta_n\mapsto\zeta_n^p,\ \sigma_p|_{\mathbb{Q}}=id|_{\mathbb{Q}}$$

可知 σ_p 是域同构, 即 $\sigma_p\in\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. 考虑 ϕ_n 在 $\mathbb{Q}(X)$ 中的不可约分解 $\phi_n(X)=Q_1(X)\cdot\mathbb{Q}_t(X)$, 其中 $Q_1=Q$. 如果 ζ^p 不是 Q 的根, 不妨设 ζ^p 为 Q_2 的根. 用 σ_p 作用在 $Q(\zeta)=0$ 上, 得 $Q(\zeta^p)=0$. 而 ζ^p 在 $\mathbb{Q}$ 上的极小多项式是 Q_2, 因此有 $Q_2|Q$, 矛盾. 故 ζ^p 也是 Q 的根. ♢

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

♣ 对 $d>0$ 且 $(d,n)=1$, 将 d 分解为 $d=p_1^{\alpha_1}\cdot\ldots\cdot p_t^{\alpha_t}$, 其中 $p_i\nmid n$, $i=1,\ldots,t$. 由*9.7*, 取 $\zeta=e^{\frac{2\pi i}{n}}$ 为 n 次本原单位根, 那么 $Q(\zeta_n)=0\Rightarrow Q(\zeta_n^{p_1})=0\Rightarrow\ldots\Rightarrow Q(\zeta_n^{p_1^{\alpha_1}\cdot\ldots\cdot p_t^{\alpha_t}})=0$, 故 $Q(\zeta_n^d)=0$. 但 $\tilde{\mu}_n(K_n)=\{\zeta_n^d\mid 1\leq d\leq n,\ (d,n)=1\}$. 因此 $\deg Q=\deg\phi_n$, 故 ϕ_n 在 $\mathbb{Q}[X]$ 中不可约. ♢

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

♣ 由 *9.7*, *9.8*, ζ_n 在 $\mathbb{Q}$ 上的极小多项式是 $P_{\zeta_n,\,\mathbb{Q}}=\phi_n$. 因此 $[\mathbb{Q}(\zeta_n:\mathbb{Q}]=\deg\phi_n=$

$\varphi(n)$. ♢

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?

♣ 设扩张次数 $[L:Q] = m < \infty$. 对 $a \in \bigcup_{n\in\mathbb{N}^*}$, 若其为 n 次本原单位根, 由 *9.9* 可知 $[\mathbb{Q}(a):\mathbb{Q}] = \phi(n)$. 但是 $\mathbb{Q} \subset L$, 由此一定有 $\phi(n) \le m$. 注意到 $\phi(n) \ge \sqrt{n} - 1$, 可知 $\bigcup_{n\in\mathbb{N}^*}\mu_n(L) \subset \bigcup_{\substack{n\in\mathbb{N}^*\\ n\le(m+1)^2}}\tilde{\mu}_n(L)$, 而对每个 $n \in N^*$, $\tilde{\mu}_n(L)$ 是有限群, 故 $\bigcup_{n\in\mathbb{N}^*}\mu_n(L)$ 也是有限群. ♢

注: 这一小问作为一个熟知的结论, 其证明可以独立给出 (不用前面的小问). 设 w 是 L 中的 n 次单位根, 令 $f(x) = x^m + c_1x^{m-1} + \ldots + c_m$ 是 w 在 $\mathbb{Q}$ 上的极小多项式, $f(x)$ 的全部根为 $w = w_1, w_2, \ldots, w_m$. 由于 $w^n = 1$, 从而 $f(x)|x^n - 1$, 于是 w 的每个共轭元均满足 $w_i^n = 1$, 也即 w_i 都是 n 次单位根. 于是 $|w_i| = 1(1 \le i \le m)$. 由韦达定理可知 $|c_i| \le \binom{m}{i}(1 \le i \le m)$. 另一方面, 由于 $f(x)$ 是 $x^n - 1$ 的首一多项式因子, 由 Gauss 引理可知 $f(x) \in \mathbb{Z}[X]$. 进而, 由于 $w \in K$, 可知 $m = \deg f = [\mathbb{Q}(w):\mathbb{Q}] \le [L:\mathbb{Q}]$ 有限. 但是次数不超过 $[L:\mathbb{Q}]$, 且 i 次项系数为不超过 $\binom{[K:\mathbb{Q}]}{i}$, $1 \le i \le [L:\mathbb{Q}]$ 的整系数多项式个数只有有限多个, 从而它们的根只有有限多个, 这就表明 L 中只有有限多个单位根.

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?

♣ 考虑域 L 中的本原 m 次单位根 α, 则由*9.9*可知 $[\mathbb{Q}(\alpha):\mathbb{Q}] = \varphi(m)$. 但 $\mathbb{Q}(\alpha) \subset$

L, 故 $[L:\mathbb{Q}]=[L:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]$, 这给出 $\varphi(m)|p^n$. 若 m 有奇素因子, 可知 $\varphi(m)$ 为偶数, 不可能是 p^n 的因子. 因此 $\exists k\in N^*$, 使得 $m=2^k$. 但此时 $\varphi(m)=2^{k-1}$, 若要整除 p^n, 只能是 $k=1$, 即 $m=2$, 故 $a=1$. 也就是说域 L 中的单位根此时只有平凡单位根 $\{\pm 1\}$. ♢

9.12 在 $p=2$ 的情形结论是否是不同的?

