18.701: Problem Set 7

Dmitry Kaysin

April 2020

Problem 1

Determine the class equation of $\mathrm{GL}_3(\mathbb{F}_2)$, the group of invertible 3×3 matrices with entries modulo 2.
Of course, you need to determine the order of the group first. I suggest basing your analysis on the possible characteristic polynomials. There are four of them. Begin by finding nice matrices for each characteristic polynomial, but remember that the characteristic polynomial may not determine the conjugacy class. Note that the centralizer of a matrix A is equal to the centralizer of $I + A$. This can be used in the analysis of the matrices whose characteristic polynomials are t^3+t^2+1 or t^3+t+1, which are more complicated than the others.

We first find the order of general linear group $G = \mathrm{GL}_3(\mathbb{F}_2)$. There are $2^3 - 1 = 7$ ways to compose a nonzero row of a 3×3 matrix with entries from $\mathbb{F}_2$, which is the number of 3-combinations with repetition from $\mathbb{F}_2$ other than $(0, 0, 0)$. Fix the first row. The second row cannot be a multiple of the first row. Since the only non-zero element of $\mathbb{F}_2$ is 1, there are 6 ways to compose the second row. The third row cannot be a multiple of the first or the second row. Moreover, the third row cannot be a linear combination of the first two rows. We notice that a linear combination of the first two rows A^2 and a_2 cannot be a multiple of either A^2 or a_2 unless A^2 or a_2 is zero. Therefore there are only 4 ways to compose the third row. We conclude that there are $7 \cdot 6 \cdot 4 = 168$ ways to compose a 3×3 matrix with entries from $\mathbb{F}_2$. Therefore the order of G is 168.

Similar matrices are in the same conjugacy class. Moreover, similar matrices have the same characteristic polynomial. However, converse of the second proposition, in general, is not true.

Characteristic polynomial $p(t)$ of a matrix in $G = \mathrm{GL}_3(\mathbb{F}_2)$ must have degree

3 and cannot have a zero root. We list all possible $p(t)$:

$$t^3 + t^2 + t + 1, \tag{1}$$
$$t^3 + t^2 + 1, \tag{2}$$
$$t^3 + t + 1, \tag{3}$$
$$t^3 + 1. \tag{4}$$

Case 1. $p(t) = t^3 + t^2 + t + 1$**.** We notice that matrix

$$A = \begin{pmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{pmatrix}$$

has characteristic polynomial (1). Moreover, $A^4 = I$ and each A^2, A^3, I have characteristic polynomial (1).

Claim. All elements of a conjugacy class have the same order.

Proof. Let x, y be elements of a conjugacy class C of a group G. Without loss of generalty, let $y = g^{-1}xg$ for some $g \in G$. Let n be the order of x, then

$$y^n = (g^{-1}xg)^n = g^{-1}xg \cdots g^{-1}xg = g^{-1}x^n g = 1,$$

hence y also has order n. □

Since A^2 and A^3 have different order;

$$(A^2)^2 = I \quad \text{and} \quad (A^3)^4 = I,$$

they cannot be in the same conjugacy class. We also notice that A and A^3 are in the same conjugacy class since $A = P^{-1}A^3P$ for

$$P = \begin{pmatrix} 1 & & \\ & 1 & 1 \\ & & 1 \end{pmatrix}.$$

All $P \in Z(A^2)$ must satisfy

$$P^{-1}A^2P = A^2 \iff A^2P = PA^2.$$

Writing P with generic entries and A^2 explicitly, we must have:

$$A^2P = \begin{pmatrix} 1 & & 1 \\ & 1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} a+g & b+h & c+i \\ d & e & f \\ g & h & i \end{pmatrix},$$

and

$$PA^2 = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} 1 & & 1 \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} a & b & a+c \\ d & e & d+f \\ g & h & g+i \end{pmatrix},$$

therefore

$$a+g=a, \quad b+h=b, \quad c+i=a+c, \quad d+f=f, \quad g+i=i,$$

and

$$g=0, \quad h=0, \quad a=i, \quad d=0.$$

Therefore $P \in Z(A^2)$ must have form

$$P = \begin{pmatrix} a & b & c \\ & e & f \\ & & a \end{pmatrix}.$$

We notice that $a \neq 1, e \neq 1$, otherwise P would have determinant zero:

$$P = \begin{pmatrix} 1 & b & c \\ & 1 & f \\ & & 1 \end{pmatrix}.$$

There are $2^3 = 8$ matrices of this form in G, including the identity matrix I and A^2 itself. Therefore $|Z(A^2)| = 8$ and the order of the conjugacy class of A^2 is $|C(A^2)| = |G|/|Z(A^2)| = 168/8 = 21$.

