

目录

1	Algebra Test	3
1.1	Algebra Q1	3
1.2	Algebra Q2	4
1.3	Algebra Q3	5
1.4	Algebra Q4	6
1.5	Algebra Q5	7
1.6	Algebra Q6	8
1.7	Algebra Q7	9
1.8	Algebra Q8	11
1.9	Algebra Q9	12
1.10	Algebra Q10	13
1.11	Algebra Q11	14
1.12	Algebra Q12	15
1.13	Algebra Q13	16
1.14	Algebra Q14	18
1.15	Algebra Q15	19
1.16	Algebra Q16	20
1.17	Algebra Q17	21
1.18	Algebra Q18	22
1.19	Algebra Q19	24

1.20 Algebra Q20	25
1.21 Algebra Q21	26
1.22 Algebra Q22	27
1.23 Algebra Q23	28
1.24 Algebra Q24	30
1.25 Algebra Q25	32
1.26 Algebra Q26	33
1.27 Algebra Q27	34
1.28 Algebra Q28	35
1.29 Algebra Q29	36
1.30 Algebra Q30	37
1.31 Algebra Q31	38
1.32 Algebra Q32	39
1.33 Algebra Q33	40
1.34 Algebra Q34	41
1.35 Algebra Q35	42
1.36 Algebra Q36	43
1.37 Algebra Q37	44
1.38 Algebra Q38	45
1.39 Algebra Q39	46
1.40 Algebra Q40	48
1.41 Algebra Q41	49
1.42 Algebra Q42	50
1.43 Algebra Q43	51
1.44 Algebra Q44	52
1.45 Algebra Q45	53
1.46 Algebra Q46	54
1.47 Algebra Q47	55
1.48 Algebra Q48	56

目录	3
1.49 Algebra Q49	58
1.50 Algebra Q51	59
1.51 Algebra Q52	61
1.52 Algebra Q53	63
2 Test Img 1	65
3 Test Img 2	67

Chapter 1

Algebra Test

1.1 Algebra Q1

Exercise

问题 1. 设 G 为对称群 S_n 的一个阿贝尔子群, p_1, \dots, p_k 为 $|G|$ 的所有素因数。证明 $p_1 + \dots + p_k \leq n$ 。

Solution

证明: 假设, 为了矛盾, $p_1 + \dots + p_k > n$ 。由于 p_i 是一个能整除 $|G|$ 的素数, 群 G 必须有一个元素的阶为 p_i 。因此, 对于每个 i , G 包含一个元素 σ_i , 其循环分解为 p_i 个循环的乘积。对于每个 j , 我们用 M_j 表示 $J_n = \{1, \dots, n\}$ 中不被 σ_j 固定的元素集。由于 G 是阿贝尔群, M_i 和 M_j 对于 $i \neq j$ 是不相交的。事实 $|M_j| \geq p_j$ 意味着

$$|J_n| \geq |M_1| + \dots + |M_k| \geq p_1 + \dots + p_k > n;$$

这与事实相矛盾。因此, $p_1 + \dots + p_k \leq n$ 。

1.2 Algebra Q2

Exercise

问题 1. 设 G 为对称群 S_n 的一个阿贝尔子群, p_1, \dots, p_k 为 $|G|$ 的所有素因数。证明 $p_1 + \dots + p_k \leq n$ 。

Solution

解决方案: 假设, 通过反证, $p_1 + \dots + p_k > n$ 。由于 p_i 是整除 $|G|$ 的素数, 群 G 必须有一个元素的阶为 p_i 。因此, 对于每个 i , G 包含一个元素 σ_i , 其循环类型分解是 p_i -循环的乘积。对于每个 j , 用 M_j 表示 $J_n = \{1, \dots, n\}$ 中不被 σ_j 固定元素的集合。由于 G 是阿贝尔群, M_i 和 M_j 对于 $i \neq j$ 是分离的。事实 $|M_j| \geq p_j$ 意味着

$$|J_n| \geq |M_1| + \dots + |M_k| \geq p_1 + \dots + p_k > n;$$

这是一个矛盾。因此, $p_1 + \dots + p_k \leq n$ 。

1.3 Algebra Q3

Exercise

设 G 为一个有限群，作用于一个有限集合 S 上。对于固定的 $x \in G$ ，定义 $f(x)$ 为集合 S 中元素 s 的数量，使得 $xs = s$ 。证明 G 在 S 上的轨道数量等于

$$\frac{1}{|G|} \sum_{x \in G} f(x).$$

Solution

考虑集合 $A = \{(x, s) \in G \times S : xs = s\}$ 。我们将 $s \in S$ 的轨道记为 C_s 。注意到 $|A| = \sum_{x \in G} f(x)$ 。另一方面，根据轨道-稳定子定理，

$$|A| = \sum_{s \in S} |\text{Stab}(s)| = \sum_{s \in S} \frac{|G|}{|C_s|} = |G| \sum_{s \in S} \frac{1}{|C_s|}.$$

由于 $\sum_{s \in S} \frac{1}{|C_s|}$ 等于轨道的数量，因此所需的公式得以证明。

1.4 Algebra Q4

Exercise

问题3. 如果同一种颜色的珍珠是无法区分的，那么可以设计出多少种由17颗黑白珍珠组成的项链？

Solution

解决方案：令 S 表示可以用黑白珠子设计的所有 17 颗珠子（带锁）的项链集合。由于 $|S| = 2^{17}$ 。二面体群 $G = D_{2n}$ 以明显的方式作用于 S 。由于我们感兴趣的是没有锁的项链，对于我们来说，两个项链相同当且仅当它们在 G 对 S 的作用下处于同一个轨道。因此，我们只需要计算 S 在此作用下的轨道数量。 G 的恒等式固定了 2^{17} 个项链；每个 16 个非平凡旋转固定了 2 个项链（这是因为 17 是质数）；每个 17 个反转固定了 2^9 个项链。因此，根据前一个问题中给出的计数轨道的公式，我们可以设计的项链数量为

$$\frac{1}{34}(2^{17} + 16 \cdot 2 + 17 \cdot 2^9) = \frac{2^{16} + 16}{17} \Theta$$

注意，由费马小定理，17 能整除 $2^{16} + 2^4 = (2^{16} - 1) + 17$ 。

1.5 Algebra Q5

Exercise

问题 4. 证明立方体的旋转对称群与 S_4 同构。

Solution

解决方案：设 G 为立方体 C 的旋转对称群， C 嵌入在 \mathbb{R}^3 空间中，且以原点为中心。固定一个面 f 。注意到 f 可以通过旋转对称映射到 C 的任意六个面。另外，它可以以四种不同的方式完成；注意每个面恰好有四个旋转对称。因此 24。

注意到 G 对主对角线集 D 进行了作用，即连接立方体两个顶点且经过原点的线段。由于 $|D| = 4$ ，该作用诱导了一个同态 $\phi : G \rightarrow S_4$ 。由于 $|G| = |S_4| = 24$ ，为了证明 ϕ 是一个同构，只需要检查它是单射的。由于没有旋转可以固定四条主对角线，因此该作用是忠实的。因此 ϕ 是单射的。因此 $G \cong S_4$ 。

1.6 Algebra Q6

Exercise

问题 5. 分类阶为 20 的群。

Solution

解答：令 G 为阶为 20 的群。如果 G 是阿贝尔群，则根据有限生成阿贝尔群的基本定理， G 必须与 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$ 或 $\mathbb{Z}_4 \times \mathbb{Z}_5$ 同构。

令 G 为非阿贝尔群，阶为 20。令 n_5 为 G 的 5-西洛群的数量。根据西洛定理， $n_5 = 1$ 。由于存在唯一一个阶为 5 的子群 N ， N 必定是正常的。令 H 为 2-西洛群。则 G 是 N 和 H 的半直接积，即 $G \cong N \rtimes_{\phi} H$ ，其中 $\phi : H \rightarrow \text{Aut}(N)$ 。

首先假设 H 与循环群 \mathbb{Z}_4 同构。如果 ϕ 是非平凡的同态，则它将 \mathbb{Z}_4 的生成元映射到 \mathbb{Z}_4 的唯一阶为 2 的元素或两个阶为 4 的元素之一。将生成元映射到每个阶为 4 的元素得到同构的非阿贝尔群。令 ϕ_1 和 ϕ_2 分别为当 \mathbb{Z}_4 的生成元映射到阶为 2 的元素或阶为 4 的元素时得到的同态。由于 $|\ker \phi_1| = 2$ 且 $|\ker \phi_2| = 1$ ，群 $\mathbb{Z}_5 \rtimes_{\phi_1} \mathbb{Z}_4$ 和 $\mathbb{Z}_5 \rtimes_{\phi_2} \mathbb{Z}_4$ 不同构。

现在假设 H 与克莱因群 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 同构。存在三个非平凡的同态 $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_5)$ 。它们由将 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 的两个非零元素发送到 \mathbb{Z}_4 中的唯一阶为 2 的元素，并将其他两个元素发送到单位元给出。由克莱因群的对称性，诱导的半直接积是同构的非阿贝尔群。然后 $\mathbb{Z}_5 \rtimes_{\phi} (\mathbb{Z}_2 \times \mathbb{Z}_2)$ ，其中 ϕ 是上面提到的两个同态中的任意一个。该段落中找到的群与前一段落中找到的群不同构，因为 $\mathbb{Z}_5 \rtimes_{\phi_1} \mathbb{Z}_4$ 和 $\mathbb{Z}_5 \rtimes_{\phi_2} \mathbb{Z}_4$ 没有阶为 4 的元素。阶为 4 的元素的缺失迫使 $\mathbb{Z}_5 \rtimes_{\phi} (\mathbb{Z}_2 \times \mathbb{Z}_2)$ 与 D_{20} 同构。

1.7 Algebra Q7

Exercise

问题6. (I.52) (a) 证明在阿贝尔群的范畴中存在推出 (即纤维积)。在这种情况下, 两个同态 $f: Y \rightarrow X$ 和 $g: Z \rightarrow X$ 的纤维积记为 $X \oplus Y$ 。证明它是因子群 $X \oplus Y = (X \oplus Y)/W$, 其中 W 是由所有元素 $(f(z), -g(z))$ 组成的子群, 其中 $z \in Z$ 。(b) 证明单射同态的推出是单射。

Solution

解决方案: 设 $f: Z \rightarrow X$ 和 $g: Z \rightarrow Y$ 为群同态。由于 X 和 Y 是阿贝尔群, 因此 $X \oplus Y$ 也是阿贝尔群。定义 $h: Z \rightarrow X \oplus Y$ 为 $h(z) = (f(z), -g(z))$ 。 $W = \text{Im}(h)$ 是 $X \oplus Y$ 的子群。我们定义 $X \oplus_Z Y = (X \oplus Y)/W$ 。设 $\pi_1: X \oplus Y \rightarrow X \oplus_Z Y$ 和 $\pi_2: X \oplus Y \rightarrow X \oplus_Z Y$ 为标准投影。我们需要找到同态 $\phi_1: X \rightarrow X \oplus_Z Y$ 和 $\phi_2: Y \rightarrow X \oplus_Z Y$, 使得 $\phi_1 \circ f = \phi_2 \circ g$ 。定义 $\phi_1(x) = (x, 0) + W$ 和 $\phi_2(y) = (0, y) + W$ 。然后 $\phi_1 \circ f(z) = (f(z), 0) + W$ 和 $\phi_2 \circ g(z) = (0, g(z)) + W$ 。我们需要证明 $(f(z), 0) + W = (0, g(z)) + W$, 这意味着 $(f(z), -g(z)) \in W$ 。这是 W 的定义。因此, 图表是可交换的。现在我们需要证明, 对于任何阿贝尔群 A 和同态 $\alpha_1: X \rightarrow A$ 和 $\alpha_2: Y \rightarrow A$, 使得 $\alpha_1 \circ f = \alpha_2 \circ g$, 存在唯一的同态 $\psi: X \oplus_Z Y \rightarrow A$, 使得 $\psi \circ \phi_1 = \alpha_1$ 和 $\psi \circ \phi_2 = \alpha_2$ 。定义 $\psi((x, y) + W) = \alpha_1(x) + \alpha_2(y)$ 。首先, 我们需要证明 ψ 是良定义的。如果 $(x, y) + W = (x', y') + W$, 则 $(x - x', y - y') \in W$ 。因此 $(x - x', y - y') = (f(z), -g(z))$, 其中 $z \in Z$ 。因此 $x - x' = f(z)$ 且 $y - y' = -g(z)$ 。然后 $\alpha_1(x) + \alpha_2(y) - (\alpha_1(x') + \alpha_2(y')) = \alpha_1(x - x') + \alpha_2(y - y') = \alpha_1(f(z)) + \alpha_2(-g(z)) = \alpha_1(f(z)) - \alpha_2(g(z))$ 。由于 $\alpha_1 \circ f = \alpha_2 \circ g$, 我们有 $\alpha_1(f(z)) - \alpha_2(g(z)) = 0$ 。因此, ψ 是良定义的。很容易检查出 ψ 是同态。另外, $\psi \circ \phi_1(x) = \psi((x, 0) + W) = \alpha_1(x) + \alpha_2(0) = \alpha_1(x)$ 和 $\psi \circ \phi_2(y) = \psi((0, y) + W) = \alpha_1(0) + \alpha_2(y) = \alpha_2(y)$ 。对于唯一性, 假设存在另一个同态 ψ' 满足条件。然后 $\psi'((x, y) + W) = \psi'((x, 0) + W + (0, y) + W) =$