♣ 此时*9.11*的结论不再成立, 即 L 中可以有非平凡的单位根. 仍采用 *9.11* 的记号, 此时要求 $\varphi(m)$ 为 2 的幂次, 我们将 m 取为 Fermat 素数即可. 比如取 $L=\mathbb{Q}(\zeta_{17})$, 则 $[L:\mathbb{Q}]=16=2^4$, 但是 L 中显然有 17 次单位根. ♢

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

♣ 有关系 $\phi_{2n}(X)=\phi_n(-X)$. 事实上, 注意到 $\zeta_{2n}^n=-1$, 有 $\zeta_{2n}=-\zeta_{2n}^{n+1}=-\zeta_n^{\frac{n+1}{2}}$. 注意 $\dfrac{n+1}{2}$ 与 n 互素, 且 $\varphi(n)$ 为偶数, 我们有:

$$\phi_n(-X)=\prod_{\substack{1\leq d\leq n,\\(d,n)=1}}(-X-\zeta_n^d)=\prod_{\substack{1\leq d\leq n,\\(d,n)=1}}(X+\zeta_n^d)=\prod_{\substack{1\leq d\leq n,\\(d,n)=1}}(X+(\zeta_n^{\frac{n+1}{2}})^d)=\prod_{\substack{1\leq d\leq n,\\(d,n)=1}}(X+(-1)^d\zeta_{2n}^d)$$

对 $1\leq d\leq n$ 分类讨论, 以考察这个乘积.

i) 若 d 是奇数, 则 $(d,2n)=(d,n)=1$, 且 $(-1)^d=-1$, 我们在以上乘积中保留这一因子.

ii) 若 d 是偶数, 则 $(d+n,2n)=1$, 且 $(d,2n)=2$, 此时 $(-1)^d=-\zeta_{2n}^n$, 我们在以上乘积中将 $(X+(-1)^d\zeta_{2n}^d)$ 替换为 $(X-\zeta_{2n}^{n+d})$.

iii) 如果 d 与 n 不互素, 则 $d+n$ 与 $2n$ 也不互素. 不必增添新的因子.

综上有

$$\phi_n(-X) = \prod_{\substack{1\le d\le n,\\ (d,n)=1}} (X + (-1)^d \zeta_{2n}^d) = \prod_{\substack{1\le d\le n,\\ (d,n)=1}} (X - \zeta_{2n}^d) = \phi_{2n}(X)$$

此即为所要证明的关系. ♢

注: 特别地, 若 $n \equiv 2 \mod 4$, 本问给出 $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/2})$. 所以通常对于分圆域 $\mathbb{Q}(\zeta_n)$, 可以规定 $n \not\equiv 2 \mod 4$. 在这一规定下, 可以证明当 $n \neq n'$ 时 $\mathbb{Q}(\zeta_n) \neq \mathbb{Q}(\zeta_{n'})$, 并且也不难决定 $\mathbb{Q}(\zeta_n)$ 的单位根群. 关于这两个命题可以参考 [6] 第一章的习题 8 和习题 9.

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.

♣ 记 P 的常数项为 c.

若 $c = 0$, 命题显然成立. 具体地, 我们有 $p|P(p),\ \forall p \in \mathcal{P}$.

若 $c \neq 0$, 假设命题不成立, 即 $\{p \in \mathcal{P} \mid \exists n \in N^*,\ p|P(n)\}$ 为有限集, 设其为 $\{p_1, p_2, \ldots, p_t\}$. 考虑 $n = c^2 \prod_{i=1}^{t} p_i^k$, 其中 $k \in \mathbb{N}^*$. 由假设, $P(n)$ 一定可以写成 p_i 幂次的乘积. 但考察 $P(n)$ 可知, 如果 $p_i \nmid c$, 有 $p_i \nmid P(n)$. 如果 $p_i|c$, 则 $v_{p_i}(P(n)) = v_{p_i}(c)$. 因此 $P(n) = c$. 当 k 取遍 $\mathbb{N}^*$ 时, 上式总成立, 这表明多项式 $P(X) - c$ 有无穷多个零点, 故 $P(X) \equiv c$, 与非常值的假设矛盾! 因此原集合一定是无限集. ♢