We then examine matrix A^3 using the same approach. Writing $P \in Z(A^3)$ with generic entries and A^3 explicitly, we must have:

$$A^3P = \begin{pmatrix} 1 & 1 & \\ & 1 & 1 \\ & & 1 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} a+d & b+e & c+f \\ d+g & e+h & f+i \\ g & h & i \end{pmatrix},$$

and

$$PA^3 = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} 1 & 1 & \\ & 1 & 1 \\ & & 1 \end{pmatrix} = \begin{pmatrix} a & a+b & b+c \\ d & d+e & e+f \\ g & g+h & h+i \end{pmatrix},$$

therefore

$$a=e=i, \quad b=f, \quad g=0, \quad d=h=0.$$

Therefore $P \in Z(A^3)$ must have form

$$P = \begin{pmatrix} a & b & c \\ & a & b \\ & & a \end{pmatrix}.$$

We notice that $a \neq 1$, otherwise P would have determinant zero:

$$P = \begin{pmatrix} 1 & b & c \\ & 1 & b \\ & & 1 \end{pmatrix}.$$

There are $2^2 = 4$ matrices of this form in G, including the identity matrix I and A^3 itself. Therefore $|Z(A^3)| = 4$ and the order of the conjugacy class of A^3 is $|C(A^3)| = |G|/|Z(A^3)| = 168/4 = 42$.

Case 2. $p(t) = t^3 + t^2 + 1$**.** Matrix

$$B = \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & 1 \end{pmatrix}$$

has characteristic polynomial (2). Writing $P \in Z(B)$ with generic entries, we must have:

$$BP = \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & 1 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} d & e & f \\ g & h & i \\ a+g & b+h & c+i \end{pmatrix},$$

and

$$PB = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & 1 \end{pmatrix} = \begin{pmatrix} c & a & b+c \\ f & d & e+f \\ i & g & h+i \end{pmatrix},$$

therefore

$$c = d = h, \quad a = e, \quad g = f = b + c, \quad i = a + g = e + f, \quad b + h = g.$$

Therefore $P \in Z(B)$ must have form

$$P = \begin{pmatrix} a & b & c \\ c & a & b+c \\ b+c & c & a+b+c \end{pmatrix}.$$

Matrix P must have nonzero determinant. To make calculations more straightforward, we simplify the expression for $\det P$:

$$\begin{aligned} \det P &= a(a + ab + ac - c(b + c)) - b(ac + bc + c - (b + c)) + c(c - ab - ac) \\ &= a + ab + ac + abc + ac + abc + bc + bc + b + bc + c + abc + ac \\ &= a + b + c + ab + bc + ac + abc. \end{aligned}$$

We then calculate $\det P$ for all combinations of (a, b, c).

a	b	c	$\det P$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

All combinations of (a, b, c), except $(0, 0, 0)$, generate valid and distinct matrices $P \in Z(B)$. There are 7 such matrices. Therefore $|Z(B)| = 7$ and the order of the conjugacy class of B is $|C(B)| = |G|/|Z(B)| = 168/7 = 24$.

Case 3. $p(t) = t^3 + t + 1$**.** We notice that matrix

$$C = I + B \begin{pmatrix} 1 & 1 & \\ & 1 & 1 \\ 1 & & \end{pmatrix}$$

has characteristic polynomial (3).

Claim. Let X be a matrix in $\mathrm{GL}_n(\mathbb{F})$. Matrices X and $I + X$ have the same centralizer.

Proof. ($\Longrightarrow$) Suppose centralizer of X is $Z(X)$. Then for any $P \in Z(X)$: $P^{-1}XP = X$. Conjugate $I + X$ by P:

$$P^{-1}(I + X)P = P^{-1}IP + P^{-1}XP = I + X.$$

($\Longleftarrow$) Suppose centralizer of $I+X$ is $Z(I+X)$. Then for any $P \in Z(I+X)$: $P^{-1}(I + X)P = I + X$.

$$I + X = P^{-1}(I + X)P = I + P^{-1}XP,$$
$$X = P^{-1}XP.$$

□

Based on the above claim, matrix $C = I + B$ must have the same centralizer as B. Therefore conjugacy classes of C and B have the same order 24.

