(*November 18, 2023*)

Discussion 04

Paul Garrett garrett@umn.edu https://www-users.cse.umn.edu/~garrett/

[04.1] Given a 3-by-3 matrix M with integer entries, find A, B integer 3-by-3 matrices with determinant ± 1 such that AMB is diagonal.

Let's give an *algorithmic*, rather than *existential*, argument this time, saving the existential argument for later.

First, note that given two integers x, y, not both 0, there are integers r, s such that $g = \gcd(x, y)$ is expressible as $g = rx + sy$. That is,

$$(\, x \quad y \,) \begin{pmatrix} r & * \\ s & * \end{pmatrix} = (\, g \quad * \,)$$

What we want, further, is to figure out what other two entries will make the second entry 0, *and* will make that 2-by-2 matrix invertible (in $GL_2(\mathbb{Z})$). It's not hard to guess:

$$(\, x \quad y \,) \begin{pmatrix} r & -y/g \\ s & x/g \end{pmatrix} = (\, g \quad 0 \,)$$

Thus, given $(x\ y\ z)$, there is an invertible 2-by-2 integer matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that

$$(\, y \quad z \,) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (\, \gcd(y, z) \quad 0 \,)$$

That is,

$$(\, x \quad y \quad z \,) \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} = (\, x \quad \gcd(y, z) \quad 0 \,)$$

Repeat this procedure, now applied to x and $\gcd(y, z)$: there is an invertible 2-by-2 integer matrix $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ such that

$$(\, x \quad \gcd(y, z) \,) \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = (\, \gcd(x, \gcd(y, z)) \quad 0 \,)$$

That is,

$$(\, x \quad \gcd(y, z) \quad 0 \,) \begin{pmatrix} a' & b' & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix} = (\, \gcd(x, y, z) \quad 0 \quad 0 \,)$$

since *gcd*s can be computed iteratively. That is,

$$(\, x \quad y \quad z \,) \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} \begin{pmatrix} a' & b' & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix} = (\, \gcd(x, y, z) \quad 0 \quad 0 \,)$$

Given a 3-by-3 matrix M, *right*-multiply by an element A_1 of $GL_3(\mathbb{Z})$ to put M into the form

$$MA_1 = \begin{pmatrix} g_1 & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix}$$

where (necessarily!) g_1 is the *gcd* of the top row. Then *left*-multiply by an element $B_2 \in GL_3(\mathbb{Z})$ to put MA into the form

$$B_2 \cdot MA_1 = \begin{pmatrix} g_2 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$$

where (necessarily!) g_2 is the *gcd* of the left column entries of MA_1. Then right multiply by $A_3 \in GL_3(\mathbb{Z})$ such that

$$B_2MA_1 \cdot A_3 = \begin{pmatrix} g_3 & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix}$$

where g_3 is the *gcd* of the top row of B_2MA_1. Continue. Since these *gcd*s divide each other successively

$$\dots |g_3|g_2|g_1 \neq 0$$

and since any such chain must be finite, after finitely-many iterations of this the upper-left entry ceases to change. That is, for some $A, B \in GL_3(\mathbb{Z})$ we have

$$BMA = \begin{pmatrix} g & * & * \\ 0 & x & y \\ 0 & * & * \end{pmatrix}$$

and also g divides the top row. That is,

$$u = \begin{pmatrix} 1 & -x/g & -y/g \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in GL_3(\mathbb{Z})$$

Then

$$BMA \cdot u = \begin{pmatrix} g & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$$

Continue in the same fashion, operating on the lower right 2-by-2 block, to obtain a form

$$\begin{pmatrix} g & 0 & 0 \\ 0 & g_2 & 0 \\ 0 & 0 & g_3 \end{pmatrix}$$

Note that since the r, s such that $\gcd(x, y) = rx + sy$ can be found via Euclid, this whole procedure is *effective*. And it certainly applies to larger matrices, not necessarily square.