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

♣ 在模 p 意义下, 即是说 $\phi_n(X)$ 作为 $\mathbb{F}_p$ 中的多项式 (每项系数模 p 得到, 仍记为 $\phi_n(X)$, 后面的 X^n-1 同理) 有根 $\bar{\alpha}$. 由于在 $\mathbb{F}_p$ 中仍然有 $\phi_n(X)|(X^n-1)$, 因此 X^n-1 在 $\mathbb{F}_p$ 中有根 $\bar{\alpha}$. 从而 $p\nmid\alpha$, 且有 $\alpha^n\equiv 1 \mod p$. 设 $\phi_n(X)$ 在 $\mathbb{F}_p[X]$ 中的不可约分解为 $\phi_n=P_1\cdot\ldots\cdot P_t$, 且 $P_1(X)=(X-\bar{\alpha})$. 若 $\bar{\alpha}$ 在 $(\mathbb{Z}/p\mathbb{Z})^*$ 中的阶 s 是比 n 更小的正整数 s, 首先有 $s|n$. 其次 $\bar{\alpha}$ 还是 $\phi_s\in\mathbb{F}_p[X]$ 的根, 这是因为 *9.4* 给出分解 $X^s-1=\prod\limits_{d|s}\phi_d$, 如果 $\bar{\alpha}$ 不是 ϕ_s 的根, 则 $\bar{\alpha}$ 是 ϕ_d 的根, 其中 $d<s$, 这给出 $\bar{\alpha}^d=1$, 与 $\bar{\alpha}$ 的阶是 s 矛盾. 再由 $X^n-1=\prod\limits_{d|n}\phi_d$ 可知, 这说明 $\bar{\alpha}$ 是 X^n-1 在 $\mathbb{F}_p$ 中的重根 (因子 ϕ_n 和 ϕ_s 各提供了一个根 $\bar{\alpha}$), 这与 $(p,n)=1$ 矛盾 ($\Rightarrow X^n-1$ 在 $\mathbb{F}_p$ 中无重根). 故 $\bar{\alpha}$ 在 $(\mathbb{Z}/p\mathbb{Z})^*$ 中的阶恰好是 n. ♢

注: 由于 $\bar{\alpha}^{p-1}\equiv 1 \mod p$, 可知 $n|p-1$, 故 p 是模 n 余 1 的素数.

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.

♣ 素数 p 模 n 余 1, 即是说 p 在乘法群 $(\mathbb{Z}/n\mathbb{Z})^*$ 中的阶为 1. 而由上问后的注可知, 对素数 p, 若存在整数 $k\in\mathbb{Z}$, 使得 $\phi_n(k)\equiv 0 \mod p$, 一定有 p 模 n 余 1.

假设只有有限多个素数 p 模 n 余 1, 设这些素数的上界为 N. 考虑 $\phi_n(m!)$, 其中 $m\geq N$. 当 m 充分大时, 由于 ϕ_n 只有有限个根, 可以设 $\phi_n(m)\neq 0$. 设 p 为 $\phi_n(m)$ 的一个素因子, 也即 $\phi_n(X)$ 在 $\mathbb{F}_p$ 中有根, 这表明 p 模 n 余 1, 因此 $p\leq N$, 从而 $p|m!$. 结合 $p|\phi_n(m!)$, 得到 p 整除 ϕ_n 的常数项. 而 ϕ_n 的常数项为 1, 自然矛盾. ♢

10.4 这个结论让你想到了什么?

♣ Dirichlet 定理: 若 a,b 互素, 则等差数列 $(an+b)_{n\in\mathbb{N}}$ 中有无穷多个素数. ♢

注: 这个定理不少同学在高中数学竞赛中接触过. 我们将在解析数论的课程中进一步学习更深刻的 Dirichlet 定理, 其刻画了模 n 余 a 的素数在自然数中的分布密度.

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.

♣ 事实上, 多项式 $X^{p^m}-X$ 在 $\bar{\mathbb{F}}_p$ 中的根给出域 $\mathbb{F}_{p^m}$, 多项式 $X^{p^n}-X$ 在 $\bar{\mathbb{F}}_p$ 中的根给出域 $\mathbb{F}_{p^n}$. 因此本题即是在问这两个多项式的公共根个数, 即求它们的最大公因式的次数. 各提取一个公因子后转化为两个形如 X^k-1 的多项式, 这两个多项式的最大公因式为 $X^{(p^m-1,p^n-1)}-1$. 因此所求根的个数为 $(p^m-1,p^n-1)+1=p^{(m,n)}=p$. ♢

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?

♣ a- 对任意 $a\in\bar{F}_p$, 考虑多项式 x^p-a, 由代数闭知其有根 α, 也即有 $Fr(\alpha)=a$, 故 Fr 为满射, 从而是同构.

b- 对 $a\in F_{p^n}$, 若 $Fr^k(a)=a$, 即 x 是 $f_k(x)=x^{p^k}-x$ 的根. 记 A_k 为 $F_{p^n}^*$ 中被 Fr^k 固定的元素, 于是 $|A_k|\le\deg(f_k)=p^k$. 另一方面, 考虑任意 $a\in F_{p^n}^*$, 有 a 是 $x^{p^n-1}-1$ 的根, 故有 $Fr^n=Id$. 若 Fr 在 $G=\mathrm{Gal}(F_{p^n}/F_p)$ 中的阶为 m, 应有 $m|n$, 故 $m\le n$. 此时应有 $|F_{p^n}|=|A_m|\le p^m$, 故 $n\le m$, 从而推得 Fr 的阶为 n. 由扩张 Galois 知 $|G|$ 等于扩张次数 n, 只能有 $G=\langle Fr\rangle$.

c- 其因子即所有 F_{p^n} 中的元素的极小多项式. 由于对任意 $d|n$, 给定 d 次不可约多

项式, 其所有根在 F_{p^d} 中, 从而在 F_{p^n} 中. 这说明任意 d 次不可约多项式均是 $x^{p^n}-x$ 的因子. 而 $x^{p^n}-x$ 本身无重根, 其因子也无重根, 且可推得其恰是所有次数整除 n 的不可约多项式的乘积. ♢

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.

