

$\Phi_n \in \mathbb{Z}[x]$, פולינום של ζ , $\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)} = \prod_{(k,n)=1} (x - \zeta^k)$

$\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}})$, $\Phi_p(x) = x^{p-1} - 1$ כי $\Phi_p(x) = \prod_{k=1}^{p-1} (x - \zeta^k)$

$Q(\zeta_n) = \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n)$

נניח $2 < q = p^a$. $L = \mathbb{Q}(\zeta_n)$ - הגדרה $\zeta = \zeta_q$ שורש יחידה פרימיטיבי. $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_n)$ - תוצאה.

$\Gamma: \mathbb{Q} \rightarrow \mathbb{Q}$ (1)

Φ_q (2)

$\alpha = 1 - \zeta \in \mathbb{O}$ ו- $L = \mathbb{Q}(\zeta)$ (3)

$\beta = \alpha^p$ (4)

$\beta = \alpha^p$ (5)

$\Gamma(\beta) = \Gamma(\alpha^p) = \Gamma(\alpha)^p = 1$

$\Gamma(\alpha) = \alpha^p = \beta$ (6)

$u_k = \frac{1 - \zeta^k}{1 - \zeta} = 1 + \zeta + \dots + \zeta^{k-1}$

$\zeta = \zeta_n$, $(k,n)=1$ (7)

$u_k = \frac{1 - \zeta^k}{1 - \zeta}$ (8)

$1 - \zeta^k = u_k(1 - \zeta)$ (9)

$\Phi_q(1) = \prod_{(k,n)=1} (1 - \zeta^k) = u_{\alpha}^{\varphi(q)}$ (10)

$\Phi_q(1) = \Phi_p(1) = p$ (11)

כדי להוכיח (4) נניח (3) ונראה כי (1) נכונה.

$$\Delta(0/\mathbb{Z}) \mid \Delta(\xi)$$

הערה: $\Delta(0/\mathbb{Z}) = 2$ כאשר $\Delta(\xi) = 2$ זהו המקרה הריבועי, כלומר $\Delta(\xi) = 2$ כאשר $\xi = 1$ או $\xi = -1$.

$$\Delta(\xi) = \frac{N_{Q(\xi)/Q}(\xi)}{N_{Q(\xi)/Q}(1)} \cdot (-1)^{\frac{1}{2}(p-1)}$$

הערה: $\xi = \zeta^{p^{a-1}}$ כאשר ζ הוא שורש יחידות.

$$(1-x) \bar{\Phi}_p(x) = x^{p-1}$$

הערה: $\bar{\Phi}_p(x) = \prod_{\chi \neq 1} (1 - \chi(x))$

$$(1-y) \bar{\Phi}'_p(y) = p y^{p-1}$$

$$\bar{\Phi}'_p(y) = \frac{p y^{p-1}}{1-y}$$

$$\bar{\Phi}'_p(x) = \bar{\Phi}'_p(x^{p^{a-1}})$$

$$\bar{\Phi}'_p(x) = \bar{\Phi}'_p(x^{p^{a-1}}) \cdot p^{a-1} \cdot x^{p^{a-1}-1}$$

$$\bar{\Phi}'_p(\xi) = \frac{p y^{p-1}}{1-y} \cdot p^{a-1} \cdot x^{p^{a-1}-1} =$$

$$= \frac{p^a y^{p-1}}{1-y} \cdot y^j = \boxed{\frac{p^a \cdot \zeta^{-1}}{1-\zeta}}$$

הערה: $\zeta = \xi^{p^{a-1}}$

$$N_{Q(\xi)/Q}(\xi^{p^{a-1}}) = p^{a-1} \cdot (-1)^{\frac{1}{2}(p-1)}$$

$$N_{Q(\xi)/Q}(1-\xi) = N_{Q(\eta)/Q}(1-\eta)^{p^{a-1}} = p^{p^{a-1}}$$

$$|Q(\xi):Q(\eta)| = \frac{[Q(\eta)]}{[Q(\eta)]} = p^{p-1}$$

$$\Delta(\xi) = (-1)^{\frac{1}{2}(p-1)} \cdot p^{p^{a-1}} \cdot (p^{a-1})^{\frac{1}{2}(p-1)} =$$

$$= (-1)^{\frac{1}{2}(p-1)} \cdot p^{p^{a-1}} \cdot (p^{a-1})^{\frac{1}{2}(p-1)}$$