$\psi'((x, 0) + W) + \psi'((0, y) + W) = \psi'(\phi_1(x)) + \psi'(\phi_2(y)) = \alpha_1(x) + \alpha_2(y) = \psi'((x, y) + W)$ 。因此, ψ 是唯一的。因此, 阿贝尔群范畴中存在推出。(b) 证明推出一个单射同态是单射。假设 $f : Z \rightarrow X$ 是单射。我们需要证明 $\phi_2 : Y \rightarrow X \oplus_Z Y$ 是单射。假设 $\phi_2(y) = 0$, 其中 $y \in Y$ 。则 $(0, y) + W = W$, 这意味着 $(0, y) \in W$ 。因此 $(0, y) = (f(z), -g(z))$, 其中 $z \in Z$ 。这意味着 $f(z) = 0$ 且 $y = -g(z)$ 。由于 f 是单射, $f(z) = 0$ 意味着 $z = 0$ 。然后 $y = -g(0) = 0$ 。因此, ϕ_2 是单射。

1.8 Algebra Q8

Exercise

问题 7. (Lang III.16) 证明一个简单群系统的逆极限，其中同态是满射的，或者是平凡群，或者是简单群。

Solution

解：设 (G_i, f_i) 为一个简单群系统，其中对于每对 $j > i$ ，同态 f_i^j 是满射。由于每个 G_i 都是简单的，每个 f_i^j 要么是平凡的，要么是同构。假设 G_i 和 G_j 都是非平凡的。取 k 使得 $k \geq i$ 且 $k \geq j$ 。由于 f_i^k 和 f_j^k 都是同构，因此 $G_i \cong G_k \cong G_j$ 。因此，系统中的所有非平凡群都是同构的。设 (G, f_i) 为 (G_i, f_i) 的逆极限。由于 G 是 $\prod G_j$ 的子群，而 $f_i : G \rightarrow G_i$ 是投影 $\pi_i : \prod G_j \rightarrow G_i$ 到 G 的限制，如果所有 i 都有 G_i 平凡，则 G 也平凡。因此，假设存在 i 使得 G_i 非平凡。在这种情况下，我们将证明 $G \cong G_i$ 。没有损失一般性地假设所有 j 都有 G_j 非平凡（即 $G_j \cong G_i$ 对所有 j ）。我们证明 f_i 是同构。首先，让我们检查 f_i 是否是满射。取 $g_i \in G_i$ 。对于任何索引 j ，存在 k 使得 $k \geq j$ 且 $k \geq i$ 。然后我们取 $g_j = f_j^k(g_k)$ ，其中 g_k 是 G_k 中唯一的元素，使得 $f_i^k(g_k) = g_i$ 。如果 k' 也满足 $k' \geq j$ 且 $k' \geq i$ ，则取 m 使得 $m \geq k$ 且 $m \geq k'$ 。由于 $f_i^k(g_k) = g_i = f_i^{k'}(g_{k'})$ ， g_k 和 $g_{k'}$ 必须提升到 G_m 中相同的元素 g_m 。因此， $f_j^k(g_k) = f_j^m(g_m) = f_j^{k'}(g_{k'})$ ，这意味着 g_j 不依赖于所选的 k 。因此，对于 $p \geq q$ ， $f_q^p(g_p) = g_q$ 。因此， (g_j) 实际上是 G 中的元素，满足 $f_i((g_j)) = g_i$ 。因此， f_i 是满射。现在我们证明 f_i 是单射。假设 (g_j) 在 f_i 的核中。则 $g_i = 1$ 。对于任何 j ，存在 k 使得 $k \geq i$ 且 $k \geq j$ 。由于 $f_i^k(g_k) = g_i = 1$ ， $g_k = 1$ 。因此， $g_j = f_j^k(g_k) = 1$ 。然后 (g_j) 是 G 的单位元，这证明了 f_i 是单射。因此， $G \cong G_i$ 是简单的。

1.9 Algebra Q9

Exercise

问题 8. (Lang IV.5) 分析以下情况下的不可约性: (a) 多项式 $x^6 + x^3 + 1$ 在有理数域上是否不可约。 (b) 多项式 $x^2 + y^2 - 1$ 在复数域上是否不可约。 (c) 多项式 $x^4 + 2011x^2 + 2012x + 2013$ 在有理数域上是否不可约。

Solution

解决方案:

(a) 设 $p(x) = x^6 + x^3 + 1$ 。注意, 多项式 $p(x)$ 可约当且仅当 $q(x) = p(x+1)$ 可约。多项式 $q(x) = (x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$ 的所有系数 (除 x^6 外) 都在素数 3 中。由于 $q(x)$ 的常数系数为 3, 且理想 (3) 是 $q(x)$ 的 Eisenstein 准则, $q(x)$ 在 \mathbb{Z} 上不可约。根据高斯引理, $q(x)$ 在 \mathbb{Q} 上也不可约。因此, 多项式 $x^6 + x^3 + 1$ 在有理数上不可约。

(b) 考虑多项式 $p(x, y) = x^2 + y^2 - 1$ 在 \mathbb{C} 上。 $p(x, y)$ 是一个变量 y 的多项式, 其系数在 $\mathbb{C}[x]$ 中。多项式 $p(x, y)$ 是单项式, 其非首项系数在 $\mathbb{C}[x]$ 的素理想 $(x-1)$ 中。由于常数系数 $x^2 - 1$ 不是 $(x-1)^2$ 的元素, 根据 Eisenstein 准则, $q(x, y)$ 在 $\mathbb{C}[x][y]$ 中作为变量 y 的多项式不可约, 其系数在 $\mathbb{C}[x]$ 中。因此, $p(x, y)$ 作为两个变量的多项式不可约。

(c) 设 $p(x) = x^4 + 2011x^2 + 2012x + 2013$ 。根据高斯引理, 只需检查 $p(x)$ 在 \mathbb{Z} 上不可约即可。另外, 注意到如果 $r(x)$ 在 \mathbb{Z} 上可约, 则 $r(x)$ 在 \mathbb{Z}_2 上也可约, 其中 $\mathbb{Z}_2[x]$ 是将 $r(x)$ 的系数模 2 减少后的结果。由于 $r(x) = x^4 + x^2 + 1$ 。由于 $r(x)$ 在 \mathbb{Z}_2 中没有根, 因此如果它在 $\mathbb{Z}_2[x]$ 中分解, 它将是两个不可约多项式的乘积, 每个多项式的次数为 2。但是, 在 $\mathbb{Z}_2[x]$ 中, 只有一个不可约多项式的次数为 2, 即 $x^2 + x + 1$ 。由于 $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq r(x)$, $r(x)$ 必定在 \mathbb{Z}_2 上不可约。因此, $r(x)$ 在有理数上不可约。

1.10 Algebra Q10

Exercise

问题 9. (Lang II.6) 设 A 为一个有因式分解的环, p 为一个素元。证明局部环 $A(p)$ 是主理想环。

Solution

解: 设 I 为 $A(p)$ 的一个合适理想, 且 $M = \{\frac{a}{b} : a \in I \text{ 和 } b \notin (p)\}$ 为 A 中的理想。由于 A 是一个有 1 的交换环, 任何理想都包含在一个极大理想中; 特别地, $I \subset M$ 。由于 $M = (1)$, I 中的任何元素都可以写成 $\frac{m}{k}$ 的形式, 其中 $m \in (p)$ 且 $k \notin (p)$ (注意 $\frac{m}{k}$ 是一个单位)。设 n_0 为最小的正整数, 使得 $\frac{p^{n_0}}{k} \in I$ 。我们将证明 $I = \frac{p^{n_0}}{k} A(p)$ 。由于 I 是一个理想, $\frac{p^{n_0}}{k} \in I$ 。为了证明逆包含, 取 $\frac{mp^k}{b^l} \in I$ 。由 n_0 的最小性, $k \geq n_0$, 因此

$$\frac{mp^k}{b^l} = \frac{mp^{k-n_0}}{b^l} p^{n_0} \in \left(\frac{p^{n_0}}{1} \right) \Theta$$

因此, $A(p)$ 的每个理想都是主理想。

1.11 Algebra Q11

Exercise

设 F 为一个域。证明 $F[[x]]$ 是一个唯一分解整环。

Solution

设 $R = F[[x]]$ 。我们将证明 R 是一个主理想环，这实际上是一个更强的陈述。设 $a = \sum a_n x^n$ 为 R 的一个元素。存在 $b = \sum b_n x^n$ 使得 $ab = ba = 1$ 当且仅当 $a_0 \neq 0$ 。为了证明这一点，我们取 $b_0 = a_0^{-1}$ ，一旦我们在 F 中选择了 b_0, \dots, b_{n-1} ，我们就取 $b_n \in F$ ，使得 $a_0 b_n + \dots + a_n b_0 = 0$ 。因此， $a_0 \neq 0$ 意味着 a 是一个单位。因此， $M = (x)$ 是 R 的唯一极大理想。由于 R 是一个交换环，且有单位元 1，每个理想都必须包含在一个极大理想中。这意味着 R 的每个非零理想都可以表示为 (x^i) 的形式，其中 $i \geq 0$ 。因此， R 是一个主环（PID），因此也是一个因数分解环（UFD）。

1.12 Algebra Q12

Exercise

问题 11. 设 F 为一个域。证明 Laurent 多项式环是主理想环。

Solution

设 $R = F[x, 1/x]$ 为 Laurent 多项式环。对于 $f(x) = \sum_{i=-k}^n a_i x^i \in R$, 其中 $a_{-k} \neq 0$, 我们定义 $\text{indeg}(f)$ 为 k , 如果 $k > 0$, 则为零。现在假设 I 是 R 的一个理想。考虑由集合 $S = \{x^{\text{indeg}(r)} r(x) : r(x) \in I\}$ 生成的理想 \bar{I} 。由于 \bar{I} 是 $F[x]$ 的一个理想, 而 $F[x]$ 是一个主理想环 (PID), 因此 $\bar{I} = (g(x))$ 。我们证明 $I = (g(x))$, 其中 $(g(x))$ 被认为是 R 的一个理想。取 I 中任意元素 $a(x) \in I$ 。则有 $x^{\text{indeg}(a)} a(x) \in \bar{I}$, 因此存在 $b(x) \in R$, 使得 $a(x) = x^{-\text{indeg}(a)} b(x) g(x) \in (g(x))$ 。另一方面, S 的每个元素都属于 I ; 这是因为 I 是一个理想。因此 $(g(x)) = (S) \subset I$ 。因此, $I = (g(x))$ 是主理想, 这意味着 R 是一个主理想环。

1.13 Algebra Q13

Exercise

问题 12. (Lang III.17) 设 n 为正整数, p 为素数。证明阿贝尔群 $A_n \approx \mathbb{Z}/p^n\mathbb{Z}$ 在规范同态 $f_{n,m} : A_m \rightarrow A_n$ 下形成逆系统, 其中 $n \leq m$, 具体来说, $f_{n,m}(x) = x \pmod{p^n}$ 。设 $A = \varprojlim A_n$ 为逆极限。证明 \mathbb{Z}_p 映射到每个 $\mathbb{Z}/p^n\mathbb{Z}$ 上是满射的, \mathbb{Z}_p 没有零除数, 并且有一个由 p 生成的唯一的极大理想。证明 \mathbb{Z}_p 是有素数分解的, 且只有一个素数, 即 p 本身。

Solution

解: 自然数集是有序索引系统的一个特例。如果 $n \geq m$, 则 $p^n\mathbb{Z} \subseteq p^m\mathbb{Z}$, 因此 $q_n : \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^m\mathbb{Z}$ 由 $a + p^n\mathbb{Z} \mapsto a + p^m\mathbb{Z}$ 给出, 其中 $a \in \mathbb{Z}$ 是一个良定义的满射同态。另外, 如果 $n \geq m \geq k$,

$$q_m^n(q_k^m(a + p^k\mathbb{Z})) = q_m^n(a + p^m\mathbb{Z}) = a + p^n\mathbb{Z} = q_k^n(a + p^k\mathbb{Z}).$$