♣ 由定义有 $\mathbb{F}_p \subset \bar{\mathbb{F}}_p^G \subset \bar{\mathbb{F}}_p^H$. 而在 Fr 下稳定的元素, 即满足 $x^p = x$ 的元素, 只有 $\mathbb{F}_p$, 又 $H =< Fr >$, 可知 $\bar{\mathbb{F}}_p^H \subset \mathbb{F}_p$, 因此有 $\mathbb{F}_p = \bar{\mathbb{F}}_p^G = \bar{\mathbb{F}}_p^H$. ♢

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 $\bar{\mathbb{F}}_p \backslash \cup_{n\in\mathbb{N}^*} \mathbb{F}_{p^n}$.

♣ a. 考虑所有满足 $X^{p^n}-X$ 的元素, 可以验证这些元素构成一个域. 由于 $X^{p^n}-X$ 在 $\mathbb{F}_p$ 中无重根, 因而这个域恰好有 p^n 个元素, 这便给出了 $\bar{\mathbb{F}}_p$ 的一个阶为 p^n 的子域. 另一方面, 如果 x 是 $\bar{F}_p$ 的一个阶为 p^n 的子域中的非零元素 (这个子域的可逆元构成 p^{n-1} 阶乘法群), 因而一定有 $x^{p^n-1}=1$, 故 x 也满足 $X^{p^n}-X=0$. 故 $\bar{F}_p$ 的 p^n 阶子域唯一.

b. 这样构造的 $\bar{\mathbb{F}}_p$ 当然是 $X^{p^n}-X$ 的分裂域, 因而与我们上课定义的 $\mathbb{F}_{p^n}$ 一致.

c.$\bar{\mathbb{F}}_p \backslash \cup_{n\in\mathbb{N}^*} \mathbb{F}_{p^n} = \varnothing$. 事实上, 对任意 $x \in \bar{F}_p$, 由于 x 在 $\mathbb{F}_p$ 上代数, 不妨设 $[\mathbb{F}_p(x) : \mathbb{F}] = n$, 则 $\mathbb{F}_p(x)$ 为 p^n 元域, 由上知这即是 $\mathbb{F}_{p^n}$, 故 $x \in \mathbb{F}_p(x) = \mathbb{F}_{p^n}$. 这表明 $\bar{\mathbb{F}}_p \subset \cup_{n\in\mathbb{N}^*}\mathbb{F}_{p^n}$(另一个方向的包含是显然的), 故 $\bar{\mathbb{F}}_p \backslash \cup_{n\in\mathbb{N}^*} \mathbb{F}_{p^n} = \varnothing$. ♢

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.

♣ a. 由 $\mathbb{F}_{p_1}^{m_1} \subset \mathbb{F}_{p_2}^{m_2}$ 考虑特征即知 $p_1 = p_2$. 由于 $\mathbb{F}_{p_1}^{m_1}$ 即是 $X^{p^m} - X$ 在 $\bar{F}_p$ 中的所有根, 引第11题可知, 必须有 $m_1|m_2$.

b. 对 $a, b \in K$, 总存在 $N \in N^*$, 使得 $a, b \in \mathbb{F}_{p^{2^n}}$, 故 a 和 b 的二元运算及逆均落在 $\mathbb{F} + p^{2^n}$ 中, 进而落在 K 中, 故 K 是域. 若 $K = \bar{\mathbb{F}}_p$, 则由 *12.3 c*可知

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

进一步地, 存在 $m \in N^*$, 使得 $\mathbb{F}_{p^3} \subset \mathbb{F}_{p^{2^m}}$. 而这显然与 a 矛盾. 故 $K \subsetneq \bar{\mathbb{F}}_p$. ♢

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.

♣ 如果这样的 L 存在, 则 $L \subset \bar{\mathbb{F}}_p^H$. 由*12.2*的结果可知 $L \subset \mathbb{F}_p$, 而 $\mathbb{F}_p$ 的阶数为 p, 没有真子域, 从而 $L = \mathbb{F}_p$. 由此得出 $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) = H$ 为循环群. 考虑 $\bar{F}_p/K$ 为 Galois 扩张. 由上一问知它是非平凡的, 其 Galois 群是 H 的非平凡子群 (任取 $\bar{F}_p \backslash K$ 中元素, 将其映到 $\bar{F}_p$ 中在 K 上的共轭根并扩张为 $\bar{F}_p$ 上即给出非平凡自同构). 但另一方面, 若 Fr^m 固定 K 中的元素, 知 Fr 固定所有的 $\mathbb{F}_{p^{2^n}}$, 于是由*12.1*知应有 $2^n|m$, 由 n 的任意性给出 $m = 0$, 与非平凡子群矛盾. ♢

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.

♣ 不妨假定 L_1/K 代数, 由于 L/L_1 代数, 给出 L/K 代数. 而 $K\subseteq L_1\cap L_2\subseteq L$, 于是 $L/L_1\cap L_2$ 代数. ♢

13.2 若上一问没有前面的假设, 结论是否还正确?