~~1/2~~ 1/2

$$\Leftrightarrow \varphi(q) = 0, 1 \pmod{4} \Leftrightarrow 4 \nmid \varphi(q) \vee 4 \mid \varphi(q) \Leftrightarrow 2 \nmid n \vee 2 \mid n$$

$$p^r O \subseteq \mathbb{Z}[\zeta]$$

∴ $f(\beta) = 1 \leftarrow |0/1|$ Now p

$$\mathbb{O}/\alpha\mathbb{O} = \mathbb{D}/p\mathbb{D}$$

6001 $\mathbb{Z}_1-2$, π_k (3) e. $\mathbb{Q}/\mathbb{Z}$ k 601p $\mathbb{Z}_1$ $\mathbb{Z}_1-2$
 , $\mathbb{Z}_1$. $\mathbb{Z}_1-2$

$$G = \langle \tau \rangle + \langle \sigma \rangle$$

$\alpha = 2$ $\gamma = 1$ $\beta = 1$

$$\alpha G \subseteq \mathbb{Z}[5] + \alpha^2 G$$

pad

$$0 \in \mathbb{Z}[\zeta] + \alpha^2 \mathcal{O} \subseteq \mathcal{O}$$

1. $\frac{1}{2}$, 2. $\frac{1}{3}$, 3. $\frac{1}{4}$, 4. $\frac{1}{5}$, 5. $\frac{1}{6}$, 6. $\frac{1}{7}$, 7. $\frac{1}{8}$, 8. $\frac{1}{9}$, 9. $\frac{1}{10}$, 10. $\frac{1}{11}$, 11. $\frac{1}{12}$, 12. $\frac{1}{13}$, 13. $\frac{1}{14}$, 14. $\frac{1}{15}$, 15. $\frac{1}{16}$, 16. $\frac{1}{17}$, 17. $\frac{1}{18}$, 18. $\frac{1}{19}$, 19. $\frac{1}{20}$, 20. $\frac{1}{21}$, 21. $\frac{1}{22}$, 22. $\frac{1}{23}$, 23. $\frac{1}{24}$, 24. $\frac{1}{25}$, 25. $\frac{1}{26}$, 26. $\frac{1}{27}$, 27. $\frac{1}{28}$, 28. $\frac{1}{29}$, 29. $\frac{1}{30}$, 30. $\frac{1}{31}$, 31. $\frac{1}{32}$, 32. $\frac{1}{33}$, 33. $\frac{1}{34}$, 34. $\frac{1}{35}$, 35. $\frac{1}{36}$, 36. $\frac{1}{37}$, 37. $\frac{1}{38}$, 38. $\frac{1}{39}$, 39. $\frac{1}{40}$, 40. $\frac{1}{41}$, 41. $\frac{1}{42}$, 42. $\frac{1}{43}$, 43. $\frac{1}{44}$, 44. $\frac{1}{45}$, 45. $\frac{1}{46}$, 46. $\frac{1}{47}$, 47. $\frac{1}{48}$, 48. $\frac{1}{49}$, 49. $\frac{1}{50}$, 50. $\frac{1}{51}$, 51. $\frac{1}{52}$, 52. $\frac{1}{53}$, 53. $\frac{1}{54}$, 54. $\frac{1}{55}$, 55. $\frac{1}{56}$, 56. $\frac{1}{57}$, 57. $\frac{1}{58}$, 58. $\frac{1}{59}$, 59. $\frac{1}{60}$, 60. $\frac{1}{61}$, 61. $\frac{1}{62}$, 62. $\frac{1}{63}$, 63. $\frac{1}{64}$, 64. $\frac{1}{65}$, 65. $\frac{1}{66}$, 66. $\frac{1}{67}$, 67. $\frac{1}{68}$, 68. $\frac{1}{69}$, 69. $\frac{1}{70}$, 70. $\frac{1}{71}$, 71. $\frac{1}{72}$, 72. $\frac{1}{73}$, 73. $\frac{1}{74}$, 74. $\frac{1}{75}$, 75. $\frac{1}{76}$, 76. $\frac{1}{77}$, 77. $\frac{1}{78}$, 78. $\frac{1}{79}$, 79. $\frac{1}{80}$, 80. $\frac{1}{81}$, 81. $\frac{1}{82}$, 82. $\frac{1}{83}$, 83. $\frac{1}{84}$, 84. $\frac{1}{85}$, 85. $\frac{1}{86}$, 86. $\frac{1}{87}$, 87. $\frac{1}{88}$, 88. $\frac{1}{89}$, 89. $\frac{1}{90}$, 90. $\frac{1}{91}$, 91. $\frac{1}{92}$, 92. $\frac{1}{93}$, 93. $\frac{1}{94}$, 94. $\frac{1}{95}$, 95. $\frac{1}{96}$, 96. $\frac{1}{97}$, 97. $\frac{1}{98}$, 98. $\frac{1}{99}$, 99. $\frac{1}{100}$, 100. $\frac{1}{101}$, 101. $\frac{1}{102}$, 102. $\frac{1}{103}$, 103. $\frac{1}{104}$, 