Case 4. $p(t) = t^3 + 1$**.** We notice that matrix

$$D = \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix}$$

has characteristic polynomial (4). Writing $Z(D)$ with generic entries, we must have:

$$DP = \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} g & h & i \\ a & b & c \\ d & e & f \end{pmatrix},$$

and

$$PD = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix} = \begin{pmatrix} b & c & a \\ e & f & d \\ h & i & g \end{pmatrix},$$

therefore

$$g = b = f, \quad c = h = d, \quad i = a = e.$$

Therefore $P \in Z(D)$ must have form

$$\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}$$

We notice that if $a = b = c$, then P is singular. We calculate $\det P$ for all combinations of (a, b, c), such that one of the variables a, b, or c is distinct from the other two.

a	b	c	$\det P$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

Therefore $|Z(D)| = 3$ and the order of the conjugacy class of D is $|C(D)| = |G|/|Z(D)| = 168/3 = 56$.

We calculate the sum of orders of all conjugacy classes we have found so far:

$$1 + 21 + 24 + 24 + 42 + 56 = 168 = |G|,$$

and conclude that there can be no other conjugacy classes in G. The class equation of G is

$$168 = 1 + 21 + 24 + 24 + 42 + 56.$$

Problem 2

With coordinates $x_1, \ldots, x_n$ in $\mathbb{R}^n$ as usual, the set of points defined by the inequalities $-1 \leq x_i \leq +1$, for $i = 1, \ldots, n$, is an n-dimensional hypercube $\mathcal{C}_n$. The 1-dimensional hypercube is a line segment and the 2-dimensional hypercube is a square. The 4-dimensional hypercube has eight face cubes, the 3-dimensional cubes defined by $\{x_i = 1\}$ and by $\{x_i = -1\}$, for $i = 1, 2, 3, 4$, and it has 16 vertices $(\pm 1, \pm 1, \pm 1, \pm 1)$.
Let G_n denote the subgroup of the orthogonal group O_n of elements that send hypercube to itself, the group of symmetries of $\mathcal{C}_n$, including the orientation-reversing symmetries. Permutations of the coordinates and sign changes are among the elements of G_n.
a) Determine the order of the group G_n.
b) Describe G_n explicitly, and identify the stabilizer of the vertex $(1, \ldots, 1)$.
Check your answer by showing that G_2 is isomorphic to the dihedral group D_4.

Denote $V_n = \{(a_1, a_2, \ldots, a_n) : a_i \in \{-1, 1\}\}$ the set of vertices of n-dimensional hypercube written in the standard basis.

Claim. Orthogonal matrix A is in G_n if and only if it permutes V_n.

Proof. ($\Longrightarrow$) Orthogonal operator A preserves length, therefore A maps corners of a hypercube (the farthest points from the origin) to corners. Since orthogonal operator is injective, A permutes corners of a hypercube.

($\Longleftarrow$) We prove that if orthogonal matrix A permutes V_n, then $A\big|_{\mathcal{C}_n}$ is injective and onto $\mathcal{C}_n$. Injectivity follows from injectivity of A.

Hypercube $\mathcal{C}_n$ is convex, therefore point p lies in $\mathcal{C}_n$ if and only if it can be represented as an affine combination of its corners V_n:

$$p = \sum_{v \in V_n} c_i v, \text{ and } \sum c_i = 1.$$

Consider image of p under A:

$$Ap = A \sum_{v \in V_n} c_i v = \sum_{v \in V_n} c_i A v.$$

Since A permutes V_n, Ap is an affine combination of V_n and, thus, a point of $\mathcal{C}_n$. Surjectivity follows via the same argument for A^{-1}.

□

Claim. Let A be an orthogonal matrix. A permutes V_n if and only if it has the form $A = SS$, where P is a permutation matrix and S is a diagonal matrix with ± 1 entries.

Proof. ($\Longrightarrow$) Suppose, A permutes V_n. There are 2^n elements in V_n, specifically all possible vectors of length n with entries in $\{-1, 1\}$. One can see that vectors in V_n span $\mathbb{R}^n$, therefore V_n must contain a set of n linearly independent vectors; denote it $C = \{v_1, v_2, \ldots, v_n\}$, which is a basis of $\mathbb{R}^n$. Let X be $n \times n$ matrix formed by vectors of C in the standard basis, i.e. $C = BX$. We note that X has integer entries.