♣ 不正确. 考虑 $L=\mathbb{C}(x)$, 令 $L_1=\mathbb{C}(x^2)$, $L_2=\mathbb{C}(x^2+x)$. 现计算 $L_1\cap L_2$, 若有有理分式 $p(t),q(t)\in\mathbb{C}(t)$ 使得 $p(x^2)=q(x^2+x)=f(x)\in L_1\cap L_2$, 不妨假定 $f(x)=\dfrac{g(x)}{h(x)}$, $g,h\in\mathbb{C}[x]$ 为互素的多项式, 由 $x^2=(-x)^2$ 和 $x^2+x=(-1-x)^2+(-1-x)$, 我们得到若 z 为 g(或 h) 的零点, 则 $-z$ 和 $-1-z$ 也是 g(或 h) 的零点, 于是给出 $z+1$ 是零点. 若 g 和 h 中有正次数多项式, 则存在零点, 但由上论述将会得到无穷多个零点, 矛盾. 故只能有 $f\in\mathbb{C}$, 这也就给出 $L_1\cap L_2=\mathbb{C}$. 而 $L/\mathbb{C}$ 不是代数的, 给出反例. ♢

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.

原注: 本题直接通过正规扩张的定义无法得到什么有效结论, 即知道 $\alpha\in L$ 在 L_1, L_2 和 $L_1\cap L_2$ 上的极小多项式分别为 f_1, f_2 和 g, 以及 f_1 和 f_2 在 L 中分裂, 通过这些条件很难直接给出 g 在 L 中分裂, 这是因为 g 的根未必是 f_1f_2 的根. 本题的结论仍然正确, 但老师在出题时可能错误估计了本题的难度 (主要难度来自课堂内容缺少有关结论), 导致其已经远超作为一道考试题的难度. 经过很多人的讨论我们找出了以下这个较优的证法, 证明来自北京师范大学 2019 级的吴相东.

♣(原来的解答) 为证本题, 我们需要若干定义和引理.

定义. 设 E/F 为域的代数扩张 (未必有限, 下同), 我们称 $a \in E$ 在 F 上是可分的, 是指扩张 $F(a)/F$ 为有限可分扩张; 称 E/F 可分是指 E 中的每个元素均在 F 上可分, 可仿照有限的情形验证复合扩张是可分等价于每一步扩张可分. 称 $a \in E$ 是扩张 E/F 的正规元, 是指 a 在 F 上的极小多项式在 E 中分裂; 称 E/F 正规是指 E 中每个元素都是正规元.

定义. 设 E/F 为代数扩张, 记 E^s 为 E 中所有在 F 上可分的元素构成的集合. 由于对任意 $a, b \in E^s$, $a+b, ab, a^{-1}$ 均在 $F(a,b)$ 中, 而 $F(a,b)/F$ 可分, 从而可知 E^s 为域, 且包含 F, 我们称扩张 E^s 为 F 在 E 中的可分闭包.

定义. 设 E/F 为特征 $p>0$ 的代数扩张, 我们称 $a \in E$ 在 F 上纯不可分, 是指存在 $n \in \mathbb{N}$ 使得 $a^{p^n} \in F$. 由 2022-06-01习题 7前的定义, 扩张 E/F 是纯不可分的即指每个元素均纯不可分, 容易验证复合扩张是纯不可分的当且仅当每一步都是纯不可分的. 记 E^i 为 E 中所有在 F 上纯不可分元素的集合, 在特征 p 下依定义容易验证这成为一个域, 我们称其为 F 在 E 中的纯不可分闭包.

引理 1. 设 E/F 为代数扩张, 且 $G = Aut(E/F)$ 为 Galois 群, 则 $E^G = F \Leftrightarrow$ 该扩张可分且正规. 此时称 E/F 为 Galois 扩张.

引理 2. ([3] Chapter V. §6, Prop 6.11) 令 E/F 为正规扩张, $G = Aut(E/F)$ 为扩张的自同构群 (即 Galois 群), 考虑 G 作用下的固定域 E^G, 则 E^G/F 为纯不可分扩张, 且 E/E^G 为可分扩张. 此时我们有 $E^i = E^G$ 以及 $E^s \cap E^G = F$.

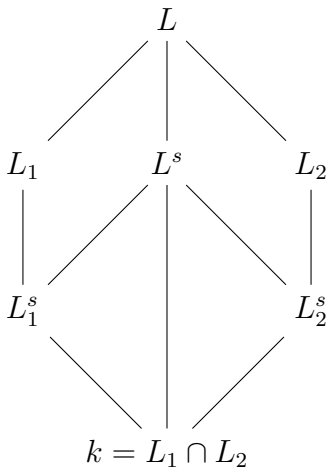
引理 3. 设 E/F 为代数扩张, 则 E/F 正规当且仅当 E^s/F 正规且 E/E^i 可分.

引理 4. (原问题可分的情形) 设 E/F 为可分扩张 (不假定有限), 且有两个子扩张 E_1/F 和 E_2/F, 若 E/E_1 和 E/E_2 均为正规扩张, 则 $E/E_1 \cap E_2$ 正规.