104. $\frac{1}{105}$, 105. $\frac{1}{106}$, 106. $\frac{1}{107}$, 107. $\frac{1}{108}$, 108. $\frac{1}{109}$, 109. $\frac{1}{110}$, 110. $\frac{1}{111}$, 111. $\frac{1}{112}$, 112. $\frac{1}{113}$, 113. $\frac{1}{114}$, 114. $\frac{1}{115}$, 115. $\frac{1}{116}$, 116. $\frac{1}{117}$, 117. $\frac{1}{118}$, 118. $\frac{1}{119}$, 119. $\frac{1}{120}$, 120. $\frac{1}{121}$, 121. $\frac{1}{122}$, 122. $\frac{1}{123}$, 123. $\frac{1}{124}$, 124. $\frac{1}{125}$, 125. $\frac{1}{126}$, 126. $\frac{1}{127}$, 127. $\frac{1}{128}$, 128. $\frac{1}{129}$, 129. $\frac{1}{130}$, 130. $\frac{1}{131}$, 131. $\frac{1}{132}$, 132. $\frac{1}{133}$, 133. $\frac{1}{134}$, 134. $\frac{1}{135}$, 135. $\frac{1}{136}$, 136. $\frac{1}{137}$, 137. $\frac{1}{138}$, 138. $\frac{1}{139}$, 139. $\frac{1}{140}$, 140. $\frac{1}{141}$, 141. $\frac{1}{142}$, 142. $\frac{1}{143}$, 143. $\frac{1}{144}$, 144. $\frac{1}{145}$, 145. $\frac{1}{146}$, 146. $\frac{1}{147}$, 147. $\frac{1}{148}$, 148. $\frac{1}{149}$, 149. $\frac{1}{150}$, 150. $\frac{1}{151}$, 151. $\frac{1}{152}$, 152. $\frac{1}{153}$, 153. $\frac{1}{154}$, 154. $\frac{1}{155}$, 155. $\frac{1}{156}$, 156. $\frac{1}{157}$, 157. $\frac{1}{158}$, 158. $\frac{1}{159}$, 159. $\frac{1}{160}$, 160. $\frac{1}{161}$, 161. $\frac{1}{162}$, 162. $\frac{1}{163}$, 163. $\frac{1}{164}$, 164. $\frac{1}{165}$, 165. $\frac{1}{166}$, 166. $\frac{1}{167}$, 167. $\frac{1}{168}$, 168. $\frac{1}{169}$, 169. $\frac{1}{170}$, 170. $\frac{1}{171}$, 171. $\frac{1}{172}$, 172. $\frac{1}{173}$, 173. $\frac{1}{174}$, 174. $\frac{1}{175}$, 175. $\frac{1}{176}$, 176. $\frac{1}{177}$, 177. $\frac{1}{178}$, 178. $\frac{1}{179}$, 179. $\frac{1}{180}$, 180. $\frac{1}{181}$, 181. $\frac{1}{182}$, 182. $\frac{1}{183}$, 183. $\frac{1}{184}$, 184. $\frac{1}{185}$, 185. $\frac{1}{186}$, 186. $\frac{1}{187}$, 187. $\frac{1}{188}$, 188. $\frac{1}{189}$, 189. $\frac{1}{190}$, 190. $\frac{1}{191}$, 191. $\frac{1}{192}$, 192. $\frac{1}{193}$, 193. $\frac{1}{194}$, 194. $\frac{1}{195}$, 195. $\frac{1}{196}$, 196. $\frac{1}{197}$, 197. $\frac{1}{198}$, 198. $\frac{1}{199}$, 199. $\frac{1}{200}$, 200. $\frac{1}{201}$, 201. $\frac{1}{202}$, 202. $\frac{1}{203}$, 203. $\frac{1}{204}$, 204. $\frac{1}{205}$, 205. $\frac{1}{206}$, 206. $\frac{1}{207}$, 207. $\frac{1}{208}$, 208. $\frac{1}{209}$, 209. $\frac{1}{210}$, 210. $\frac{1}{211}$, 211. $\frac{1}{212}$, 212. $\frac{1}{213}$, 213. $\frac{1}{214}$, 214. $\frac{1}{215}$, 215. $\frac{1}{216}$, 216. $\frac{1}{217}$, 217. $\frac{1}{218}$, 218. $\frac{1}{219}$, 219. $\frac{1}{220}$, 220. $\frac{1}{221}$, 221. $\frac{1}{222}$, 222. $\frac{1}{223}$, 223. $\frac{1}{224}$, 224. $\frac{1}{225}$, 225. $\frac{1}{226}$, 226. $\frac{1}{227}$, 227. $\frac{1}{228$