[04.2] Given a row vector $x = (x_1, \dots, x_n)$ of integers whose *gcd* is 1, prove that there exists an n-by-n integer matrix M with determinant ± 1 such that $xM = (0, \dots, 0, 1)$.

(*The iterative/algorithmic idea of the previous solution applies here, moving the gcd to the right end instead of the left.*)

[04.3] Given a row vector $x = (x_1, \dots, x_n)$ of integers whose *gcd* is 1, prove that there exists an n-by-n integer matrix M with determinant ± 1 whose bottom row is x.

This is a corollary of the previous exercise. Given A such that

$$xA = (\,0 \quad \dots \quad 0 \quad \gcd(x_1, \dots, x_n)\,) = (\,0 \quad \dots \quad 0 \quad 1\,)$$

note that this is saying

$$\begin{pmatrix} * & \dots & * \\ \vdots & & \vdots \\ * & \dots & * \\ x_1 & \dots & x_n \end{pmatrix} \cdot A = \begin{pmatrix} * & \dots & * & * \\ \vdots & & \vdots & \vdots \\ * & \dots & * & * \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} * & \dots & * \\ \vdots & & \vdots \\ * & \dots & * \\ x_1 & \dots & x_n \end{pmatrix} = \begin{pmatrix} * & \dots & * & * \\ \vdots & & \vdots & \vdots \\ * & \dots & * & * \\ 0 & \dots & 0 & 1 \end{pmatrix} \cdot A^{-1}$$

This says that x is the bottom row of the invertible A^{-1}, as desired.

[04.4] Show that $GL(2, \mathbb{F}_2)$ is isomorphic to the permutation group S_3 on three letters.

There are exactly 3 non-zero vectors in the space $\mathbb{F}_2^2$ of column vectors of size 2 with entries in $\mathbb{F}_2$. Left multiplication by elements of $GL_2(\mathbb{F}_2)$ permutes them, since the invertibility assures that no non-zero vector is mapped to zero. If $g \in GL_2(\mathbb{F}_2)$ is such that $gv = v$ for all non-zero vectors v, then $g = 1_2$. Thus, the map

$$\varphi : GL_2(\mathbb{F}_2) \to \text{permutations of the set } N \text{ of non-zero vectors in } \mathbb{F}_2^2$$

is *injective*. It is a group homomorphism because of the associativity of matrix multiplication:

$$\varphi(gh)(v) = (gh)v = g(hv) = \varphi(g)(\varphi(h)(v))$$

Last, we can confirm that the injective group homomorphism φ is also surjective by showing that the order of $GL_2(\mathbb{F}_2)$ is the order of S_3, namely, 6, as follows. An element of $GL_2(\mathbb{F}_2)$ can send any basis for $\mathbb{F}_2^2$ to any other basis, and, conversely, is completely determined by telling what it does to a basis. Thus, for example, taking the first basis to be the standard basis $\{e_1, e_2\}$ (where e_i has a 1 at the i^{th} position and 0s elsewhere), an element g can map e_1 to any non-zero vector, for which there are $2^2 - 1$ choices, counting *all* less 1 for the zero-vector. The image of e_2 under g must be linearly independent of e_1 for g to be invertible, and conversely, so there are $2^2 - 2$ choices for ge_2 (*all* less 1 for 0 and less 1 for ge_1). Thus,

$$|GL_2(\mathbb{F}_2)| = (2^2 - 1)(2^2 - 2) = 6$$

Thus, the map of $GL_2(\mathbb{F}_2)$ to permutations of non-zero vectors gives an isomorphism to S_3.

[04.5] Determine all conjugacy classes in $GL(2, \mathbb{F}_3)$.