因此 (A_n, q_m^n) 是一个逆系统。用 f_{ij} 表示从 \mathbb{Z}_p 到 A_j 的同态。固定索引 i 并取 $a_i \in A_i$ 。递归定义 a_{i+j} , 使得 $q_{i+j}^{i+j+1}(a_{i+j+1}) = a_{i+j}$, 从 $j = 1$ 开始。另外, 对于 $i \geq j$, 定义 $q_j(a_j)$ 。由此可知, 对于任何 $i \geq j$, $q_j(a_i) = a_j$, 这意味着 $(a_j) \in \varprojlim \mathbb{Z}/p^j\mathbb{Z}$ 。由于 $f_j((a_i)) = a_j$, f_j 是满射。为了检查 A_p 是否不包含任何零除数, 取 $(a_i + p^i\mathbb{Z})$ 和 $(b_i + p^i\mathbb{Z})$ 在 \mathbb{Z}_p 中, 其乘积为零。假设存在 r, s , 使得 p^r 不整除 a_r 且 p^s 不整除 b_s 。因此, p 不整除 a_r 且 p 不整除 b_s 。然后 p^{r+s} 不整除 a_rb_s , 这意味着 $a_rb_s + p^{r+s}\mathbb{Z}$ 非零。但是, 这与乘积 $(a_i + p^i\mathbb{Z})$ 和 $(b_i + p^i\mathbb{Z})$ 为零相矛盾。因此, $(a_i + p^i\mathbb{Z})$ 或 $(b_i + p^i\mathbb{Z})$ 必须为零。因此, \mathbb{Z}_p 没有零除数。为了证明理想 M 由 p 生成是 \mathbb{Z}_p 的唯一最大理想, 取 \mathbb{Z}_p 中不在 M 中的元素 $(a_i + p^i\mathbb{Z})$ 。然后 p 不整除 a_i , 这意味着 $(a_i, p^i) = 1$ 。对于每个 i , 取 b_i , 使得 $a_ib_i = 1 \pmod{p^i}$ 。由于 p^i 整除 $a_ib_i - 1$ 和 p^i , 且 p^i 整除 p^i , 因此 p^i 整除 $a_ib_i - 1$ 。因此, p^i 整除 $b_i - b_j$, 这意味着 $q_j^i(b_i + p^i\mathbb{Z}) = b_j + p^j\mathbb{Z}$ 。因此, $(b_i + p^i\mathbb{Z})$ 是 $(a_i + p^i\mathbb{Z})$ 在

\mathbb{Z}_p 中的逆元。由于 M 之外的任何元素都是单位, M 是 \mathbb{Z}_p 的唯一最大理想。因此, \mathbb{Z}_p 是一个局部环。由于 \mathbb{Z}_p 是一个交换环, 任何理想都包含在一个最大理想中。另一方面, M 是 \mathbb{Z}_p 的唯一最大理想, 因此任何理想都包含在 M 中。这意味着 \mathbb{Z}_p 的每个理想都是主理想。因此, \mathbb{Z}_p 是一个主理想环 (PID)。特别地, \mathbb{Z}_p 是一个因式分解环 (UFD)。由于 M 是一个素理想, p 是 \mathbb{Z}_p 中的素数。假设 q 是一个素数。那么理想 (q) 包含在 M 中。因此, $q = up^k$, 其中 u 是一个单位。由于 q 是不可约的, $k = 1$, 这意味着 q 与 p 关联。因此,

1.14 Algebra Q14

Exercise

问题 13. 设 ω 为 $x^2 - x + 1$ 的一个根。证明 $\mathbb{Z}[\omega]$ 是欧几里得整环。

Solution

解：设 $R = \mathbb{Z}[\omega]$ 。由于 $x^2 - 1 = (x - 1)(x^2 + x + 1)$ ，因此 ω 是一个六次方根，事实上是一个原始的六次方根。我们可以假设没有失去普遍性， ω 是主要的六次方根。因此， \mathbb{Z} 由以下线的交点组成：

(i) 与实轴平行的线，交于虚轴于 $ib\sqrt{3}$ ，其中 $b \in \mathbb{Z}$ ； (ii) 斜率为 $\sqrt{3}$ 的线，交于虚轴于 $ib\sqrt{3}$ ，其中 $b \in \mathbb{Z}$ ； (iii) 斜率为 $-\sqrt{3}$ 的线，交于虚轴于 $ib\sqrt{3}$ ，其中 $b \in \mathbb{Z}$ 。

因此， R 的点在 \mathbb{C} 中形成一个由等边单极三角形组成的网格。这意味着对于任何 $x \in \mathbb{C}$ ，都存在 $q \in R$ 使得 $|x - q| \leq 1$ 。因此，对于 $a, b \in R$ 且 $b \neq 0$ ，存在 $q \in R$ 使得 $|a/b - q| \leq \frac{1}{2}$ 。设 $r = a - qb$ ，则有

$$|r| = |a - qb| = |a/b - q||b| \leq \frac{\sqrt{3}}{2}|b| < |b|.$$

因此 $a = qb + r$ ，其中 $|r| < |b|$ 。因此， R 是一个欧几里得域。

1.15 Algebra Q15

Exercise

问题 14. 设 R 为半单环, $L \subset R$ 为左理想。证明存在幂等元 e 使得 $L = Re$ 。

Solution

解: 将 L 视为 R 的左 R 子模。由于 R 作为自身的模块是半单的, 所以存在 R 的左 R 子模 L' , 使得 $R = L \oplus L'$ 。取 L 中的 e 和 L' 中的 e' , 使得 $1 = e + e'$ 。那么我们有

$$e + 0 = e = e(e + e') = e^2 + ee'.$$

1.16 Algebra Q16

Exercise

问题 15. 确定所有半单环的同构类，且这些环的阶为 1008。其中有多少个是可交换的？

Solution

解答：设 R 为半单环，且 $|R| = 1008 = 2^4 \cdot 3^2 \cdot 7$ 。由于 R 为有限环，因此它是阿廷环。因此，根据阿廷-韦德伯恩定理， R 是有限多个 $n_i \times n_i$ 矩阵环的乘积，其中这些矩阵的元素来自除环 R_i 。由于 R 为有限环，因此对于每个索引 i ， R_i 也为有限环。因此，每个 R_i 都是域。特征为 2 的域上的矩阵环的可能乘积为 $M_2(\mathbb{F}_2)$ 、 \mathbb{F}_{16} 、 $\mathbb{F}_4 \times \mathbb{F}_4$ 、 $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$ 和 $\mathbb{F}_2 \times \mathbb{F}_8 \times \mathbb{F}_2$ 。使用特征为 3 的域代替特征为 2 的域，矩阵环的可能乘积为 \mathbb{F}_9 和 $\mathbb{F}_3 \times \mathbb{F}_3$ 。在特征为 7 的情况下，只有一个这样的乘积，即 \mathbb{F}_7 。将我们之前获得的乘积组合起来，我们可以得到 1008 阶半单环的每个同构类的代表。共有 10 个同构类。只有包含一个 $n \times n$ 矩阵环作为因子且 $n > 1$ 的代表不是可交换的。因此，同构的半单环中有 8 个是可交换的。

1.17 Algebra Q17

Exercise

问题16. 设 P 为任意环 R 上的一个循环投射模块。证明存在 R 的某个幂等元 e 使得 $P \approx Re$ 。

Solution

解决方案: 很容易检查 g_x 是一个 R -模同态。还要注意 $\ker(g_x) = \text{Ann}(x)$ 。因此, 我们有以下短正合序列:

$$0 \rightarrow \text{Ann}(x) \rightarrow R \xrightarrow{g_x} Rx \rightarrow 0.$$

由于 Rx 是投射的, 所以存在一个同态 $f: Rx \rightarrow R$, 使得 $g_x \circ f = 1_{Rx}$ 。这意味着 $f(x)x = x$ 。定义 $e = f(x)$ 为 $f(x)$, 并观察到 $(e - 1)x = 0$ 。所以 $e - 1 \in \text{Ann}(x)$ 。对于 $e \in \text{Ann}(x)$, 使得 $e = e + e$, 我们有:

$$e = (e + a)e = e^2 + ae = e^2 + af(x) = e^2 + f(ax) = e^2 + f(0) = e^2.$$

因此 e 是一个幂等元。由于 $g_x \circ f = 1_{Rx}$, 映射 f 是单射的。因此 $Re \approx Rx$, 其中 Re 是 Rx 由 f 映射的像。

1.18 Algebra Q18

Exercise

问题 17. (Lang III.10) (a) 设 A 为一个有单位元的交换环。如果 \mathfrak{p} 是一个素理想，且 $S = A - \mathfrak{p}$ 是环 A 中 \mathfrak{p} 的补集，则 $S^{-1}M$ 表示为 $M_{\mathfrak{p}}$ 。证明模块 M 到所有局部化 $M_{\mathfrak{m}}$ 的直接积的自然映射

$$M \rightarrow \prod_{\mathfrak{m}} M_{\mathfrak{m}}$$

是单射的，其中 \mathfrak{m} 遍历所有的极大理想。

Solution (by LLM)

由LLM生成的解答可能不准确，请自行验证。

解答：

我们需要证明自然映射

$$M \rightarrow \prod_{\mathfrak{m}} M_{\mathfrak{m}}$$

是单射，其中 \mathfrak{m} 遍历所有极大理想。

设 M 是一个 A -模， \mathfrak{m} 是 A 的极大理想。对于每个 \mathfrak{m} ，我们有局部化 $M_{\mathfrak{m}} = S^{-1}M$ ，其中 $S = A - \mathfrak{m}$ 。自然映射 $M \rightarrow M_{\mathfrak{m}}$ 由 $m \mapsto \frac{m}{1}$ 给出。

考虑自然映射

$$\phi : M \rightarrow \prod_{\mathfrak{m}} M_{\mathfrak{m}}, \quad \phi(m) = \left(\frac{m}{1} \right)_{\mathfrak{m}}.$$

我们需要证明 ϕ 是单射，即如果 $\phi(m) = 0$ ，则 $m = 0$ 。

假设 $\phi(m) = 0$ ，即对于所有极大理想 \mathfrak{m} ， $\frac{m}{1} = 0$ 在 $M_{\mathfrak{m}}$ 中。这意味着对于每个 \mathfrak{m} ，存在 $s_{\mathfrak{m}} \in S = A - \mathfrak{m}$ ，使得 $s_{\mathfrak{m}}m = 0$ 。

考虑理想 $I = \{a \in A \mid am = 0\}$ 。由于 $s_{\mathfrak{m}} \in I$ 且 $s_{\mathfrak{m}} \notin \mathfrak{m}$, I 不在任何极大理想 \mathfrak{m} 中。因此, I 必须是整个环 A , 即 $1 \in I$ 。这意味着 $1 \cdot m = 0$, 即 $m = 0$ 。

因此, ϕ 是单射。

1.19 Algebra Q19

Exercise

问题18. 找出满足以下条件的模块M。 1. M既是投射模块，也是注射模块。 2. M是投射模块，但M不是注射模块。 3. M是注射模块，但M不是投射模块。 4. M既不是投射模块，也不是注射模块。

Solution

解决方案： 1. 设 F 为一个域。令 M 为 F 模块 F 。由于 M 是一个自由的 F 模块，因此它是投射的。另一方面， M 是可除的，因此由于 F 是一个 PID， M 是可注射的。 2. 令 M 为 \mathbb{Z} 模块 \mathbb{Z} 。由于 M 是自由的，因此它是投射的。另一方面， M 不是可注射的：这是因为 \mathbb{Z} 是一个 PID 且 M 不是 \mathbb{Z} 模块的可除模块。 3. 令 M 为 \mathbb{Z} 模块 \mathbb{Q} 。由于 \mathbb{Q} 是一个可除的阿贝尔群，因此它是一个可注射的 \mathbb{Z} 模块。让我们证明 \mathbb{Q} 不是投射的。假设，通过矛盾， \mathbb{Q} 是投射的。那么它是自由 \mathbb{Z} 模块的直接和。令 B 为 F 的基数，令 $i : \mathbb{Q} \rightarrow F$ 为包含映射。存在 $n \in \mathbb{N}$, $b_1, \dots, b_n \in B$, 和 $z_1, \dots, z_n \in \mathbb{Z}$, 使得 $i(1) = \sum_{i=1}^n z_i b_i$ 。由于 $i(1) = mi(1)/m$ 对于每个 $m \in \mathbb{N}$ 和 $i(1) = \sum_{i=1}^n z_i b_i$, 我们推断出 m 必须除以 z_i 对于每个 $i = 1, \dots, n$ 。因此，对于每个 $i = 1, \dots, n$, $z_i = 0$, 因此 $i(1) = 0$ 。现在，如果 $f : F \rightarrow \mathbb{Q}$ 是投射映射，我们有 $1 = f(i(1)) = f(0) = 0$, 这是一个矛盾。因此， \mathbb{Q} 不是投射的。 4. 令 M 为 $\mathbb{Z}/2\mathbb{Z}$ 模块 $\mathbb{Z}/2\mathbb{Z}$ 。考虑 $\mathbb{Z}/4\mathbb{Z}$ 模块的序列

$$0 \rightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\text{mult by } 2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\text{mod } 2} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

很容易检查上述序列实际上是一个短正合序列。然而，它不分裂，因为 $\mathbb{Z}/4\mathbb{Z}$ 不同构于 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 。因此， M 既不是投射的，也不是可注射的。