$$0 \subseteq \mathbb{Z}[5] + \alpha^{109} 0 \subseteq 0$$

$$\mathbb{Z}/5\mathbb{Z} + \alpha^{109} \mathbb{G} \subseteq \mathbb{G} \rightarrow \text{SPB}$$

$$0 \in \mathbb{Z}[5] \subseteq \mathbb{Q} \Rightarrow \mathbb{Z}[5] = 0$$

D

سورة النجم

- 210(μ) ? 1.200 m, $Q[S_m] = 0$ $Q[S_7] = 1$ 0.2210 μ

$$m = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \dots \cdot p_i^{a_i}$$

$\therefore \int f(x) dx$

$$Q[\xi_m] = Q[\xi_{p_1} \dots \xi_{p_r}] =$$

$$= Q[\zeta_{par}] \cdot \text{---} \cdot Q[\zeta_{par}]$$

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 84

$Q(z_1, a)$ $Q(z_2, a)$
 1/1000 1/1000
 $P_1 \rightarrow$ brown $P_2 \rightarrow$ brown
 10 10
 Q_1 Q_2

[illegible]

$$\begin{aligned} [Q(p_1^{a_1} - p_1^{a_2}) : Q] &= \varphi(p_1^{a_1}) (\cancel{\varphi(p_2^{a_2})} / \cancel{\varphi(p_2^{a_2})}) = \\ &= \varphi(p_1^{a_1} p_2^{a_2}) / \cancel{\varphi(p_2^{a_2})} \\ \Delta_{p_1^{a_1} p_2^{a_2}} &= \Delta_{p_1^{a_1}} \Delta_{p_2^{a_2}} \end{aligned}$$

$$\Rightarrow \sigma = \sum [\zeta_{p_1^{a_1} p_2^{a_2}}] = \sum [\zeta_{p_1^{a_1} p_2^{a_2}}]$$

$$\{Q(\zeta_m) : Q\} = \mathcal{P}_m, \quad - \text{Eq. 3.3.14}$$

$$O = \mathbb{Z}[\zeta_m]$$

$$p \mid m \Leftrightarrow \text{factor } p$$

$$\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^* \quad \text{2020 N}$$

$$\sigma|_{\mu} : \mu_{112} \rightarrow \mu_{112}$$

$$(\mathbb{Z}/2\mathbb{Z})^{\times} \quad (\mathbb{Z}/2\mathbb{Z})^{\times}$$

~~$\sigma \in \text{Aut}(\mathbb{Z}/m\mathbb{Z})$~~ , $\sigma \in \text{Aut}(\mathbb{Z}/m\mathbb{Z})$. $\mathbb{Z}/m\mathbb{Z}$ ነ. አውታሪ ወይ σ , ρ
• $\sigma \in (\mathbb{Z}/m\mathbb{Z})^*$, ከዚህ. $\sigma \in \text{Aut}(\mathbb{Z}/m\mathbb{Z})$