First, $GL_2(\mathbb{F}_3)$ is simply the group of *invertible* k-linear endomorphisms of the $\mathbb{F}_3$-vectorspace $\mathbb{F}_3^2$. As observed earlier, conjugacy classes of endomorphisms are in bijection with $\mathbb{F}_3[x]$-module structures on $\mathbb{F}_3^2$, which we know are given by *elementary divisors*, from the Structure Theorem. That is, all the possible structures are parametrized by monic polynomials $d_1 | \dots | d_t$ where the sum of the degrees is the dimension of the vector space $\mathbb{F}_3^2$, namely 2. Thus, we have a list of irredundant representatives

$$\begin{cases} \mathbb{F}_3[x]/\langle Q \rangle & Q \text{ monic quadratic in } \mathbb{F}_3[x] \\ \mathbb{F}_3[x]/\langle x - \lambda \rangle \oplus \mathbb{F}_3[x]/\langle x - \lambda \rangle & \lambda \in \mathbb{F}_3^\times \end{cases}$$

We *can* write the first case in a so-called rational canonical form, that is, choosing basis $1, x \bmod Q$, so we have two families

$$\begin{cases} (1) & \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix} & b \in \mathbb{F}_3,\ a \in \mathbb{F}_3^\times \\ (2) & \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} & \lambda \mathbb{F}_3^\times \end{cases}$$

But the first family can be usefully broken into 3 sub-cases, namely, depending upon the reducibility of the quadratic, and whether or not there are repeated roots: there are 3 cases

$$\begin{array}{rcl} Q(x) & = & \text{irreducible} \\ Q(x) & = & (x-\lambda)(x-\mu) \quad (\text{with } \lambda \neq \mu) \\ Q(x) & = & (x-\lambda)^2 \end{array}$$

And note that if $\lambda \neq \mu$ then (for a field k)

$$k[x]/\langle (x-\lambda)(x-\mu)\rangle \approx k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle x-\mu\rangle$$

Thus, we have

$$\begin{cases} (1a) & \begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix} & x^2+ax+b \text{ irreducible in } \mathbb{F}_3[x] \\ (1b) & \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} & \lambda \neq \mu \text{ both nonzero} \qquad (\text{modulo interchange of } \lambda, \mu) \\ (1b) & \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} & \lambda \in \mathbb{F}_3^2 \\ (2) & \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} & \lambda \in \mathbb{F}_3^\times \end{cases}$$

One might, further, list the irreducible quadratics in $\mathbb{F}_3[x]$. By counting, we know there are $(3^2-3)/2 = 3$ irreducible quadratics, and, thus, the guesses x^2-2, x^2+x+1, and x^2-x+1 (the latter two being cyclotomic, the first using the fact that 2 is not a square mod 3) are all of them.

[04.6] Determine all conjugacy classes in $GL(3, \mathbb{F}_2)$.

Again, $GL_3(\mathbb{F}_2)$ is the group of *invertible* k-linear endomorphisms of the $\mathbb{F}_2$-vectorspace $\mathbb{F}_2^3$, and conjugacy classes of endomorphisms are in bijection with $\mathbb{F}_2[x]$-module structures on $\mathbb{F}_2^3$, which are given by *elementary divisors*. So all possibilities are parametrized by monic polynomials $d_1|\dots|d_t$ where the sum of the degrees is the dimension of the vector space $\mathbb{F}_2^3$, namely 3. Thus, we have a list of irredundant representatives

$$\begin{cases} (1) & \mathbb{F}_2[x]/\langle Q\rangle & Q \text{ monic cubic in } \mathbb{F}_2[x] \\ (2) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle \\ (3) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \end{cases}$$

since the only non-zero element of $\mathbb{F}_2$ is $\lambda = 1$. We *can* write the first case in a so-called rational canonical form, that is, choosing basis $1, x, x^2 \bmod Q$, there are three families

$$\begin{cases} (1) & \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -b \\ 0 & 1 & -a \end{pmatrix} & x^3+ax^2+bx+1 \text{ in } \mathbb{F}_2[x] \\ (2) & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \\ (3) & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{cases}$$