1.20 Algebra Q20

Exercise

问题19. 证明局部环上的有限生成的投射模块是自由模块。

Solution

解: 设 R 为局部环, M 为有限生成的射影 R - 模块。取最小的 n , 使得 $M = Rm_1 + \cdots + Rm_n$, 其中 $m_i \in M$ 。由于 R^n 是自由的, 因此存在 R - 模同态 $\phi: R^n \rightarrow M$, 使得以下短正合序列成立:

$$0 \rightarrow K \rightarrow R^n \xrightarrow{\phi} M \rightarrow 0,$$

其中 K 是 ϕ 的核。由于 M 是射影的, 因此上述序列分裂, 因此 $M \oplus K \cong R^n$ 。设 \mathfrak{m} 为 R 的最大理想。将 $M \oplus K \cong R^n$ 张量化为 R/\mathfrak{m} , 我们发现 $(R/\mathfrak{m})^n \cong M/\mathfrak{m}M \oplus K/\mathfrak{m}M$ 是 R/\mathfrak{m} 上的向量空间。元素 m_1, \dots, m_n 生成 $M/\mathfrak{m}M$, 其中 $\overline{m_i} = m_i + \mathfrak{m}M$ 。假设现在 $r_i \in R$ 且 $r_i \in R/\mathfrak{m}$, 这意味着 $\sum r_i m_i \in \mathfrak{m}M$, 因此 $r_i \in M$ 对于所有 i 。因此, 元素 m_1, \dots, m_n 在 $M/\mathfrak{m}M$ 中是线性无关的, 因此是基。因此 $\dim M/\mathfrak{m}M = n$, 这意味着 $N/\mathfrak{m}N$ 是平凡的。由于 $N = \mathfrak{m}N$ 且 R 是具有最大理想 \mathfrak{m} 的局部环, 中山引理意味着 $N = 0$ 。因此, $M \cong R^n$ 是自由的 R - 模块。

1.21 Algebra Q21

Exercise

问题20. (Lang III.19) 设 (A_i, f_{ij}) 为一个有向模块族。设 $a_k \in A_k$ ，且假设 a_k 在直极限 A 中的像为 0。证明存在某个 $m \geq k$ ，使得 $f_{km}(a_k) = 0$ 。换句话说，对于某个群 A 中的任意一个元素，在直极限中消失的现象已经可以在原始数据中观察到。

Solution

解决方案：对于索引 i ，令 $f_i : A_i \rightarrow A$ 为直接极限给出的映射。令 $S = \{a_i\}$ ，对于 $x_i \in A_i$ ，用 x'_i 表示直接和中第 i 个分量为 x_i ，其余分量为零的元素。令 N 为 S 的子群，由元素 $(\dots, 0, x_i, -f_{ij}(x_i), 0, \dots)$ 生成，其中 $x_i \in A_i$ ， $-f_{ij}(x_i) \in A_j$ ，且 $i \leq j$ 。事实 $f_k(a_k) = 0$ 意味着 $a_k \in N$ 。因此，我们可以将 a_k 写为

$$(\dots, 0, a_k, \dots) = \sum (\dots, 0, a_i, -f_{ij}(a_i), 0, \dots)$$

其中 $r \geq 1$ ，且 $i_t \leq j_t$ 对于 $1 \leq t \leq r$ 。尽管上述索引 i_t 和 j_t 可能分布在不同的分量中，但当 $s \leq k$ 时，第 s 个分量的和为零，当 $s = k$ 时，第 s 个分量的和为 a_k 。因此，对于 $m \geq \max\{k, j_1, \dots, j_r\}$ （该值必定存在），我们有

$$\begin{aligned} f_{km}(a_k) &= f_{km}(a_k) - \sum f_{j_tm}(f_{i_tj_t}(a_{i_t})) + \sum f_{i_tm}(a_{i_t}) - \sum f_{j_tm}(f_{i_tj_t}(a_{i_t})) \\ &= \sum (f_{i_tm}(a_{i_t}) - f_{j_tm}(f_{i_tj_t}(a_{i_t}))) + f_{i_tm}(a_{i_t}) - f_{j_tm}(a_{i_t}) \\ &= 0\Theta \end{aligned}$$

因此， m 就是我们要找的索引。

1.22 Algebra Q22

Exercise

问题 21. (Lang III.24) 证明任何模块都是有限生成子模块的直接极限。

Solution

解：设 R 为一个环， M 为 R -模块。对于 M 的任意有限子集 S ，记 M_S 为由 S 生成的 M 的有限子模块。 M 的有限子集形成一个有向索引系统。对于 M 的有限子集 S 和 T ，其中 $S \subseteq T$ ，记 $i_{S,T}$ 为从 M_S 到 M_T 的包含映射。 $(M_S, i_{S,T})$ 是有限生成 R -模块的有向系统。我们证明 (M, i_S) 是 $(M_S, i_{S,T})$ 的直接极限，其中 $i_S : M_S \rightarrow M$ 是包含映射。对于 $S \subset T$ ， $i_T \circ i_{S,T} = i_S$ 。设 (N, f_S) ，其中 N 是 R -模块，对于 M 的每个有限子集 S ， $f_S : M_S \rightarrow N$ 是 R -模块同态，且 $f_T \circ i_{S,T} = f_S$ 。定义 $f : M \rightarrow N$ 如下。对于 $m \in M$ ，设 $f(m) = f_{\{m\}}(m)$ 。如果 S 是包含 m 的 M 的有限子集，则 $f_S(m) = f_{\{m\}}(m)$ 。因此，如果 $a, b \in M$ 且 $c \in R$ ，则 $f(a+b) = f_{\{a,b\}}(a+b) = f_{\{a,b\}}(a) + f_{\{a,b\}}(b) = f(a) + f(b)$ 。因此 f 是同态。对于 M 的有限子集 S 和 $m \in M_S$ ， $f(i_S(m)) = f(m) = f_{\{m\}}(m) = f_S(m)$ 。因此， M 是其有限生成子模块的直接极限。

1.23 Algebra Q23

Exercise

问题22. (Lang III.21) 设 (M'_i, f'_{ij}) 和 (M_i, g_{ij}) 是模块的有向系统。模块 (M'_i) 到 (M_i) 的同态指的是一族同态 $u_i : M'_i \rightarrow M_i$ ，其中每个 i 都与 f'_{ij} 和 g_{ij} 交换。假设我们有一个精确序列

$$0 \rightarrow M'_i \xrightarrow{\alpha_i} M_i \xrightarrow{\beta_i} M''_i \rightarrow 0$$

有向系统的精确序列，意味着对于每个 i ，序列

$$0 \rightarrow M'_i \xrightarrow{\alpha_i} M_i \xrightarrow{\beta_i} M''_i \rightarrow 0$$

是精确的。证明直接极限保持精确性，即

$$0 \rightarrow \varinjlim M'_i \rightarrow \varinjlim M_i \rightarrow \varinjlim M''_i \rightarrow 0$$

是精确的。

Solution

解：令 M' 、 M 和 M'' 分别表示直极限 $\varinjlim M'_i$ 、 $\varinjlim M_i$ 和 $\varinjlim M''_i$ 。我们知道 (M'_i, α_i) 是一个有向系统的模块， $\alpha_i : M'_i \rightarrow M_i$ 与 g'_{ij} 和 h'_{ij} 通勤。只要证明序列 $M' \rightarrow M \rightarrow M''$ 在 M 处是精确的，因为在 M' 和 M'' 处的精确性可以通过考虑序列 $0 \rightarrow M' \rightarrow M$ 和 $M \rightarrow M'' \rightarrow 0$ 得到。

我们将证明 $\ker(v) = \text{Im}(u)$ 。对于每个 $m' \in M'$ ，存在 i 和 $m'_i \in M'_i$ ，使得 $m' = f_i(m'_i)$ 。考虑以下交换图

$$\begin{array}{ccccccccc} 0 & \rightarrow & M'_i & \xrightarrow{\alpha_i} & M_i & \xrightarrow{\beta_i} & M''_i & \rightarrow & 0 \\ & & \downarrow f_i & & \downarrow g_i & & \downarrow h_i & & \\ 0 & \rightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \rightarrow & 0 \end{array}$$

我们得到

$$v(u(m')) = v(u(f_i(m'_i))) = v(g_i(\alpha_i(m'_i))) = h_i(\beta_i(\alpha_i(m'_i))) = h_i(0) = 0;$$

因此序列是精确的。因此 $\text{Im}(u) \subseteq \ker(v)$ 。为了证明反向包含，取 $m \in \ker(v)$ 。然后取 i 和 $m_i \in M_i$ ，使得 $m = g_i(m_i)$ 。由于 $h_i(\beta_i(m_i)) = v(g_i(m_i)) = 0$ ，存在 $j \geq i$ ，使得 $h_j(\beta_i(m_i)) = 0$ 。因此 $g_j(\beta_i(m_i)) = 0$ 。由于 $g_j(\beta_i(m_i)) \in \ker(v_j) = \text{Im}(u_j)$ ，存在 $m'_j \in M'_j$ ，使得 $u_j(m'_j) = g_j(m_i)$ 。取 $m' = f_j(m'_j) \in M'$ ，

$$u(m') = u(f_j(m'_j)) = g_j(u_j(m'_j)) = g_j(g_j(m_i)) = g_j(m_i) = m.$$

因此 $\ker(v) \subseteq \text{Im}(u)$ ，这意味着序列 $M' \rightarrow M \rightarrow M''$ 在 M 处是精确的。

1.24 Algebra Q24

Exercise

问题 23. (Lang III.23) 设 (M_i) 为一个环上的有向模块族。对于任意模块 N , 证明:

$$\lim \leftarrow \text{Hom}(N, M_i) = \text{Hom}(N, \lim \leftarrow M_i)。$$

Solution

解决方案: 对于 $i \leq j$, 我们用 $f_{ji}: M_j \rightarrow M_i$ 表示模块 (M_i) 的有向族中的同态, 并用 M 表示其逆极限。对于 $i \leq j$, 我们用 $\neg f_{ji}: \text{Hom}(N, M_j) \rightarrow \text{Hom}(N, M_i)$ 表示由 $\neg f_{ji}(\phi)(x) = f_{ji}(\phi(x))$ 对于 $\phi \in \text{Hom}(N, M_j)$ 和 $x \in N$ 给出的同态。由于 (M_i) 是模块的有向族, 因此 $(\text{Hom}(N, M_i), \neg f_{ji})$ 也是模块的有向族。

我们用 $\neg f_i$ 表示从 $\text{Hom}(N, M)$ 到 $\text{Hom}(N, M_i)$ 的同态, 由 $\neg f_i(\phi)(x) = f_i(\phi(x))$ 给出。我们只需要证明 $(\text{Hom}(N, M), \neg f_i)$ 是模块的有向族 $(\text{Hom}(N, M_i), \neg f_{ji})$ 的逆极限。

如果 $\phi \in \text{Hom}(N, M)$ 且 $x \in N$, 我们有

$$(\neg f_{ji}(\neg f_j(\phi)))(x) = f_{ji}(\neg f_j(\phi)(x)) = f_{ji}(f_j(\phi(x))) = f_i(\phi(x)) = \neg f_i(\phi)(x),$$

对于任何 $i \leq j$ 。因此 $\neg f_{ji} \circ \neg f_j = \neg f_i$ 对于 $i \leq j$ (即上述图表中的上三角形是可交换的)。现在假设 (A, α_i) , 其中 $\alpha_i: A \rightarrow \text{Hom}(N, M_i)$ 满足 $\neg f_{ji} \circ \alpha_j = \alpha_i$ 。我们定义 $\alpha: A \rightarrow \text{Hom}(N, M)$ 由 $\alpha(a)(x) = (\alpha_i(a)(x))$ 对于 $a \in A$ 和 $x \in N$ 。若 $i \leq j$, $f_{ji}(\alpha_j(a)(x)) = \alpha_i(a)(x)$ 对于每个 $a \in A$ 和 $x \in N$ 。因此 $(\alpha_i(a)(x)) \in M$ 对于每个 $a \in A$ 和 $x \in N$, 这意味着 $\alpha(a): N \rightarrow M$ 是一个良定义的映射。映射 α 在以下图表中用虚线表示:

$$\begin{array}{ccccccc} \text{Hom}(N, M_j) & \text{Hom}(N, M_i) & \text{Hom}(N, M) & A & \neg f_{ji} & \neg f_j & \neg f_i \\ & & & & \alpha_j & \alpha_i & \alpha \end{array}$$

对于 A 中的每个 a , 映射 $\alpha_i(a)$ 都是同态, 因此映射 $\alpha(a)$ 也是同态。因此, 我们有 α 是良定义的。事实上 α 是模块同态, 来自于 α_i 是每个索引

i 的模块同态。最后，对于任何索引 i 和 $a \in A$ ，我们有

$$\neg f_i(\alpha(a))(x) = f_i(\alpha(a)(x)) = f_i((\alpha j(a)(x))) = \alpha i(a)(x),$$

对于所有 $x \in N$ 。因此 $\neg f_i \circ \alpha = \alpha i$ 对于所有索引 i (即 α 保持上述图表的可交换性)。因此 $(\text{Hom}(N, M), \neg f_i)$ 是模块的有向族 $(\text{Hom}(N, M_i), \neg f_{ji})$ 的逆极限。



1.25 Algebra Q25

Exercise

问题 24. (Lang V.13) 如果某个单变量多项式 $f(x) \in k(x)$ 在某个分裂域中的根是不同的, 并且形成一个域, 则 $\text{char}(k) = p$ 且 $f(x) = x^{p^m} - x$, 其中 $m \geq 1$ 。

Solution

解: 设 $F = \{r_1, \dots, r_n\}$ 为 f 的根集。由于 F 是一个域, 对于任何 $k \in \mathbb{N}$, $k \cdot 1$ 都是 f 的根。由于多项式只有有限个根, $\text{char}(k) = p$ 。由于 f 在 F 上分解, 即 $f(x) = (x - r_1) \dots (x - r_n)$, 且 F 由 f 的根生成, F 必定是 f 的分解域。设 \mathbb{F}_p 为 F 的素域。由于 F 是 \mathbb{F}_p 上的有限维向量空间, $n = |F| = p^m$ 。我们还知道, 阶为 p^m 的有限域是多项式 $x^{p^m} - x$ 的分解域。因此, $f(x) = x^{p^m} - x$ 。