$1 \rightarrow (\mathbb{Z}/p\mathbb{Z})^{\times^2} \rightarrow (\mathbb{Z}/p\mathbb{Z})^{\times} \xrightarrow{\chi \mapsto \chi^2} 1$

[illegible]

$$\left(\frac{a}{p}\right) = (a)^{\frac{p-1}{2}} \pmod{p} \in \{\pm 1\}$$

אנחנו רוצים לראות $\left(\frac{a}{p}\right) = 0$ אם $p \mid a$.
 $\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{1}{p}\right)$

קשה לראות את זה ישירות. ננסה לראות את זה עבור $p=3, 5, \dots$

המשפט 1.3.3
 יהי p ראשוני

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right)$$

אם p ראשוני, $L/\mathbb{Q}$ שדה מסתובב, אז $\text{Gal}(L/\mathbb{Q})$ הוא קבוצת סימטריות של L מעל $\mathbb{Q}$.

$$\sigma \in \text{Gal}(L/\mathbb{Q})$$

$$\sigma(x) = x^2 \text{ עבור } x \in \mathbb{Q}$$

$$(x \mapsto x^2) \in \text{Gal}(L(\sqrt{2})/\mathbb{Q})$$

אם $\sigma \in \text{Gal}(L/\mathbb{Q})$ אז σ הוא איזומורפיזם של שדות. נניח $\sigma \in \text{Gal}(L/\mathbb{Q})$ אז σ הוא איזומורפיזם של שדות.

$$\sigma = \text{Frob}_{\mathbb{Q}, L}$$

$$E(p) = (-1)^{\frac{p-1}{2}}$$

אם p ראשוני, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ שדה מסתובב, אז $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \mathbb{Z}/(p-1)\mathbb{Z}$$

$$\text{Frob}_{\mathbb{Q}, \mathbb{Q}(\zeta_p)} = \zeta_p$$

$$\sum \text{Frob}_{\mathbb{Q}, L} = \sum \zeta_p^i \text{ (mod } p)$$

$$\sum \zeta_p^i = \sum \zeta_p^i \text{ (mod } p)$$

$$\text{Frob}_{\mathbb{Q}, L} = \zeta_p$$

$$\begin{array}{c} \mathbb{Q}(\zeta_p) \\ (\mathbb{Z}/p\mathbb{Z})^{\times-1} \\ \downarrow \\ \mathbb{Q} \end{array}$$

ד = $E(p)p$ - נכס
- ע"מ

$$\left(\frac{e_{\mathbb{Q}}}{q}\right) \cdot \left(\frac{p}{f}\right) = \left(\frac{e(p)}{f}\right) = \text{Frob}_{\mathbb{Z}, \mathbb{Q}(\sqrt{p})} = \left(\frac{p}{f}\right)$$

المسألة

$$\left(\frac{1}{p}\right)\left(\frac{p}{p}\right) = \left(\frac{1}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{p-1}{2}}$$

ਜਾਂਤਾ ਨਿਰਪੱਖ 'ਤੇਲ' ਦੇਣਾ

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \quad - \quad \varphi: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/k\mathbb{Z}$$

$\partial''N$ r_0 , n RNN BNN $I^N - V$

- $\{u_1, \dots, u_n\}$ - פ'ח'ס'ו

$$C_i = \{ \sum_{j=1}^n a_j u_j \mid 0 \leq a_j \leq r_j \}, \text{Vol}(C) = r_1 \cdots r_n$$

$-y_i$ जो $0 > u_1, \dots, u_n$ से



$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = A \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

541

$$G' = \left\{ \sum_{i=1}^n r_i v_i \mid 0 \leq r_i \leq a_i \right\}$$



$$v_0 \in CC' = |\det(\Lambda)| \cdot a_1 \cdots a_n$$

ל' תר"פ

מבט: מה שיש לי - זהו

$$\mathcal{L} = v_1 \mathbb{Z} + \dots + v_n \mathbb{Z}$$

$k=u$ את כל ה- n של $\sum_{i=1}^n u_i = n$

2. $\lim_{n \rightarrow \infty} (v_1, \dots, v_n) = v$ is not true

2) $\forall i \in \{1, \dots, n\}$ et

5. מתייחדות, המלמד, וימים, מן, $\sum (L_n)$ (מחזק)