引理 5. 设 E/F 为代数扩张, 且有子扩张 E_1, E_2. 若 E/E_1 和 E/E_2 均是 Galois

扩张, 则 $E/E_1 \cap E_2$ 是 Galois 扩张.

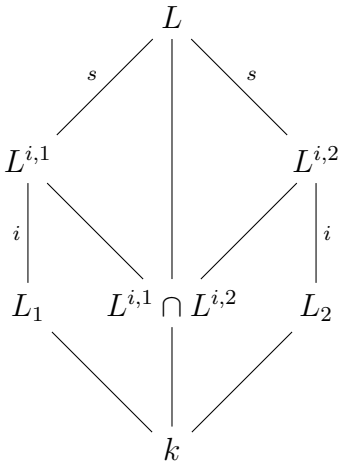
引理的证明我们留在末尾, 我们先证明原题. 特征 0 时所有代数扩张都可分, 故直接由引理 4即可证明, 以下只需讨论特征 $p > 0$ 的情形. 记 $L_1 \cap L_2 = k$, 令 L_1^s, L_2^s, L^s 为在各自域中 k 上的可分闭包, 则 $L_1^s = L_1 \cap L^s$, $L_2^s = L_2 \cap L^s$.



为使用引理 3, 我们需要分别证明 L^s/k 正规和 L/L^i 可分, 其中 L^i 是 k 在 L 中的纯不可分闭包.

在上图中, 考虑下边的正方形部分, 由于 $L_j^s \subseteq L_j$, 我们有 $k \subseteq L_1^s \cap L_2^s \subseteq L_1 \cap L_2 = k$, 给出 $k = L_1^s \cap L_2^s$. 此时下方正方形部分的所有扩张依定义均是可分的, 于是只需证 L^s/L_j^s 正规即可由引理 4 得到 L^s/k 正规. 设 $x \in L^s$, 由于 x 在 k 上可分, 进而在 L_1 上可分. 由 L/L_1 正规, x 在 L_1 上的共轭元均在 L 中, 且它们在 k 上有相同的极小多项式 (因为也在 k 上共轭), 故每个共轭元都在 k 上可分. 另一方面, x 在 L_1 上的极小多项式 f 的系数正是这些共轭元的多项式, 故也在 k 上可分, 进而这些系数落在 L_1^s 里. 于是, $f \in L_1^s[X]$, 且在 $L_1[X]$ 中不可约, 故在 L_1^s 中不可约, 这给出 f 也是 x 在 L_1^s 上的极小多项式, 从而 L^s/L_1^s 正规. 同理 L^s/L_2^s 正规, 于是 L^s/k 正规.

令 $L^{i,1}$, $L^{i,2}$ 分别为 L_1, L_2 在 L 中的纯不可分闭包, 有



由引理 3有 $L/L^{i,1}$ 和 $L/L^{i,2}$ 可分, 对任意 $x\in L$, 有 x 在 k 上纯不可分 $\Leftrightarrow \exists n\in\mathbb{N}$ 使得 $x^{p^n}\in k=L_1\cap L_2\Leftrightarrow \exists n\in\mathbb{N}$ 使得 $x^{p^n}\in L_j,\ j=1,2\Leftrightarrow x$ 在 L_j 上纯不可分, $j=1,2\Leftrightarrow x\in L^{i,1}\cap L^{i,2}$. 因此我们有 $L^i=L^{i,1}\cap L^{i,2}$. 而 $L/L^{i,1}$ 和 $L/L^{i,2}$ 也是正规的 (因为 L/L_j 正规), 故是 Galois 扩张. 由引理 5即可得到 L/L^i 可分, 从而完成证明. $\diamondsuit$

引理 1的证明

$\clubsuit$ $\Rightarrow$: 对 $x\in E$, 考虑 x 在 G 作用下的轨道为 $G(x)=\{x_1=x,\cdots,x_n\}$, 则 G 在 $G(x)$ 上有作用. 令 $f(X)=\prod\limits_{i=1}^{n}(X-x_i)$, 由于 G 置换 x_i, 给出 f 在 G 作用下不动, 从而有 $f\in E^G[X]=F[X]$, 于是给出 x 的一个零化多项式. 而任给零化多项式 h, G 作用不变将有 $G\cdot(X-x_1)$ 为 h 的因式, 进而 $f|h$, 这说明 f 为 x 的极小多项式, 此时依定义有 x 在 F 上可分且关于 E/F 正规, 故 E/F 可分且正规.