Suppose map φ permutes V_n. Let $D = \varphi(C)$, another basis of $\mathbb{R}^n$. Let Y be a $n \times n$ matrix formed by vectors of D in the standard basis, i.e. $D = BY$. Since vectors in D are corners of a hypercube, entries of Y must be integers. Matrix of φ with respect to bases C and D is the identity matrix I. We change bases of the matrix of φ from C and D to the standard basis.

$$T = (Y^{-1})^{-1} I X^{-1} = Y X^{-1}$$

We note that matrix X has integer entries and determinant ± 1, thus it is invertible and its inverse has integer entries (Artin, Chapter 1, Exercise 6.2). Therefore matrix T has integer entries. It must also be orthogonal. Therefore in each of the columns of T there must be one ± 1 entry and the rest are zeroes. This is equivalent to the required decomposition $T = PS$.

($\Longleftarrow$) Let $A = PS$, as specified. To be a permutation of V_n, map $A\big|_{V_n}$ must be injective and onto V_n. Since A is orthogonal, it is injective, so its restriction to V_n is also injective. Consider arbitrary $v \in V_n$:

$$v = (\pm 1, \pm 1, \ldots, \pm 1)^t.$$

Since each row of A has only one nonzero entry (either -1 or 1), image of v under A must have the form

$$Av = (\pm 1, \pm 1, \ldots, \pm 1)^t,$$

which must be an element of V_n. Since V_n is finite, $A\big|_{V_n}$ must be onto V_n. Hence, A is a permutation of V_n.

□

Therefore elements of G_n are exactly $n \times n$ signed permutation matrices. The number of possible matrices P is $n!$; the number of possible matrices S is 2^n. Hence, the number of possible matrices $SP \in G_n$ and, therefore, the order of G_n is $n! \cdot 2^n$.

Denote vertex $p = (1, 1, \ldots, 1)$. Stabilizer of p, denote it G_p, includes matrices in G_n with non-negative entries. We notice that each matrix in G_p corresponds to a permutation of the columns (rows) of an identity matrix. Therefore G_p is isomorphic to S_n. Order of G_p is $n!$. Matrices in G_p can be either orientation preserving or orientation reversing isometries, which corresponds to even and odd permutations in S_n.

For the case of $n = 2$ the order of G_2 is equal to $2! \cdot 2^2 = 8$. There are five groups of order 8, but only two of them are non-abelian: D_4, dihedral group, and Q, quaternion group. Quaternion group has only one element of order 2. However, G_2 has five elements of order 2: 180° rotation, two reflections about centers of opposite sides, two reflections about diagonal lines. Therefore G_w is isomorphic to a dihedral group D_4.

Problem 3

Determine the class equations of S_6 and A_6.

Order of symmetric group S_6 is $6! = 720$. By Artin, Proposition 7.5.1, two elements of the symmetric group are conjugate if and only if their cycle decompositions have the same structure. Structure of the cycle decomposition of an element of S_6 corresponds to a partition of the set of 6 elements $\mathcal{S} = \{1, 2, 3, 4, 5, 6\}$. We list all combinations of possible lengths of cycles for 6 elements, each combination representing a conjugacy class, and calculate the number of distinct elements in each class.

Structure of cycle decomposition	Order of conjugacy class
$\{1,1,1,1,1,1\}$	1
$\{1,1,1,1,2\}$	$\binom{6}{2} = 15$
$\{1,1,1,3\}$	$\frac{6!}{(6-3)!\cdot 3} = 40$
$\{1,1,2,2\}$	$\binom{6}{2}\binom{4}{2}\frac{1}{2} = 45$
$\{1,1,4\}$	$\frac{6}{(6-4)!\cdot 4} = 90$
$\{1,2,3\}$	$\binom{6}{2}\frac{4!}{(4-3)!\cdot 3} = 120$
$\{1,5\}$	$\frac{6!}{(6-5)!\cdot 5} = 144$
$\{2,2,2\}$	$\binom{6}{2}\cdot\binom{4}{2}\frac{1}{6} = 15$
$\{2,4\}$	$\binom{6}{2}\frac{4!}{(4-4)!\cdot 4} = 90$
$\{3,3\}$	$\frac{6!}{(6-3)!\cdot 3}\frac{3!}{(3-3)!\cdot 3}\frac{1}{2} = 40$
$\{6\}$	$\frac{6!}{(6-6)!\cdot 6} = 120$