1.26 Algebra Q26

Exercise

问题25. (Lang V.14) 设 $\text{char}(K) = p$ 。设 L 是 K 的有限扩张, 且 $[L : K]$ 与 p 互质。证明 L 在 K 上是可分的。

Solution

解: 取 L 中的一个元素 α 。由于 $L : K$ 是有限的, α 是代数的。设 $f(x) \in K[x]$ 是 α 在 K 上的不可约多项式。由于 $m = \deg f$ 能整除 $[L : K]$, 我们有 $(m, p) = 1$ 。设 f' 是 $K[x]$ 中一个可分多项式, 使得 $f(x) = (f'(x))^{p^e}$, 其中 e 是非负整数。这意味着 $m = \deg f' \cdot p^e \deg f_{\text{sep}}$, 因此 p^e 能整除 m 。事实 $(m, p) = 1$ 迫使 e 为零。因此 $f = f_{\text{sep}}$ 在 K 上是可分的。

1.27 Algebra Q27

Exercise

问题 26. (Lang V.15) 假设 $\text{char}(K) = p$ 。令 $a \in K$ 。如果 a 在 K 中没有 p 次方根, 证明对于所有正整数 n , $x^{p^n} - a$ 在 $K[x]$ 中是不可约的。

Solution

解: 设 n 为正整数, $f(x) = x^{p^n} - a$ 。如果 β_1 和 β_2 是 f 在某个分裂域中的根, 则有 $(\beta_1 - \beta_2)^{p^n} = \beta_1^{p^n} - \beta_2^{p^n} = a - a = 0$, 因此 $\beta_1 = \beta_2$ 。因此, f 是完全不可分的, 因此在 K 上的某个分裂域 F 中存在 β , 使得 $f(x) = (x - \beta)^{p^n} = x^{p^n} - \beta^{p^n}$ 。如果 g 是 β 在 K 上的不可约多项式, 则在 F 中, $g(x) = (x - \beta)^k$, 其中 k 为某个正整数。由于 f 是不可约的且完全不可分的, g 的次数必定是 p 的幂。由于 g 能整除 $K[x]$ 中的 f , 因此有 $k \leq p^n$ 。如果 $k < p^n$, 则 $g(x) = (x - \beta)^k$, 因此 g 是不可约的。设 $k < n$, 由此可知 β^{p^k} 是 g 的系数, 因此 $\beta^{p^k} \in K$ 。如果 $a = \beta^{p^n}$, 则有 $a = (\beta^{p^k})^{p^{n-k}} \in K$ 。因此, 有 $a = \alpha^{p^k}$, 其中 $\alpha \in K$ 。这与 a 在 K 中没有 p 次方根的事实相矛盾。

1.28 Algebra Q28

Exercise

问题27. (Lang V.16) 设 $\text{char}(K) = p$ 。设 α 是 K 的代数数。证明 α 可分割当且仅当对于所有正整数 n , $K(\alpha) = K(\alpha^{p^n})$ 。

Solution

解决方案: 首先, 我们假设 α 是可分的。鉴于 $K(\alpha)$ 是可分的, 足以证明 α 是可分的。由于 α 是多项式 $x^{p^n} - \alpha^{p^n} \in K(\alpha^{p^n})[x]$ 的根, α 在 $K(\alpha^{p^n})$ 上的不可约多项式 $g(x)$ 能整除 $x^{p^n} - \alpha^{p^n}$ 。因此, 在 $K(\alpha^{p^n})[x]$ 中, $g(x) = (x - \alpha)^{p^n}$ 。如果 $g(x)$ 是 α 在 K 上的不可约多项式, 则 $g(x)$ 能整除 $K[x]$ 中的 $(x - \alpha)^{p^n}$ 。由于 α 是可分的, $g'(x) \neq 0$ 。因此, $\alpha \in K(\alpha^{p^n})$ 。

另一方面, 假设对于所有正整数 n , $K(\alpha) = K(\alpha^{p^n})$ 。令 $a(x)$ 为 α 在 K 上的不可约多项式。存在一个可分多项式 $a_{\text{sep}}(x) \in K[x]$ 和一个非负整数 e , 使得 $a(x) = a_{\text{sep}}(x^{p^e})$ 。由于 α 是 $a(x)$ 的根, α^{p^e} 是 $a_{\text{sep}}(x)$ 的根。由于域 $K(\alpha)$ 是不可约的, $a_{\text{sep}}(x)$ 也是不可约的。因此, $a_{\text{sep}}(x)$ 是 α^{p^e} 在 K 上的不可约多项式。由此可知

$$\deg a_{\text{sep}}(x) = [K(\alpha^{p^e}) : K] = [K(\alpha) : K] = \deg a(x)\Theta$$

这意味着 $k = 0$, 因此 $a(x) = a_{\text{sep}}(x)$ 。因此, $\alpha(x)$ 是可分的。

1.29 Algebra Q29

Exercise

问题 28. (Lang V.18) 证明有限域中的每个元素都可以表示为该域中两个平方和。

Solution

设 F 为有限域。若 $\text{char}(F) = 2$ ，则弗罗贝尼乌斯同态是满射的，因此对于任何 $y \in F$ ，存在 $x \in F$ 使得 $y = x^2 = x^2 + 0^2$ 。现在假设 $\text{char}(F) = p$ 为奇素数。则 $|F|$ 为奇数，因此 $|F^\times| = 2k$ ，其中 k 为某个自然数。此外， F^\times 是循环群；设 $F^\times = \langle a \rangle$ 。注意到 a 的每个偶数次方都是平方数。由于 0 也是 F 中的平方数，因此至少有 $k+1$ 个元素是平方数。设 S 为 F 中所有平方数的集合。对于 F 中的任意元素 y ，以下不等式成立：

$$|y - S| = |S| = k + 1 \geq \frac{|F|}{2}$$

根据鸽巢原理，存在 $s \in (y - S) \cap S$ ，这意味着 $s = s_1^2$ ，其中 $s_1 \in F$ ，且 $s = y - s_2^2$ ，其中 $s_2 \in F$ 。因此 $y = s_1^2 + s_2^2$ 。

1.30 Algebra Q30

Exercise

问题29. (Lang V.24) 证明原始元素定理不一定对有限不可分扩张成立。

Solution

解: 设 $F = \mathbb{Z}_p(Y, Z)$, 其中 Y 和 Z 是 \mathbb{Z}_p 上的两个代数独立的超越元素。设 E 为 F 的一个代数闭包。考虑多项式 $p(x) = x^p - Y$ 和 $q(x) = x^p - Z$ 在 $F[x]$ 中。由于 $p(x)$ 和 $q(x)$ 是关于素理想 (Y) 和 (Z) 的 Eisenstein 多项式, 因此这两个多项式在 $F[x]$ 中是不可约的。根据高斯引理, 它们也是 F 上不可约的。设 α 和 β 分别为 $p(x)$ 和 $q(x)$ 在 E 中的根。考虑域扩张 $F(\alpha, \beta)/F$ 。由于 $p(x) = (x - \alpha)^p$ 在 $F(\alpha)[x]$ 中 (在 F 中约化), 我们将得到 $F \subset F(\alpha)$, 因此 $\beta^p = Z \in F(\alpha)$, 其中 $c_i \in F$ 。但这将意味着 $Z = \sum c_i \alpha^i$, 这不可能发生, 因为 Y 和 Z 是代数独立的。因此, $q(x)$ 在 $F(\alpha)$ 上是不可约的。这意味着

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] = p^2.$$

现在, 对于 $F(\alpha, \beta)$ 中的 γ , 存在 $c_{ij} \in F$, 使得 $\gamma = \sum c_{ij} \alpha^i \beta^j$ 。因此,

$$\gamma^p = \sum c_{ij}^p (\alpha^i \beta^j)^p = \sum c_{ij}^p Y^i Z^j \in F.$$

因此, $[F(\gamma) : F] \leq p$, 这意味着 $F(\alpha, \beta)$ 不能是 F 的简单扩张。

1.31 Algebra Q31

Exercise

问题30. (Hungerford V.5.9) 如果 $n \geq 3$, 证明 $x^{2^n} + x + 1$ 在 \mathbb{F}_2 上是可约的。

Solution

解: 令 $p(x) = x^{2^n} + x + 1$ 。假设, 为了矛盾, $p(x)$ 是不可约的。令 r 为 $p(x)$ 在某个分裂域 F 中的根。则 $[\mathbb{F}_2(r) : \mathbb{F}_2] = n$ 。这意味着 $\mathbb{F}_2(r) = \mathbb{F}_{2^n}$ 。此外, 我们知道 \mathbb{F}_{2^n} 是多项式 $q(x) = x^{2^n} - x \in \mathbb{F}_2[x]$ 的分裂域。注意, 对于任何 $a \in \mathbb{F}_{2^n}$,

$$p(r+a) = (r+a)^{2^n} + (r+a) + 1 = (r^{2^n} + r + 1) + (a^{2^n} - a) = 0 \ominus$$

因此, 对于每个 $a \in \mathbb{F}_{2^n}$, $r+a$ 是 $p(x)$ 的根。由于 $r^{2^n} + r + 1 = 0$, \mathbb{F}_{2^n} 中的任何元素都是 $p(x)$ 的根。特别地, $0 = p(0) = 1$, 这是一个矛盾。因此, $p(x)$ 是不可约的。

1.32 Algebra Q32

Exercise

31. (Hungerford V.5.12) 设 p 为素数。证明, 对于任意正整数 n , $\mathbb{F}_p[x]$ 中存在一个次数为 n 的不可约多项式。

Solution

解: 我们知道, 存在一个唯一的 (同构意义下) 阶为 p^n 的域, 记为 F 。令 F^\times 为 F 的单位的乘法子群。由于 F 是 \mathbb{F}_p 上的向量空间, 且 $|F| = p^n$, 因此 $[F : \mathbb{F}_p] = n$ 。由于 F^\times 是有限的, 因此它一定是循环的。因此存在 $a \in F$, 使得 $F^\times = \langle a \rangle$ 。因此, $F = \mathbb{F}_p(a)$ 。令 $f(x)$ 为 a 的不可约多项式。则 $\deg f = [\mathbb{F}_p(a) : \mathbb{F}_p]$ 。因此, $f(x)$ 是一个次数为 n 的不可约多项式。

1.33 Algebra Q33

Exercise

问题 32. (Lang VI.11) 如果多项式 $f(x)$ 的根为 α , 则 $1/\alpha$ 也是其根, 则称 $f(x)$ 为可逆多项式。假设 $f(x)$ 的系数在复数域的实子域 k 中。若 $f(x)$ 在 k 上不可约且有一个非实根的绝对值为 1, 证明 $f(x)$ 是偶数次的可逆多项式。

Solution

解: 设 β 为 $f(x)$ 的一个非实根, 且其绝对值为 1, 设 α 为 $f(x)$ 的任意一个根。设 K 为 $f(x)$ 在 \mathbb{C} 中的分裂域, 设 G 为 K/k 的 Galois 群。由于 $f(x)$ 在 k 上不可约, G 在 $f(x)$ 的根上作用是可传递的。因此存在 $\sigma \in G$, 使得 $\sigma(\beta) = \alpha$ 。这意味着 $\sigma(\bar{\beta}) = \overline{\sigma(\beta)} = \bar{\alpha}$ 。由于 β 是 $f(x)$ 的根, 因此 α^{-1} 也是 $f(x)$ 的根; 这是因为 σ 把 $f(x)$ 的根进行了排列。因此, $f(x)$ 是一个回文多项式。

由于 $f(x)$ 是一个不可约多项式, 且其系数域的特征为零, 因此 $f(x)$ 是可分的。我们知道, $f(x)$ 的非实根成对出现。由于 $f(x)$ 是回文多项式, 因此实根也成对出现。因此, $f(x)$ 在 K 中有偶数个根。因此, $f(x)$ 的次数为偶数。

1.34 Algebra Q34

Exercise

第33题 (Lang VI.12) 求有理数域上的多项式 $x^5 - 4x + 2$ 的 Galois 群。

Solution

解决方案: (a) 令 $p(x) = x^5 - 4x + 2$, G 为 $p(x)$ 的伽罗瓦群。我们将 G 视为 S_5 的子群。根据 Eisenstein 准则, 多项式 $p(x)$ 在 \mathbb{Z} 上是不可约的。高斯引理则意味着 $p(x)$ 在有理数上是不可约的。因此, G 包含一个长度为 5 的循环。由于 $p'(x) = 5x^4 - 4$ 只有两个实根, $p(x)$ 最多有三个实根。鉴于 $p(-\infty) = -\infty$ 、 $p(0) = 2$ 、 $p(1) = -1$ 和 $p(\infty) = \infty$, $p(x)$ 恰好有三个实根。由于 $p(x)$ 只有两个非实根, 它们是共轭的, 共轭自同构表示 G 中的一个交换。由于 $G \leq S_5$ 包含一个 5-循环和一个交换, $G = S_5$ 。