$\Leftarrow$: 考虑 $x\in E\backslash F$, 则 x 在 F 上有次数大于 1 的极小多项式 f. 由于扩张可分且正规, f 在 E 中有不同于 x 的根 y. 于是给出 F-同态 $F(x)\to\bar{F},\ x\mapsto y$, 其中 $\bar{F}$ 为一个包含 E 的代数闭包, 将其扩张到 E 上即得到 $E\to\bar{F}$. 可验证此时 E 的像仍在 E 中, 从而给出 E 的自同构, 即 G 中的元素, 于是 x 在 G 中某个元素作用下映到 $y\neq x$, 给出 $x\notin E^G$. 反之显然有 $F\subseteq E^G$, 故取等号. $\diamondsuit$

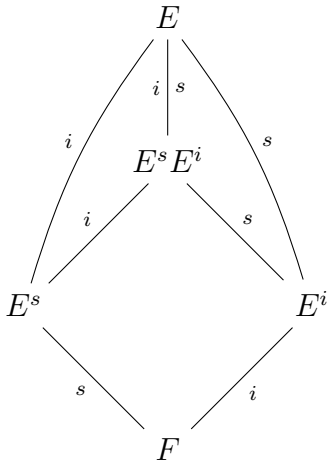
引理 2的证明

♣ 假设 $\alpha \in E^G$ 在 F 上有共轭根 β, 令 $\tau\colon F(\alpha) \to \bar{F},\ \alpha \mapsto \beta$, 并将其延拓到 E 上记为 τ'. 由于 E/F 正规, 故 $\tau'(E) \subseteq E$, 这说明 $\tau' \in G$, 于是 $\beta = \tau(\alpha) = \alpha \Rightarrow \alpha$ 的共轭根只有自己. 于是 α 在 F 上的极小多项式 f 形如 $(X-\alpha)^m$. 令 $m = p^n r$, 其中 $n \in \mathbb{N}$, r 与 p 互素, 则 $f(X) = (X^{p^n} - \alpha^{p^n})^r = X^{p^n r} - r\alpha^{p^n} X^{p^n(r-1)} + \cdots$, 其中省略的项次数不超过 $p^n(r-2)$. 由于 $f \in F[X]$, 有 $r\alpha^{p^n} \in F$, 而 r 是与 p 互素的整数, 故在 F 中非 0, 从而得到 $\alpha^{p^n} \in F$, 即 α 在 F 上纯不可分. 于是 $E^G \subseteq E^i$. 而容易发现有 $G = Aut(E/E^G)$, 从而由引理 1给的定义知 E/E^G 是 Galois 扩张, 进而是可分扩张. 依可分和纯不可分的定义容易验证 $E^s \cap E^i = F$. 此时有 $E^G \subseteq E^i$, 易知它是纯不可分扩张, 而 E^i/E^G 同时还是 E/E^G 的子扩张, 故是可分扩张, 这将推出 $E^i = E^G$. ♢

引理 3的证明

♣ ⇒:引理 2已经证明 E/E^i 可分. 对 E 中在 F 上可分的元素 x, 由于 E/F 正规, x 在 F 上的共轭根均在 E 中, 而可分元素的共轭元仍为可分元素, 故这些共轭根都在 E^s 里, 也就给出 E^s/F 正规.

⇐: 我们考虑以下扩张塔



由 2022-06-01 的习题 9.2可得 E/E^s 纯不可分 (证明没有用到 E/F 为有限扩张, 整个证明可以完全搬到无限扩张的情形). 从而上图中标注的可分及纯不可分都已得到验证, 注意到此时 E/E^sE^i 可分且纯不可分, 故只能有 $E = E^sE^i$. 此时 E^i/F 正规, 且由条件有 E^s/F 正规, 故有 E^iE^s/F 正规, 也即 E/F 正规. ♢

引理 4/引理 5的证明 (该引理可能是老师原本希望作为考试题的东西)

♣ 由于 E/F 可分, 此时涉及的子扩张均可分, 相应的由条件有 E/E_1 和 E/E_2 为 Galois 扩张, 故引理 4 仅是引理 5 的特殊情形, 我们直接证明引理 5. 记 $G_1 = \mathrm{Gal}(E/E_1)$, $G_2 = \mathrm{Gal}(E/E_2)$, $G = \mathrm{Gal}(E/E_1 \cap E_2)$, 此时 G_1 和 G_2 均可视为 G 的子群, 借助引理 1, 我们有 $x \in E^G \Rightarrow x \in E^{G_1}$ 且 $x \in E^{G_2} \Rightarrow x \in E^{G_1} \cap E^{G_2} = E_1 \cap E_2$, 从而 $E^G \subseteq E_1 \cap E_2$. 反向包含是显然的, 故 $E_1 \cap E_2 = E^G$, 从而 $E/E_1 \cap E_2$ 是 Galois 的. ♢

后注: 整本讲义整理完后, 许金兴老师在审稿期间提供了本题的一种简单证明. 这个证明来自 20 级中法班的刘🄵名同学. 首先不妨将原问题约化为以下问题:

设 $K \subset L_1$, $K \subset L_2$, $L_1 \subset L$, $L_2 \subset L$ 均为域的有限扩张，并且 $L_1 \cap L_2 = K$, 以及 $L_i \subset L$ 为正规扩张, $i = 1, 2$. 求证: $K \subset L$ 为正规扩张.