Therefore, class equation of S_6 is:

$$|S_6| = 720 = 1 + 15 + 15 + 40 + 40 + 45 + 90 + 90 + 120 + 120 + 144.$$

Alternating group A_6 is a group of even permutations. A_6 has order $6!/2 = 360$. Elements that have even number of disjoint transpositions are even. Cycle of odd length can be represented as an even number of transpositions; cycle of even length can be represented as an odd number of transpositions. Therefore, A_6 includes elements with the following lengths of cycle decomposition:

$$\{1,1,1,1,1,1\}, \quad \{1,1,1,3\}, \quad \{1,1,2,2\}, \quad \{1,5\}, \quad \{2,4\}, \quad \{3,3\}.$$

In A_6, unlike S_6, structure of a cycle decomposition may not correspond to a single conjugacy class. For example, (12345) and (15342) are conjugates in S_6 since $(15)(24)(23)\cdot(12345)\cdot(23)(24)(15) = (15342)$ but they are not conjugates in A_6.

Identity element is in its own conjugacy class. By Artin, Lemma 7.5.5b we know that 3-cycles form a single conjugacy class in A_6, therefore order of the conjugacy class of 3-cycles in A_6 is 40, the same as in S_6.

For cases $\{1,1,2,2\}$ and $\{1,1,2,2\}$ we choose two elements $q, q' \in A_6$, both with either structure of the cycle decomposition. Since q and q' are conjugates in S_6, $q' = pqp^{-1}$ for some $p \in S_6$. If p is even, then q and q' are conjugates in A_6

as well. If p is odd, we notice that $q' = (p\tau)q(p\tau)^{-1}$ where τ is a transposition, disjoint from q. We can see that if p is odd, then $p\tau$ is even, and we have that q and q' are conjugates in A_6.

For case $\{1, 5\}$ we will first prove that all elements in the stabilizer of a 5-cycle in S_6 are even. Let q be an arbitrary 5-cycle. Order of $Z(q)$ in S_6 is prime $(720/144 = 5)$, thus $Z(q)$ must be a cyclic subgroup of S_6. $Z(q)$ is generated by an even permutation, otherwise, with $Z(q) = \langle a \rangle$, a is odd implies that $a^5 = 1$ is odd, which is not the case. Therefore, all elements of $Z(q)$ are even and any given 5-cycle has a stabilizer of order 5. From this we can see that conjugacy class of any 5-cycle in A_6 has order $360/5 = 72$. In total, there are 144 distinct 5-cycles in A_6. Since conjugacy classes partition the group, there are exactly two conjugacy classes in A_6 with cycle structure $\{1, 5\}$, each of order 72.

Now we consider permutations with cycle structure $\{2, 4\}$. Without loss of generality, let $q = (12)(3456)$ be permutation with such cycle structure. Centralizer of q in S_6 includes both even and odd permutations, for example (12) and identity. Since $Z(q) < S_6$ is a group and even permutations form the kernel K of the sign homomorphism $Z(q) \to \{-1, 1\}$, the order of K is half that of the order of $Z(q) < S_6$ by the First Isomorphism Theorem. Order of $Z(q) < S_6$ is $720/90 = 8$. Therefore, the order of $K = Z(q) < A_6$ is $8/2 = 4$. The order of the conjugacy class of permutations in A_6 with cycle structure $\{2, 4\}$ is thus $360/4 = 90$, the same as in S_6.

This applies to any permutation with cycle structure that commutes with some odd permutation. For example, centralizer of any permutation q with cycle structure $\{3, 3\}$ includes both even and odd permutations. For example, $(123)(456)$ commutes with $(14)(25)(36)$. Therefore, the order of $Z(q) < A_6$ is half that of the order of $Z(q) < S_6$ and is equal to $(720/40)/2 = 9$. The order of the conjugacy class of permutations with cycle structure $\{3, 3\}$ is thus $360/9 = 40$.

Therefore, class equation of A_6 is:

$$|A_6| = 360 = 1 + 40 + 40 + 45 + 72 + 72 + 90.$$