1.35 Algebra Q35

Exercise

问题34. (Lang VI 13) 找出多项式 $x^4 + 2x^2 + x + 3$ 在有理数域上的伽罗瓦群。

Solution

解: 设 $p(x) = x^4 + 2x^2 + x + 3$ 。对 2 取模后, 我们得到 $p(x) = x^4 + x^2 + 1$ 。由于 $p(x)$ 在 \mathbb{Z}_2 中没有根, 如果它不可约, 则必须分解为两个不可约多项式的乘积, 每个多项式的次数为 2。但是, \mathbb{Z}_2 上唯一的不可约多项式是 $X^2 + X + 1$, 而 $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq p(x)$ 。因此, $p(x)$ 在 \mathbb{Z}_2 上是不可约的。由于每个有限域的有限扩张都是循环的, $p(x)$ 在 \mathbb{Z}_2 上的伽罗瓦群包含一个 4 阶元素。因此, G 包含一个 4 阶元素。

现在对 3 取模, 我们得到 $p(x) = x(x^3 + 2x + 1)$ 。由于 $x^3 + 2x + 1$ 在 \mathbb{Z}_3 中没有根, 因此它在 \mathbb{Z}_3 上是不可约的。因此, $p(x)$ 在 \mathbb{Z}_3 上的伽罗瓦群包含一个 3 阶元素。因此, G 包含一个 3 阶元素。

由于 G 包含一个 3 阶元素和一个 4 阶元素, 因此 $|G|$ 可以被 12 整除。由于 G 与 S_4 的子群同构, 因此 G 与 A_4 或 S_4 同构。由于 A_4 中没有 4 阶元素, 因此 G 必须与 S_4 同构。

1.36 Algebra Q36

Exercise

****问题 35.**** 求多项式 $x^5 - 5$ 在 \mathbb{Q} 上的伽罗瓦群。

Solution

解决方案: 令 $p(x) = x^5 - 5$ 。根据 Eisenstein 准则和 Gauss 引理, $p(x)$ 在 \mathbb{Q} 上是不可约的。令 $a = \sqrt[5]{5}$, ω 为 5 次单位根的原始根。则 $p(x)$ 在 \mathbb{Q} 上的分裂域为 $F = \mathbb{Q}(a, \omega)$; 这是因为 $p(x)$ 的根由 $\omega^i a$ 给出, 其中 $1 \leq i \leq 5$ 。由于 a 是 $p(x)$ 的根, 而 $p(x)$ 在 \mathbb{Q} 上是不可约的, 因此我们有 $[\mathbb{Q}(a) : \mathbb{Q}] = 5$ 。另一方面, 由于 ω 的不可约多项式是 $x^4 + x^3 + x^2 + x + 1$, 因此 $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ 。由于 $(4, 5) = 1$, 因此 $[F : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}][\mathbb{Q}(\omega) : \mathbb{Q}] = 20$ 。因此, $p(x)$ 的 Galois 群 $G = \text{Gal}(F/\mathbb{Q})$ 的阶为 20。

根据问题 1, S_5 不包含阶为 20 的任何 Abelian 子群。因此, G 不是 Abelian 的。根据问题 4, G 必须与阶为 20 的二面体或两个非同构的半直接积 $\mathbb{Z}_5 \rtimes_{\phi} \mathbb{Z}_4$ 中的一个同构。

1.37 Algebra Q37

Exercise

求多项式 $x^5 - 5$ 在 \mathbb{Q} 上的伽罗瓦群。

Solution

设 $p(x) = x^5 - 5$ 。根据 Eisenstein 判别法和高斯引理, $p(x)$ 在 \mathbb{Q} 上是不可约的。设 $a = \sqrt[5]{5}$, ω 为 5 次本原单位根。则 $p(x)$ 在 \mathbb{Q} 上的分裂域为 $F = \mathbb{Q}(a, \omega)$; 这是因为 $p(x)$ 的根由 $a\omega^i$ 给出, 其中 $1 \leq i \leq 5$ 。由于 a 是 $p(x)$ 的根, 而 $p(x)$ 在 \mathbb{Q} 上是不可约的, 因此我们有 $[\mathbb{Q}(a) : \mathbb{Q}] = 5$ 。另一方面, 由于 ω 的不可约多项式是 $x^4 + x^3 + x^2 + x + 1$, 因此 $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ 。由于 $(4, 5) = 1$, 因此 $[F : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}][\mathbb{Q}(\omega) : \mathbb{Q}] = 20$ 。因此, $p(x)$ 的 Galois 群 $G = \text{Gal}(F/\mathbb{Q})$ 的阶为 20。

根据问题 1, S_5 中没有阶为 20 的阿贝尔子群。因此, G 不是阿贝尔群。根据问题 4, G 必须与阶为 20 的二面体群或两个非同构的半直接积 $\mathbb{Z}_5 \rtimes_{\phi} \mathbb{Z}_4$ 中的一个同构。

1.38 Algebra Q38

Exercise

问题36. (Lang VI.14) 证明, 对于一个对称群 S_n , 存在一个多项式 $f(x) \in \mathbb{Z}[x]$, 其首项系数为1, 其在 \mathbb{Q} 上的伽罗瓦群是 S_n 。

Solution

解决方案: 我们在问题 30 中看到, 对于任何素数 p 和任何 $n \in \mathbb{N}$, 存在一个不可约多项式 $g(x) \in \mathbb{F}_p[x]$ 的次数为 n 。取一个不可约多项式 $p_1(x) \in \mathbb{F}_2[x]$ 的次数为 n 。另外, 取一个不可约多项式 $p_2(x) \in \mathbb{F}_3[x]$ 的次数为 $n-1$ 。最后, 取一个不可约多项式 $p_3(x) \in \mathbb{F}_5[x]$ 的次数为 n 。根据中国剩余定理, 存在一个多项式 $f(x) \in \mathbb{Z}[x]$, 使得

$$f(x) \equiv p_1(x) \pmod{2}$$

$$f(x) \equiv xp_2(x) \pmod{3}$$

$$f(x) \equiv q(x)p_3(x) \pmod{5}$$

其中 $q(x)$ 是奇数次数不可约多项式的乘积, 选择方便。设 G 为 $f(x)$ 在有理数域上的 Galois 群, 视为 S_n 的子群。第一个等式意味着 G 包含一个 n 个循环, 因此 G 是 S_n 的一个超越子群。第二个和第三个等式分别保证存在一个 $(n-1)$ 个循环和一个置换在 G 中。正如我们在前一个问题中看到的, 如果一个超越子群 S_n 包含一个 $(n-1)$ 个循环和一个置换, 那么它一定是全群。因此, $G \cong S_n$ 。

1.39 Algebra Q39

Exercise

问题37. (Lang VI.23) 证明以下陈述。(a) 设 G 为一个阿贝尔群。则存在一个阿贝尔扩张，其Galois群为 G 。(b) 设 k 为 \mathbb{Q} 的有限扩张， $G \neq \{1\}$ 为一个有限阿贝尔群。则存在无穷多个阿贝尔扩张，其Galois群为 G 。

Solution

(a) 根据有限生成的阿贝尔群的基本定理，我们有 $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ ，其中 $n_1, \dots, n_k \in \mathbb{N}$ 。根据狄利克雷定理，对于 $i \in \{1, \dots, k\}$ ，存在无穷多个素数 p ，使得 $p-1 \in (n_i)$ 。因此，我们可以选择不同的素数 p_1, \dots, p_k ，使得 $p_i-1 \in (n_i)$ 。由于 (p_i) 和 (p_j) 是互质的，对于 $i \neq j$ ，如果 $n = p_1 \cdots p_k$ ，根据中国剩余定理，我们有 $\mathbb{Z}_n \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$ 。这意味着

$$(\mathbb{Z}_n)^\times \cong (\mathbb{Z}_{p_1})^\times \times \cdots \times (\mathbb{Z}_{p_k})^\times \Theta$$

因此，我们有 $(\mathbb{Z}_n)^\times \cong \mathbb{Z}_{p_1-1} \times \cdots \times \mathbb{Z}_{p_k-1}$ 。现在，如果 ζ 是一个原始的 n 次单位根，

$$H = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}_n)^\times \cong \mathbb{Z}_{p_1-1} \times \cdots \times \mathbb{Z}_{p_k-1} \Theta$$

注意到 H 有一个子群 $N = N_1 \times \cdots \times N_k$ ，其中 N_i 是 \mathbb{Z}_{p_i-1} 的一个循环子群，阶为 n_i 。由于 N 是阿贝尔群， N 是 H 的一个正常子群。设 F 为 N 在伽罗瓦扩张 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 中的不动点域。然后，根据伽罗瓦对应定理， F/\mathbb{Q} 是伽罗瓦扩张，其伽罗瓦群由 H/N 给出。由于 $\mathbb{Z}_{p_i-1}/N_i \cong \mathbb{Z}_{n_i}$ ，我们有 $H/N \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} = G$ 。因此，我们得到所需的结果。(b) 根据狄利克雷定理，存在无穷多个素数 p ，使得 $p-1 \in (n_i)$ 。因此，我们可以创建一个族 $\mathcal{F} = \{S_i : i \in \mathbb{N}\}$ ，其中 $S_i = \{p_{i1}, \dots, p_{ik}\}$ ，使得 p_{ij} 是素数，满足 $p_{ij}-1 \in (n_j)$ ，且 $S_r \cap S_t$ 为空集，对于 $r \neq t$ 。定义 $c_i = \prod_{j=1}^k p_{ij}$ ，对于所有 $i \in \mathbb{N}$ 。现在考虑扩张 $\mathbb{Q}(\zeta_{c_i})$ ，其中 ζ_{c_i} 是一个原始的 c_i 次单位根。由

于 $(c_r, c_t) = 1$, 对于 $r \neq t$, 我们有 $\mathbb{Q}(\zeta_{c_r}) \cap \mathbb{Q}(\zeta_{c_t}) = \mathbb{Q}$ 。对于每个 i , 我们生成一个中间域 F_i , 其伽罗瓦群为 G , 与我们在 (a) 中所做的类似。由于 $[k : \mathbb{Q}] < \infty$ 且 $\mathbb{Q}(\zeta_{c_r}) \cap \mathbb{Q}(\zeta_{c_t}) = \mathbb{Q}$, 对于所有 $r \neq t$, 只有有限多个 i 使得 $\mathbb{Q}(\zeta_{c_i}) \cap k$ 严格包含 \mathbb{Q} 。因此, 对于无穷多个 i , 满足 $F_i \cap k = \mathbb{Q}$,

$$\text{Gal}(kF_i/k) \cong \text{Gal}(F_i/\mathbb{Q}) \cong G\Theta$$

1.40 Algebra Q40

Exercise

问题38. (Lang VI.24) 证明存在无穷多个非零互质整数 a, b , 使得 $-4a^3 - 27b^2$ 是 \mathbb{Z} 中的完全平方数。

Solution

解决方案: (感谢我的教授 Vera Serganova 提供的解决方案。) 我们可以通过以下方式来实现。我们想要 $d^2 = -4a^3 - 27b^2$ 或等价地, $a^3 = (d^2 + 27b^2)/4$ 。我们注意到右边是域 $\mathbb{Q}(\omega)$ 中 $(d+3b\sqrt{-3})/2$ 的范数, 其中 ω 是一个原始的三次方根。对于任何 $\alpha \in \mathbb{Z}[\omega]$, α^3 的范数是 α 的范数的立方。由于 α 的范数是整数, 我们可以取任何 α 并设置 $\alpha^3 = (d+3b\sqrt{-3})/2$, 然后 a 就是 α 的范数。为了使 a 和 b 相对质, 我们可以取例如 $a = (1+3p\sqrt{-3})/2$, 其中 p 是素数。然后 b 和 d 是互质的, 因此 a 和 b 也互质。

1.41 Algebra Q41

Exercise

问题39. (Lang VI.31) 设 F 为有限域, K 为 F 的有限扩张。证明 $N_{K/F}$ 和 $T_{K/F}$ 是满射 (作为从 K 到 F 的映射)。

Solution

证明: 设 p 为 F 的特征。我们将 $T_{K/F}$ 和 $N_{K/F}$ 简写为 T 和 N 。首先, 我们证明迹是满射的。由于 $T: K \rightarrow F$ 是 F 上的向量空间的线性变换, 且 F 的维数为 1, 因此 $\text{Im}(T)$ 要么是 0, 要么是 F 。由于 K/F 是有限伽罗瓦扩张, 其伽罗瓦群 G 是有限的。因此, 根据 Artin 定理, G 的元素必须线性独立。这意味着存在 $a \in K^\times$ 使得 $T(a) \neq 0$ 。因此 $\text{Im}(T) = F$ 。现在我们证明 N 是满射。假设 $|K| = p^n$ 。由于 K/F 是有限且可分的, 因此扩张 K/F 是伽罗瓦扩张。设 G 为 K/F 的伽罗瓦群。由于每个有限域的有限扩张都是循环的, 因此存在 $\varphi \in G$ 使得 $G = \langle \varphi \rangle$ 。另一方面, K 和 F 的单位群 K^* 和 F^* 是循环的。由于 N 是乘法的, 因此它诱导了一个群同态 $L_N: K^* \rightarrow F^*$, 由 $L_N(a) = N(a)$ 给出。 K^* 中的元素 a 在 $\ker(L_N)$ 中当且仅当

$$1 = \prod_{i=0}^{n-1} \varphi^i(a) = \prod_{i=0}^{n-1} a^{p^i} = a^{1+p+\cdots+p^{n-1}} \Theta$$