ולכן $\pm 1 =$ רציונל

מגדל ת 7321 - נעלם ה שלם יש ע, עב מנהל

המס' 310' (המס' 4/1000) - חלק

$$T = \{ \sum_{i=1}^n r_i v_i \mid 0 \leq r_i < 1 \}$$



$$\text{Vol}(T) = \text{Vol}(L) - \text{הנפח של } T \text{ שמתחת ל-} L$$

צדקה: יהי L מרחב T, K ונחשב $\text{Vol}(L)$ ונחסר את הנפח של T שמתחת ל- L .

$$V = \bigcup_{x \in L} \{x + T\}$$

הצדקה: לכל $a \in \mathbb{R}$ נחשב $a = n + r$ כאשר $n \in \mathbb{Z}$ ו- $0 \leq r < 1$. נראה ש- $a \in V$, כלומר a שייך ל- V .

$$a = \sum_{i=1}^n a_i v_i = \sum_{i=1}^n n_i v_i + \sum_{i=1}^n r_i v_i$$

□ $\sum_{i=1}^n n_i v_i \in L$ (כי L הוא מרחב) ו- $\sum_{i=1}^n r_i v_i \in T$ (כי $0 \leq r_i < 1$). לכן $a \in L + T = V$.

הצדקה: נראה ש- $V = L + T$. נניח $x \in V$. אז $x = y + z$ עבור $y \in L$ ו- $z \in T$. לכן $x \in L + T$.

משפט: L הוא מרחב $\Leftrightarrow V$ הוא מרחב. (כלומר, L הוא מרחב אם ורק אם V הוא מרחב).

הוכחה: נניח L הוא מרחב. נראה ש- V הוא מרחב.

$$\left| \text{Vol}(L \cap L) \right| = \left| \sum_{i=1}^n r_i v_i \mid \sum_{i=1}^n r_i v_i \right| \leq \sum_{i=1}^n (2r_i) v_i \leq \sum_{i=1}^n 2v_i = 2 \sum_{i=1}^n v_i < \infty$$

לכן, L הוא מרחב.

נניח V הוא מרחב. נראה ש- L הוא מרחב.

$$L \cap L = \{ \sum_{i=1}^n r_i v_i \mid 0 \leq r_i < 1 \} = T$$

(כי L הוא מרחב, לכן $L \cap L = L$).

הינן $|x|, u=av$, אם $u \in L \cap U_{(n)}$ נניח

היה, $u \in L$ נניח, $u \in L$ אז $u \in L$, $u \in L$, $u \in L$

הכלל

$$x = u + y, u \in \mathbb{Z}, y \in [0, 1)$$

הכלל

$$L \ni u - uu = yu \Rightarrow y = 0$$

הכלל, כעת כל סעיף

הכלל, כעת כל סעיף $\dim L \neq \dim V$ אז $\dim L < \dim V$

הכלל, כעת כל סעיף $\dim L < \dim V$ אז $\dim L < \dim V$

$$L_0 = L \cap V_0, V_0 = B_{v_1} + \dots + B_{v_{n-1}}$$

$$L_0 = \sum u_i + \dots + \sum u_{n-1}$$

$$\lambda = \sum_{i=1}^{n-1} r_i u_i + r_n u_n \in L$$

$$r_i = 0 \text{ (אם } i \neq n), r_n = 1$$

הכלל, כעת כל סעיף

$$L \ni u_1, \dots, u_{n-1}, \lambda$$

הכלל 12

הכלל, כעת כל סעיף $\dim L < \dim V$ אז $\dim L < \dim V$

הכלל, כעת כל סעיף $\dim L < \dim V$ אז $\dim L < \dim V$

$$\frac{x+y}{2} \in X \text{ אז } x, y \in X$$

$$\frac{x+y}{2} \in X \text{ אז } x, y \in X$$

הכלל, כעת כל סעיף

$$\dim L \leq \dim V$$

$$\phi \neq \lambda + \tau \text{ אז } \phi \neq \lambda + \tau$$