

Assignatura: **STRUCTURES**

Estudiant/

Data: **08/05/2021**

①

a) El polinomi $g(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ és irreductible $\Leftrightarrow$ no té anells i no és producte de dos irreductibles de grau 2.

• No té anells: en $\mathbb{F}_2$ només hi ha 2 elements, el 0 i el 1.

$$\left. \begin{aligned} g(0) &= 0 + 0 + 1 = 1 \neq 0 \\ g(1) &= 1 + 1 + 1 = 3 \bmod 2 = 1 \neq 0 \end{aligned} \right\} \Rightarrow g(x) \text{ no té anells.}$$

• Els irreductibles de $\mathbb{F}_2[x]$ de grau 2 són els polinomis de grau 2 que no tenen anells $\Rightarrow$ són els polinomis de grau 2 amb

3 coeficients $\neq 0$ i que tenen terme independent 1 $\Rightarrow$ l'única irreductible de grau 2 és $g(x) = 1 + x + x^2$

$$(1 + x + x^2)(1 + x + x^2) = 1 + x + x^2 + x + x^2 + x + x^2 + x^3 + x^3 + x^4 = 1 + x^2 + x^4 \neq g(x) \Rightarrow g(x) \text{ no és producte d'irreductibles de grau 2}$$

$\Rightarrow g(x)$ irreductible a $\mathbb{F}_2[x]$.

b) Tenim que $z \in \overline{\mathbb{F}_2} \Rightarrow z \text{ alg. } / \mathbb{F}_2$ i a més sabem que z és una anel de $g(x) \Rightarrow g(z) = z^4 + z + 1 = 0$

Sabem que el grup multiplicatiu d'un cos és un grup abelià $\Rightarrow$ com que $\mathbb{F}_2(z)$ és un cos $\mathbb{F}^* = \mathbb{F}_2(z)^*$ és abelià. Hem vist a classe que tot grup abelià que sigui el grup multiplicatiu d'un cos finit és cíclic.

$$\mathbb{F}_2(z) \text{ és finit ja que } z \text{ alg. } / \mathbb{F}_2 \Rightarrow \mathbb{F}_2(z) \simeq \mathbb{F}_2[x] / (g(x)) =$$

$$= \langle a_0 + a_1x + a_2x^2 + a_3x^3 : a_i \in \mathbb{F}_2 \rangle \Rightarrow |\mathbb{F}_2(z)| = 4 \cdot 2 = 8$$

$$\Rightarrow \mathbb{F}^* \text{ és cíclic i com que } z \in \mathbb{F}^* \text{ ja que } \frac{1}{z} \in \mathbb{F}_2(z) \Rightarrow \mathbb{F}^* = \langle z \rangle.$$

$$\text{Observem que si } |\mathbb{F}| = 8 \Rightarrow |\mathbb{F}^*| = 7 = |\langle z \rangle|$$

c) É uma ação já que: $\bullet$ e de $\mathbb{Z}/32\mathbb{Z}$ addition of $\mathbb{Z}/32\mathbb{Z}$

$$0 * x = x^2 = x^1 = x$$

$$e^{a+b} \cdot x = x^{a+b} = x^a \cdot x^b = (x^a)^b = (x^b)^a = x^{ab}$$

$$= a * x^2 = a * (b * x)$$

d) Les orbites de l'action sont de la forme : $\mathbb{Z}/3\mathbb{Z} \cdot D = \{a * D : a \in \mathbb{Z}/3\mathbb{Z}\}$
 $= \{D^2 : a \in \mathbb{Z}/3\mathbb{Z}\}$

Sabem que aquestes òrbites ens donen una partició de $\mathbb{F} = \mathbb{F}_2(\mathbb{Z})$.

$$F = F^* \cup \langle \sigma \rangle$$

$0 = 0 \Rightarrow 0 = 0 \Rightarrow 0 \neq 0 = 0^2 \Rightarrow A \Rightarrow$ l'élément 0 est un ~~élément~~

o si $\alpha \neq 0 \Rightarrow \alpha \in \mathbb{F}^* \Rightarrow D = \mathbb{Z}^n$. Tenim que els elements de

$$\mathbb{Z}/32\mathbb{Z} \cdot \mathbb{Z}^m \text{ nicht is } \mathbb{Z}^m \text{ t.g. } \mathbb{Z}^m = (\mathbb{Z}^m)^{\mathbb{Z}^a} = \mathbb{Z}^{m \cdot a} \text{ für alle } m$$