这当且仅当 a 是多项式 $p(x) = x^c - 1$ 的根, 其中 $c = 1 + p + \cdots + p^{n-1}$ 。因此 $|\ker(L_N)| = c$, 因此

$$|K^* / \ker(L_N)| = \frac{p^n - 1}{c} = p - 1 \Theta$$

根据第一个同构定理, $|\text{Im}(L_N)| = p - 1$ 。因此, L_N 是满射的, 然后 N 也满射。

1.42 Algebra Q42

Exercise

问题40. (Hungerford V.8.9) 如果 $n > 2$ 且 ζ 是 \mathbb{Q} 上的原始 n 次单位根, 则 $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \phi(n)/2$ 。

Solution

解: 设 K 为域 $\mathbb{Q}(\zeta + \zeta^{-1})$ 。设 G 为域扩张 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 的伽罗瓦群。设 $\sigma \in G$ 为共轭自同构。考虑 G 的循环子群 $\langle \sigma \rangle$ 。我们将证明 K 是 $\langle \sigma \rangle$ 的不动点域。很容易看出 σ 固定 K 。假设 $\phi \in G$ 固定 $\zeta + \zeta^{-1}$ 。则

$$\zeta + \zeta^{-1} = \phi(\zeta + \zeta^{-1}) = \phi(\zeta) + \phi(\zeta)^{-1}.$$

由于 ζ 是原始的, $\phi(\zeta) = \zeta^i$, 其中 i 为某个整数。将 $\phi(\zeta) = \zeta^i$ 代入上式, 我们得到 $(\zeta + \zeta^{-1} - 1)(\zeta^i - 1) = 0$ 。因此 i 要么是 $1 \pmod{n}$, 要么是 $-1 \pmod{n}$ 。因此, K 是 $\langle \sigma \rangle$ 的不动点域。然后, 由伽罗瓦对应定理可知, $[\mathbb{Q}(\zeta) : K] = 2$ 。这意味着

$$[K : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}] / [\mathbb{Q}(\zeta) : K] = \phi(n)/2.$$

1.43 Algebra Q43

Exercise

41. (Hungerford V.8.9) 设 p 为素数, ζ 为 p 次本原单位根。求出所有满足 $[F : \mathbb{Q}] = 2$ 的 $\mathbb{Q}(\zeta)$ 的子域 $F \subseteq \mathbb{Q}(\zeta)$ 。

Solution

解决方案: 扩张 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 的伽罗瓦群 G 与 $(\mathbb{Z}/p\mathbb{Z})^*$ 同构。由于 G 是循环群且 $|G| = p - 1$, 因此它仅包含一个阶为 $(p - 1)/2$ 的子群 H 。这意味着, 根据伽罗瓦对应定理, 存在唯一一个中间域 F , 使得 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 的度为 2, 即 H 的不动点域。由于 H 是一个循环群, 我们可以写成 $H = \langle \sigma \rangle$, 其中 $\sigma \in H$ 。如果 $\tau = T_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x) \in F$, 则 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 不一定是 p 的素数。由于 $\zeta - \zeta^{-1}$ 是 $\mathbb{Q}(\zeta)$ 的形式, 因此可以将其唯一地写为 ζ^i 的线性组合。事实上, G 固定 F , 这意味着对于某个 x , $\sigma(x) = x$ 。因此, $p = \sigma^j \in H$ 。因此, 我们可以得出结论: $F = \mathbb{Q}(\tau)$ 是 \mathbb{Q} 上唯一的中间域, 其度为 2。

1.44 Algebra Q44

Exercise

证明任何有限群都与某个有限扩张 $F \subseteq E$ 的伽罗瓦群同构。

Solution

假设 G 是一个有限群，阶为 n 。 G 在自身上的左乘法作用诱导了一个同态 $f: G \rightarrow S_n$ 。由于 f 是单射，我们可以把 G 想象成 S_n 的一个子群。此外，我们已经看到，对于每个 n ，对称群 S_n 都是域扩张 E/F 的伽罗瓦群。由于 G 是 S_n 的一个子群，根据伽罗瓦对应关系，在扩张 E/F 中存在一个中间域 K ，使得 $\text{Gal}(E/K)$ 与 G 同构。

1.45 Algebra Q45

Exercise

问题 43. 设 $\overline{\mathbb{Q}} \subset \mathbb{C}$ 表示代数数的子域, G 表示 $\overline{\mathbb{Q}}$ 在 \mathbb{Q} 上的 (无穷) 伽罗瓦群。我们称 $\alpha \in \overline{\mathbb{Q}}$ 为完全实数, 如果对于任何 $g \in G$, $g(\alpha) \in \mathbb{R}$ 。
(a) 证明所有完全实数的集合 H 是 $\overline{\mathbb{Q}}$ 的一个子域。 (b) 域扩张 H/\mathbb{Q} 是否是正常的?

Solution

(a) 假设 $\alpha, \beta \in H$ 。对于任何 $g \in G$, $g(0) = 0 \in \mathbb{R}$ 且 $g(\alpha + \beta) = g(\alpha) + g(\beta) \in \mathbb{R}$ 。此外, $g(1) = 1$, 如果 $\beta \neq 0$, 则 $g(\alpha\beta^{-1}) = g(\alpha)g(\beta)^{-1} \in \mathbb{R}$ 。因此, H 是 $\overline{\mathbb{Q}}$ 的一个子域。

(b) 假设 $f(x) \in \mathbb{Q}[x]$ 是一个不可约多项式, 其分裂域为 $F \subset \overline{\mathbb{Q}}$ 。设 α 为 $f(x)$ 在 H 中的一个根。设 $\beta \in F$ 为 $f(x)$ 的另一个根。由于 $f(x)$ 是不可约的, $G_F = \text{Gal}(F/\mathbb{Q})$ 在 $f(x)$ 的根上作用是可交换的。因此存在 $\sigma \in G_F$, 使得 $\sigma(\alpha) = \beta$ 。由于 F 的任何自同构都可以扩展到其代数闭包 $\overline{\mathbb{Q}}$, 因此存在 $\bar{\sigma} \in G$, 使得 $\bar{\sigma}|_F = \sigma$ 。现在假设 g 是 G 的任意元素。则 $g(\beta) = (g \circ \bar{\sigma})(\alpha) \in \mathbb{R}$; 这是因为 $g \circ \bar{\sigma} \in G$ 且 $\alpha \in H$ 。因此, $\beta \in H$ 。因此, $f(x)$ 的所有根都在 H 中。由于 $f(x)$ 是任意选择的, 因此 H/\mathbb{Q} 是一个正规扩张。

1.46 Algebra Q46

Exercise

问题 44. 设 p 为素数, F 为多项式 $x^{p^r} - 1$ 的分裂域, 其中 $r > 0$ 。证明 F 在 \mathbb{Q} 上的伽罗瓦群与逆极限 $\varprojlim (\mathbb{Z}/p^r\mathbb{Z})^*$ 同构。

Solution

解: 多项式 $x^{p^r} - 1$ 的分裂域是 $F_r = \mathbb{Q}(\zeta_{p^r})$, 其中 ζ_{p^r} 是 p^r 次单位根的原始根。因此, $F = \mathbb{Q}(\zeta_p, \zeta_{p^2}, \dots)$ 。由于每个 ζ_{p^r} 都是 \mathbb{Q} 上的可分扩张, 因此 F 也可分。因此, F/\mathbb{Q} 是一个伽罗瓦扩张。设 G 为扩张 F/\mathbb{Q} 的伽罗瓦群, $G_r \cong (\mathbb{Z}/p^r\mathbb{Z})^*$ 为扩张 F_r/\mathbb{Q} 的伽罗瓦群。

对于 $j \geq i$, 我们定义 $\phi_{j,i} : G_j \rightarrow G_i$ 为 $\sigma \mapsto \sigma|_{F_i}$ 。则 $(G_r, \phi_{j,i})$ 是一个有向的群族。设 G 为其逆极限。我们证明 G 与 G 同构。定义映射 $f : G \rightarrow G$ 为 $f(\sigma) = (\sigma|_{F_r})$ 。由于 $\sigma|_{F_r}(\zeta_{p^r}) = \zeta_{p^r}^k$, 其中 $k \in \mathbb{Z}$, 因此映射 f 是良定义的。同时, f 也是一个同态。我们证明 f 是单射的。如果 $f(\sigma) = f(\tau)$, 则对于任何 $r > 0$, $\sigma|_{F_r}$ 都是恒等映射。由于 $F = \cup F_r$, 对于每个 $x \in F$, 都存在 r 使得 $x \in F_r$ 。因此, $\sigma(x) = \sigma|_{F_r}(x) = x$ 。因此, f 是单射的。现在, 取 $(s_r) \in G$ 。定义 $\sigma \in G$ 如下: 对于 $x \in F$, 取 r 使得 $x \in F_r$ 。然后设 $\sigma(x) = s_r(x)$ 。假设 $x \in F_r$ 且 $x \in F_s$, 其中 $r < s$ 。由于 (s_r) 在 G 中, 因此 $s_r|_{F_s} = s_s$ 。因此, $\sigma(x)$ 不依赖于 r 的选择。由于 $F_1 \subset F_2 \subset \dots$ 是一个递增的域序列, 其并集是 F , 因此对于每个 $r > 0$, F_r/\mathbb{Q} 都是自同构, 这意味着 σ 是 F 的自同构。由于 $\sigma \in G$ 且 $f(\sigma) = (\sigma|_{F_r})$, 因此同态 f 是满射的。因此, f 是一个同构, 这意味着

$$\text{Gal}(F/\mathbb{Q}) = G \cong \varprojlim_r \text{Gal}(F_r/\mathbb{Q}) \cong \varprojlim_r (\mathbb{Z}/p^r\mathbb{Z})^*.$$

1.47 Algebra Q47

Exercise

问题 45. 证明以下陈述。证明 $\text{PSL}(2, \mathbb{F}_5) \approx A_5$ 。

Solution (by LLM)

由LLM生成的解答可能不准确，请自行验证。

证明： 我们需要证明 $\text{PSL}(2, \mathbb{F}_5) \approx A_5$ ，即 $\text{PSL}(2, \mathbb{F}_5)$ 与 A_5 同构。

首先， $\text{PSL}(2, \mathbb{F}_5)$ 是 $\text{SL}(2, \mathbb{F}_5)$ 模去其中心 $\{I, -I\}$ 得到的群，其中 I 是单位矩阵。 $\text{SL}(2, \mathbb{F}_5)$ 是所有行列式为1的 2×2 矩阵构成的群， \mathbb{F}_5 是5个元素的有限域。

$\text{PSL}(2, \mathbb{F}_5)$ 的阶数为：

$$|\text{PSL}(2, \mathbb{F}_5)| = \frac{|\text{SL}(2, \mathbb{F}_5)|}{|\{I, -I\}|} = \frac{120}{2} = 60$$

而 A_5 是5个元素的交错群，其阶数也是60。

接下来，我们证明 $\text{PSL}(2, \mathbb{F}_5)$ 与 A_5 同构。首先， $\text{PSL}(2, \mathbb{F}_5)$ 是一个单群，因为 $\text{SL}(2, \mathbb{F}_5)$ 是一个单群，且 $\text{PSL}(2, \mathbb{F}_5)$ 是其商群。 A_5 也是一个单群。

由于 $\text{PSL}(2, \mathbb{F}_5)$ 和 A_5 都是阶数为60的单群，且在同构意义下，阶数为60的单群只有 A_5 ，因此 $\text{PSL}(2, \mathbb{F}_5) \approx A_5$ 。

综上所述，我们证明了 $\text{PSL}(2, \mathbb{F}_5) \approx A_5$ 。

1.48 Algebra Q48

Exercise

问题 46. 将所有的 \mathbb{Z} 理想视为一个有向系统，通过可整除性。证明

$$\lim_{\leftarrow} \mathbb{Z}/(a) = \prod_p \mathbb{Z}_p,$$

其中极限是取所有理想 (a) ，并且乘积是取所有素数 p 。

Solution (by LLM)

由LLM生成的解答可能不准确，请自行验证。

解答：

我们需要证明在由整除关系构成的有向系统中， \mathbb{Z} 的所有理想的逆向极限同构于所有 p -进整数环的直积，即

$$\lim_{\leftarrow} \mathbb{Z}/(a) \cong \prod_p \mathbb{Z}_p.$$

步骤1：理解逆向极限的定义

给定由所有非零理想 (a) 构成的有向集，其中 $(a) \leq (b)$ 当且仅当 $b \mid a$ 。对于每对 $(a) \leq (b)$ ，存在自然的投影同态 $\pi_{b,a} : \mathbb{Z}/(b) \rightarrow \mathbb{Z}/(a)$ ，定义为 $x + (b) \mapsto x + (a)$ 。逆向极限 $\lim_{\leftarrow} \mathbb{Z}/(a)$ 是所有相容族 $(x_a)_{a \in \mathbb{Z} \setminus \{0\}}$ 的集合，其中 $x_a \in \mathbb{Z}/(a)$ ，且对于 $(a) \leq (b)$ ，有 $\pi_{b,a}(x_b) = x_a$ 。