♣ 假设 $K \subset L$ 不是正规扩张, 则存在 $\alpha_1 \in L$, 其在 K 上的极小多项式 $P_1(x) \in K[x]$ 不能在 L 上分解为一次因子的乘积. 这样 $P_1(x)$ 在 $L[x]$ 中的分解具有形式 $P_1(x) = (x-\alpha_1)\cdots(x-\alpha_n)Q_1(x)\cdots Q_m(x)$, 其中 $\alpha_i \in L$, $\forall 1 \le i \le n$, Q_j 为 $L[x]$ 中次数大于 1 的不可约多项式, $\forall 1 \le j \le m$. 并且 $m \ge 1$. 令 $R_1(x) \in L_1[x]$ 为 α_1 在 L_1 上的极小多项式, 则 $R_1(x) | P_1(x)$. 由于 $L_1 \subset L$ 为正规扩张, $R_1(x)$ 在 $L[x]$ 中分解为一次因子的乘积, 从而 $P_2(x) := \frac{P_1(x)}{R_1(x)} \in L_1[x]$ 在 $L[x]$ 中有分解 $P_2(x) = T_2(x)Q_1(x)\cdots Q_m(x)$, 其中 $T_2(x)$ 为 $L[x]$ 中一些一次因子的乘积. 如果 $\deg T_2(x) > 0$, 我们可以继续取 $T_2(x)$

的一个根, 不妨设为 $\alpha_2 \in L$, 考虑 α_2 在 L_1 上的极小多项式 $R_2(x)$, 则 $R_2(x)|P_2(x)$. 令 $P_3(x) = \frac{P_2(x)}{R_2(x)} \in L_1[x]$, 则在 $L[x]$ 中有 $P_3(x) = T_3(x)Q_1(x)\cdots Q_m(x)$, 其中 $T_3(x)$ 为 $L[x]$ 中一些一次因子的乘积. 如果 $\deg T_3(x) > 0$, 则继续操作下去, 直到某个 $P_i(x) = Q_1(x)\cdots Q_m(x)$ 为止. 由于 $P_i(x) \in L_1[x]$, 从而得到 $Q_1(x)\cdots Q_m(x) \in L_1[x]$. 同样的推理得到 $Q_1(x)\cdots Q_m(x) \in L_2[x]$. 从而 $Q_1(x)\cdots Q_m(x) \in K[x]$. 这与 $P(x)$ 在 $K[x]$ 上不可约矛盾. ♢

可以看到, 这个证明要轻盈地多. 有趣的是, 这道试题是唯一一道在 19 级和 20 级的期末考试中都出现的习题, 但两届同学中没有任何一人在考场上给出正确解答. 比起上面那个辗转许久而得到的繁重解答, 这个证明实在让人眼前一亮.

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 ι_1, ι_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 σ 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 ι_1 给出有限扩张. 证明此时有 $L_1 = L_2$.

♣ 我们记 L_1 到 L_2 的自然含入为 $i\colon L_1 \to L_2$, 则条件即为 $\iota_2 \circ \sigma = i \circ \iota_1$, 结合题干条件, 我们得到 $i \circ \iota_1 = \tilde{\sigma} \circ \iota_1$, 这相当于说, 分别通过 ι_1 和 $i \circ \iota_1$ 将 L_1 和 L_2 视为 K_1-代数后, i 和 $\tilde{\sigma}$ 是 K_1-代数同态, 进而是 K_1-线性映射. 由于 $\iota_1\colon K_1 \to L_1$ 为有限扩张, 故 L_1 为有限维 K_1-线性空间, 而 $\tilde{\sigma}$ 为同构说明 L_2 与 L_1 有相同的维数, 故由 i 是有限维同维数线性空间之间的单射知 i 为双射, 即 $L_1 = L_2$. ♢

14.2 在上一问中去掉 ι_1 为有限扩张的条件, 此时结论是否仍正确?

♣ 不正确. 考虑 $K_1 = K_2 = k$, $k(x^2) =: L_1 \subseteq L_2 := k(x)$, 其中 x 为 k 上的超越元.

考虑 $\tilde{\sigma}\colon L_1 \to L_2,\ x^2 \mapsto x$ 给出同构, 且相应的限制 σ 即为 id_k, 此时自然满足题中条件, 但 $L_1 \neq L_2$. ♢

14.3 与前一问相反, 我们保留 ι_1 有限的条件, 但去掉 $\iota_2 \circ \sigma = \iota_1$, 此时结论是否仍正确?

♣ 不正确, 考虑 $K_1 = L_1 = k(x^2),\ K_2 = L_2 = k(x)$, 相应的 ι_1, ι_2 为恒等, $\sigma, \tilde{\sigma}$ 为 $k(x^2)$ 到 $k(x)$ 的同构, 此时给出的满足条件, 但 $L_1 \neq L_2$. ♢

注: 以上*3*的例子与*1*中不同之处在于, 此时的 $\tilde{\sigma}$ 并不是 K_1-代数同态.

参考文献

[1] M.F. Atiyah, *Introduction to commutative algebra*, ADDISON-WESLEY PUBLISHING COMPANY, 1994.

[2] Joseph J.Rotman, *Universitext an introduction to homological algebra*, Springer, 2000.

[3] Serge Lang, *Graduate texts in mathematics 211 algebra*, Springer, 2005.

[4] Benjamin Sambale, *An invitation to formal power series*, arXiv, 2023.

[5] Albrecht Fröhlich Martin Taylor, *Algebraic number theory*, Cambridge University Press, 1991.

[6] 冯克勤, 代数数论, 科学出版社, 2000.