$a \in \mathbb{Z}/32\mathbb{Z}$. Això passa si $m \equiv m^a \pmod{\text{ord}(z)}$ i sabem

que l'ordre de $\mathbb{Z}_{55}$ $\bar{7} = |\mathbb{F}|$. Per tant els elements d'aquesta àlgebra són $\mathbb{Z}^m$ t. q. $m \equiv n^a \pmod{7}$ per algun $a \in \mathbb{Z}/32\mathbb{Z}$

e) El grup d'isotrofia de $\mathbb{Z}$ és $\mathbb{Z}/32\mathbb{Z} = \{a \in \mathbb{Z}/32\mathbb{Z} : a * \mathbb{Z} = \mathbb{Z}\} = \{a \in \mathbb{Z}/32\mathbb{Z} : \mathbb{Z}^a = \mathbb{Z}\}$.

Com que $F^{\lambda} = \langle Z \rangle$ cúbica $\Rightarrow \text{ord}(Z) = |F^{\lambda}| = 7$

$$\Rightarrow z^4 = z \Leftrightarrow z^{4-1} = 1 \Leftrightarrow z^{2^2-1} = 1 \Leftrightarrow z^{2^2-1} \equiv 1 \pmod{2^2-1} \quad \checkmark$$

$$\Rightarrow \mathcal{A}/\mathcal{B} \equiv \{a \in \mathcal{A} \mid b \in \mathcal{B}\}.$$

8) Para a seguinte afirmação: $(F)^a = \{x \in F : a \cdot x = x\}$ é um subgrupo de F

Wien Que :

verilen que :
 $\bullet 0, 1 \in (F)^a$ için $a * e = e^{2^a} = \begin{cases} e = 1 : 1^{2^a} = 1 \\ 0 = e : 0^{2^a} = 0 \end{cases}$

$$\bullet x, y \in (F)^a \Rightarrow a * (x, y) = (x, y)^a = x^a y^a$$

$$\bullet x, y \in (F)^a \Rightarrow a \ast (x+y) = (x+y)^a = x^a + y^a \quad \text{r}$$

no se com-ja aquest per país i ha de veure amb.

new ones.

Assignatura:

ESTRUCTURES

Estudiant/a

Data:

08/02/2021

1

$$8) (F)^2 = \{x \in F : x^4 = x\} \quad x^4 = x \Rightarrow \begin{cases} x = 0 \\ x^3 = 1 \end{cases}$$

$$x^3 = 1 \text{ si } \text{ord}(x) \mid 3 \Rightarrow \begin{cases} \text{ord}(x) = 3 \\ \text{ord}(x) = 1 \end{cases} \text{ però els ordres dels elements d'un}$$

grup cíclic han de dividir el cardinal del grup $\Rightarrow$ com que $3 \nmid 7$

$$\Rightarrow \text{ord}(x) = 1 \wedge (F)^2 = \{0, 1\} \text{ només té 2 elements.}$$

ESTRUCTURES ALGEBRAIQUES

Assignatura:

Estudiant/a

Data: 08/10/2021

2) Sabem que $100 = 2^2 \cdot 5^2$ i volem un grup abelià de cardinal

a) 100. El nostre grup tindrà 2-subgrups de Sylow i 5-subgrups de Sylow.

$$\left. \begin{array}{l} n_2 \equiv 1 \pmod{2} \\ n_2 | 5^2 = 25 \end{array} \right\} \Rightarrow n_2 = \{1, 5, 25\}$$



$$\left. \begin{array}{l} n_5 \equiv 1 \pmod{5} \\ n_5 | 2^2 = 4 \end{array} \right\} \Rightarrow n_5 = 1$$

Si sabem que el grup sigui abelià aleshores tots els subgrups han de ser normals $\Rightarrow n_2 = 1$ i $n_5 = 1$.

Tenim $|H_2| = 4$ i el grup abelià $\Rightarrow H_2 \cong \mathbb{Z}/4\mathbb{Z}$ o $H_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$|H_5| = 25$ i el grup abelià $\Rightarrow H_5 \cong \mathbb{Z}/25\mathbb{Z}$ o $H_5 \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Com que $n_2 = 1 = n_5$ sabem que $G = H_2 \times H_5$. Si volem que tots els elements de G tinguin ordre divisió de 10 $\Rightarrow$

Si $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \Rightarrow$ hi ha un element d'ordre 100 ∇ ?

Si $\otimes G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \Rightarrow$ hi ha un element d'ordre 20 ∇

Si $G \cong \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \Rightarrow$ hi ha un element d'ordre 50 ∇

$\Rightarrow G$ no es pot ser $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ que pel T. Cauchy és isomorfa $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, i per tant tot element ha de tenir ordre divisible per 10.