步骤2：中国剩余定理的应用

对于任意正整数 a ，设其质因数分解为 $a = \prod_p p^{n_p}$ ，其中 $n_p \geq 0$ 且只有有限多个 $n_p > 0$ 。根据中国剩余定理，有

$$\mathbb{Z}/(a) \cong \prod_p \mathbb{Z}/(p^{n_p}).$$

因此，逆向极限可以分解为

$$\lim_{\leftarrow} \mathbb{Z}/(a) \cong \lim_{\leftarrow} \prod_p \mathbb{Z}/(p^{n_p}).$$

步骤3：分解为各质数的逆向极限

由于逆向极限与直积可交换，我们有

$$\lim_{\leftarrow} \prod_p \mathbb{Z}/(p^{n_p}) \cong \prod_p \lim_{\leftarrow} \mathbb{Z}/(p^{n_p}).$$

对于每个固定的质数 p ， $\mathbb{Z}/(p^{n_p})$ 的逆向极限 $\lim_{\leftarrow} \mathbb{Z}/(p^{n_p})$ 正是 p -进整数环 \mathbb{Z}_p 的定义。因此，

$$\prod_p \lim_{\leftarrow} \mathbb{Z}/(p^{n_p}) = \prod_p \mathbb{Z}_p.$$

步骤4：验证同构

综上，我们得到

$$\lim_{\leftarrow} \mathbb{Z}/(a) \cong \prod_p \mathbb{Z}_p.$$

这一同构将每个相容族 $(x_a)_a$ 映射到其在各质数 p 处的投影 $(x_{p^{n_p}})_p$ ，其中 $x_{p^{n_p}} \in \mathbb{Z}_p$ 。

结论：

因此，原命题得证：

$$\lim_{\leftarrow} \mathbb{Z}/(a) \cong \prod_p \mathbb{Z}_p.$$

1.49 Algebra Q49

Exercise

问题47. 找到一个环 R ，使得 R 与 R^{op} 不全同。

Solution (by LLM)

由LLM生成的解答可能不准确，请自行验证。

问题47. 找到一个环 R ，使得 R 不同构于 R^{op} 。

解答：

我们考虑四元数环 \mathbb{H} 。四元数环 \mathbb{H} 由形如 $a + bi + cj + dk$ 的元素组成，其中 $a, b, c, d \in \mathbb{R}$ ，且 i, j, k 满足以下乘法关系：

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad ik = -j.$$

四元数环 \mathbb{H} 的乘法是非交换的，即存在 $q_1, q_2 \in \mathbb{H}$ 使得 $q_1 q_2 \neq q_2 q_1$ 。因此， \mathbb{H} 与它的对偶环 \mathbb{H}^{op} 不同构。

具体来说， \mathbb{H}^{op} 的乘法定义为：

$$q_1 \cdot_{\text{op}} q_2 = q_2 q_1.$$

由于 \mathbb{H} 的乘法是非交换的， \mathbb{H} 与 \mathbb{H}^{op} 的乘法结构不同，因此 \mathbb{H} 不同构于 \mathbb{H}^{op} 。

综上所述，四元数环 \mathbb{H} 是一个满足 R 不同构于 R^{op} 的环。

1.50 Algebra Q51

Exercise

问题49. 设 k 为一个域, G 为一个有限群, $k[G]$ 表示群环。(a) 证明: 任何一个有限生成的 $k[G]$ -模块都是 k 上的有限维模块。(b) 证明: 任何一个有限维的射影模块都是注射模块。

Solution (by LLM)

由LLM生成的解答可能不准确, 请自行验证。

Problem 49. Let k be a field, G be a finite group, and $k[G]$ denote the group ring.

(a) Show that any finitely generated $k[G]$ -module is finite-dimensional over k .

Solution (a): Let M be a finitely generated $k[G]$ -module. Then there exists a finite set $\{m_1, \dots, m_n\}$ such that $M = k[G]m_1 + \dots + k[G]m_n$. Since G is finite, the group ring $k[G]$ is finite-dimensional over k , with dimension $|G|$.

For each m_i , the cyclic submodule $k[G]m_i$ is a quotient of $k[G]$ by the annihilator of m_i , hence $\dim_k(k[G]m_i) \leq \dim_k(k[G]) = |G|$. Therefore, M is a sum of n subspaces each of dimension at most $|G|$, so $\dim_k(M) \leq n|G| < \infty$.

(b) Show that any finite dimensional projective module is injective.

Solution (b): Let P be a finite-dimensional projective $k[G]$ -module. Since $k[G]$ is a finite-dimensional algebra over k , it is a Frobenius algebra. In particular, $k[G]$ is self-injective, meaning that $k[G]$ is injective as a $k[G]$ -module.

Since P is projective, it is a direct summand of a free module $k[G]^n$ for some n . But $k[G]^n$ is injective because $k[G]$ is injective and finite direct sums

of injective modules are injective. Therefore, P is a direct summand of an injective module, hence injective itself.

This completes the proof.

1.51 Algebra Q52

Exercise

问题50. (Lang III.25) 证明任意模块都是有限呈现模块的有向极限。

Solution (by LLM)

由LLM生成的解答可能不准确，请自行验证。

Problem 50. (Lang III.25) Show that any module is a directed limit of finite presented modules.

Solution:

Let M be a module over a ring R . We will construct M as a directed limit of finitely presented modules.

Step 1: Construct the directed system.

Consider the set \mathcal{F} of all finitely generated submodules of M . For $N_1, N_2 \in \mathcal{F}$, define $N_1 \leq N_2$ if $N_1 \subseteq N_2$. This makes \mathcal{F} a directed set because for any $N_1, N_2 \in \mathcal{F}$, $N_1 + N_2 \in \mathcal{F}$ and $N_1, N_2 \leq N_1 + N_2$.

For each $N \in \mathcal{F}$, let F_N be a finitely generated free module with a surjection $\pi_N : F_N \rightarrow N$. Let $K_N = \ker(\pi_N)$, so we have an exact sequence:

$$0 \rightarrow K_N \rightarrow F_N \xrightarrow{\pi_N} N \rightarrow 0$$

Since N is finitely generated, K_N is also finitely generated (as R is Noetherian in many cases, but more generally, we can choose F_N and π_N such that K_N is finitely generated). Thus, N is finitely presented.

Step 2: Define the transition maps.

For $N_1 \leq N_2$ in \mathcal{F} , the inclusion $\iota_{N_1, N_2} : N_1 \rightarrow N_2$ induces a homomor-

phism $\phi_{N_1, N_2} : F_{N_1} \rightarrow F_{N_2}$ such that the following diagram commutes:

$$\begin{array}{ccc} F_{N_1} & \xrightarrow{\pi_{N_1}} & N_1 \\ \downarrow \phi_{N_1, N_2} & & \downarrow \iota_{N_1, N_2} \\ F_{N_2} & \xrightarrow{\pi_{N_2}} & N_2 \end{array}$$

This gives a directed system (F_N, ϕ_{N_1, N_2}) of finitely presented modules.

Step 3: Take the directed limit.

The directed limit $\varinjlim F_N$ satisfies the universal property of the colimit. There is a natural homomorphism:

$$\varinjlim F_N \rightarrow M$$

induced by the $\pi_N : F_N \rightarrow N \hookrightarrow M$. This map is surjective because every element of M is contained in some finitely generated submodule $N \in \mathcal{F}$, and hence in the image of some F_N .

To show injectivity, suppose $x \in \varinjlim F_N$ maps to 0 in M . Then x is represented by some $y \in F_N$ for some $N \in \mathcal{F}$, and $\pi_N(y) = 0$ in M . But $\pi_N(y) = 0$ implies $y \in K_N$, so $x = 0$ in $\varinjlim F_N$.

Thus, $\varinjlim F_N \cong M$, showing that M is a directed limit of finitely presented modules. \square

1.52 Algebra Q53

Exercise

问题 51. (Lang III.26) 设 E 为一个环上的模块, (M_i) 为一个有向模块族。如果 E 是有限生成的, 证明自然同态

$$\varinjlim \operatorname{Hom}(E, M_i) \rightarrow \operatorname{Hom}(E, \varinjlim M_i)$$

是单射的。如果 E 是有限表示的, 证明这个同态是同构的。

Solution (by LLM)

由LLM生成的解答可能不准确, 请自行验证。

解答:

首先, 我们回顾一下题目中的概念和符号。设 E 是一个环上的模, (M_i) 是一个有向的模块族。我们需要证明当 E 是有限生成模时, 自然同态

$$\varinjlim \operatorname{Hom}(E, M_i) \rightarrow \operatorname{Hom}(E, \varinjlim M_i)$$

是单射; 当 E 是有限展示模时, 这个同态是同构。

第一部分: E 是有限生成模时, 同态是单射。

设 E 是有限生成模, 即存在有限个元素 e_1, \dots, e_n 生成 E 。我们需要证明自然同态

$$\phi : \varinjlim \operatorname{Hom}(E, M_i) \rightarrow \operatorname{Hom}(E, \varinjlim M_i)$$

是单射。

设 $f \in \varinjlim \operatorname{Hom}(E, M_i)$, 且 $\phi(f) = 0$ 。这意味着对于每个 e_j , $f(e_j)$ 在 $\varinjlim M_i$ 中为零。由于 $\varinjlim M_i$ 是 M_i 的直极限, 存在某个 i 使得 $f(e_j)$ 在 M_i 中为零。由于 E 是有限生成的, 我们可以找到一个共同的 i 使得 $f(e_j) = 0$ 对所有 j 成立。因此, f 在 M_i 中为零, 从而 f 在 $\varinjlim \operatorname{Hom}(E, M_i)$ 中为零。这表明 ϕ 是单射。

第二部分: E 是有限展示模时, 同态是同构。

设 E 是有限展示模，即存在一个有限生成自由模 F 和一个有限生成子模 K 使得 $E \cong F/K$ 。我们需要证明自然同态 ϕ 是同构。

首先，我们已经知道 ϕ 是单射。现在我们需要证明 ϕ 是满射。

设 $g \in \text{Hom}(E, \varinjlim M_i)$ 。由于 E 是有限展示的，我们可以将 g 提升到 F 上的同态 $g' : F \rightarrow \varinjlim M_i$ 。由于 F 是有限生成的，存在某个 i 使得 g' 可以分解为 $F \rightarrow M_i \rightarrow \varinjlim M_i$ 。因此， g 可以表示为 $\phi(f)$ ，其中 f 是某个 $\text{Hom}(E, M_i)$ 中的元素。这表明 ϕ 是满射。

综上所述，当 E 是有限展示模时， ϕ 是同构。

结论：

当 E 是有限生成模时，自然同态 ϕ 是单射；当 E 是有限展示模时， ϕ 是同构。

Chapter 2

Test Img 1

Exercise

整环 R 为UFD 当且仅当每个非零素理想 $0 \neq p \in \text{Spec}(R)$ 均包含素元.

Solution

若 R 为UFD, 令 $0 \neq p \in \text{Spec}(R)$, 则存在 $0 \neq a = \pi_1 \dots \pi_n \in p$, 其中 π_i 为素元. 因 p 为素理想, 某一个 π_i 包含于 p 内. 若每个非零素理想均包含素元, 假设非单位 x 无素因子分解, 则根据引理3, 主理想 (x) 中任何元素均无素因子分解. 令 S 为 R 内一切素元生成的乘性子集, 则根据上述性质3与引理3, $S^{-1}(x)$ 为 $S^{-1}R$ 的真子理想. 于是 $S^{-1}R$ 有包含 x 的极大理想 m . 但素理想 $i^{-1}(m)$ 不含任何素元, 矛盾.

Chapter 3

Test Img 2

Exercise

含么交换环 R 有唯一素理想与 R 非单位必为幂零元素等价

Solution

证明(1) \Rightarrow (2) 假设 R 有唯一素理想 P 。由于所有素理想的交集是幂零元集合(即nilradical), 且 P 是唯一素理想, 因此 nilradical 等于 P , 即 P 由所有幂零元组成。设 $a \in R$ 为非单位元素。由于 a 不是单位, 它属于某个极大理想, 而极大理想是素理想, 因此 $a \in P$ (因为 P 是唯一素理想)。故 a 是幂零元。因此, 每个非单位元素都是幂零元素。

证明(2) \Rightarrow (1) 假设 R 中每个非单位元素都是幂零元素。令 N 为 nilradical, 即所有幂零元的集合。由于幂零元形成理想, N 是理想。注意到单位元素不可能是幂零元 (因为如果是单位且 $u^n = 0$, 则 $1 = u^{-1}u$, 乘以 u^{-n} 得 $1 = 0$, 矛盾), 因此 N 恰好由所有非单位元素和零组成。由于每个不在 N 中的元素都是单位, N 是极大理想 (因为任何真理想都包含在 N 中)。现在, 设 P 为任意素理想。由于 P 是真理想, $P \subseteq N$ 。另一方面, 素理想必须包含所有幂零元, 因此 $N \subseteq P$ 。故 $P = N$ 。因此, 所有素理想都等于 N , 即

R 有唯一素理想 N 。