Ⓐ Pel T. Cauchy $\ncong \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \Rightarrow$ element d'ordre 20 $= \text{lcm}(20, 5)$

Ⓑ Pel T. Cauchy $\cong \mathbb{Z}/50\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \Rightarrow$ element d'ordre 50 $= \text{lcm}(50, 2)$.

1.5

1.5

b) Els elements de S_5 són, descomposats en cicles disjunts, les "multiplicació" de $(a_1 \dots a_j)$ $j=1, \dots, 5$, i.e. cicles de mida 1, 2, 3, 4, 5

Com que són cicles disjunts poden tenir 0, 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, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000

$\Rightarrow$ l'ordre de l'element maximal de S_5 és: $\text{mcd}(5, \text{mcd}(4, 1), \text{mcd}(3, 2), \text{mcd}(3, 1), \text{mcd}(2, 1)) = \text{mcd}(5, 4, 6, 3, 2) = \text{mcd}(5, 4, 6) = 5 \cdot 4 \cdot 3 = 60$

El centralitzador d'un element $\sigma \in S_5$ és:

$$C_{S_5}(\sigma) = \{ \gamma \sigma \gamma^{-1} : \gamma \in S_5 \}$$

$$\gamma \sigma \gamma^{-1} = \sigma \uparrow$$

Vull veure.

Assignatura: ESTRUCTURES ALGEBRAIQUES

Estudiant/

Data: 08/02/2021

③

a) $T(M) = \{m \in M : \exists a \in A \text{ } am = 0\}$

Com que $g: M \rightarrow N$ és un isomorfisme tenim que la imatge del 0 és menys el 0

$$g(am) = 0 \Leftrightarrow am = 0 \Leftrightarrow \underbrace{g(a)g(m)}_{\in N} = 0 \Rightarrow \underbrace{g(a)g(m)}_{\in T(N)} \in T(N)$$

~~$g(T(M)) \subseteq T(N)$~~ $\Rightarrow g(T(M)) \subseteq T(N)$

Si $am = 0$ com que g és isomorfisme $\exists g^{-1}: N \rightarrow M$ c.g.

$$\underbrace{g(a)}_{\in N} g^{-1}(m) = 0 \Rightarrow \underbrace{g^{-1}(m)}_{\in M} g^{-1}(a) \in T(M)$$

$$\Rightarrow \underbrace{g(T(M))}_{\subseteq T(N)} \subseteq T(M) \Rightarrow g(T(M)) \subseteq T(N)$$

$$\Rightarrow g(T(M)) = T(N)$$

Assignatura: ESTRUCTURES

Estudiant/a: [REDACTED]

Data: 08/01/2021

(4b)

Sigui $(b_0, b_2, \dots)$ l'expressió p-àdica de $x = \frac{1}{2}$. Tenim que si

$$x = \frac{1}{2} \Leftrightarrow 2x = 1, \text{ per tant}$$

$\dots b_3 b_2 b_1 b_0$	x
$\dots 0 0 0 1$	2

• A $\mathbb{Z}_7$ $2b_0 \equiv 1 \pmod{7} \Rightarrow b_0 = 4$ i m'én porta 1

$2b_1 + 1 \equiv 0 \pmod{7} \Rightarrow b_1 = 3$ i m'én porta 1

$2b_2 + 1 \equiv 0 \pmod{7} \Rightarrow b_2 = 3$ i m'én porta 1

$\vdots$

$2b_m + 1 \equiv 0 \pmod{7} \Rightarrow b_m = 3$ i m'én porta 1 $\forall m > 0$

$\Rightarrow (\dots 3334)$ és l'expressió p-àdica de $\frac{1}{2}$ a $\mathbb{Z}_7$

• A $\mathbb{Z}_{11}$ $2b_0 \equiv 1 \pmod{11} \Rightarrow b_0 = 6$ i m'én porta 1

$2b_1 + 1 \equiv 0 \pmod{11} \Rightarrow b_1 = 5$ i m'én porta 1

$2b_2 + 1 \equiv 0 \pmod{11} \Rightarrow b_2 = 5$ i m'én porta 1

$\vdots$

$2b_m + 1 \equiv 0 \pmod{11} \Rightarrow b_m = 5$ i m'én porta 1

$\Rightarrow (\dots 5556)$ és l'expressió p-àdica de $\frac{1}{2}$ a $\mathbb{Z}_{11}$