It is useful to look in detail at the possible factorizations in case 1, breaking up the single summand into more summands according to relatively prime factors, giving cases

$$\begin{cases} (1a) & \mathbb{F}_2[x]/\langle x^3+x+1\rangle \\ (1a') & \mathbb{F}_2[x]/\langle x^3+x^2+1\rangle \\ (1b) & \mathbb{F}_2[x]/\langle (x-1)(x^2+x+1)\rangle \\ (1c) & \mathbb{F}_2[x]/\langle (x-1)^3\rangle \end{cases}$$

since there are just two irreducible cubics x^3+x+1 and x^3+x^2+1, and a unique irreducible quadratic, x^2+x+1. (The counting above tells the number, so, after any sort of guessing provides us with the right number of check-able irreducibles, we can stop.) Thus, the 6 conjugacy classes have irredundant matrix representatives

$$(1a)\quad \begin{pmatrix} 0&0&1\\1&0&1\\0&1&0\end{pmatrix} \qquad (1a')\quad \begin{pmatrix} 0&0&1\\1&0&0\\0&1&1\end{pmatrix} \qquad (1b)\quad \begin{pmatrix} 1&0&0\\0&0&1\\0&1&1\end{pmatrix} \qquad (1c)\quad \begin{pmatrix} 1&0&0\\1&1&0\\0&1&1\end{pmatrix}$$

$$(2)\quad \begin{pmatrix} 1&0&0\\0&1&0\\0&1&1\end{pmatrix} \qquad (3)\quad \begin{pmatrix} 1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

[04.7] Determine all conjugacy classes in $GL(4,\mathbb{F}_2)$.

Again, $GL_4(\mathbb{F}_2)$ is *invertible* k-linear endomorphisms of $\mathbb{F}_2^4$, and conjugacy classes are in bijection with $\mathbb{F}_2[x]$-module structures on $\mathbb{F}_2^4$, given by *elementary divisors*. So all possibilities are parametrized by monic polynomials $d_1|\dots|d_t$ where the sum of the degrees is the dimension of the vector space $\mathbb{F}_2^4$, namely 4. Thus, we have a list of irredundant representatives

$$\begin{cases} \mathbb{F}_2[x]/\langle Q\rangle & Q \text{ monic quartic}\\ \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)Q(x)\rangle & Q \text{ monic quadratic}\\ \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle & \\ \mathbb{F}_2[x]/\langle Q\rangle \oplus \mathbb{F}_2[x]/\langle Q\rangle & Q \text{ monic quadratic}\\ \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle & \end{cases}$$

since the only non-zero element of $\mathbb{F}_2$ is $\lambda=1$. We could write all cases using rational canonical form, but will not, deferring matrix forms till we've further decomposed the modules. Consider possible factorizations

into irreducibles, giving cases

$$\begin{cases} (1a) & \mathbb{F}_2[x]/\langle x^4+x+1\rangle \\ (1a') & \mathbb{F}_2[x]/\langle x^4+x^3+1\rangle \\ (1a'') & \mathbb{F}_2[x]/\langle x^4+x^3+x^2+x+1\rangle \\ (1b) & \mathbb{F}_2[x]/\langle (x-1)(x^3+x+1)\rangle \\ (1b') & \mathbb{F}_2[x]/\langle (x-1)(x^3+x^2+1)\rangle \\ (1c) & \mathbb{F}_2[x]/\langle (x-1)^2(x^2+x+1)\rangle \\ (1d) & \mathbb{F}_2[x]/\langle (x^2+x+1)^2\rangle \\ (1e) & \mathbb{F}_2[x]/\langle (x-1)^4\rangle \\ (2a) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)(x^2+x+1)\rangle \\ (2b) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^3\rangle \\ (3) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle \\ (4a) & \mathbb{F}_2[x]/\langle x^2+x+1\rangle \oplus \mathbb{F}_2[x]/\langle x^2+x+1\rangle \\ (4b) & \mathbb{F}_2[x]/\langle (x-1)^2\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle \\ (5) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \end{cases}$$

since there are exactly three irreducible quartics (as indicated), two irreducible cubics, and a single irreducible quadratic. Matrices are, respectively, and unilluminatingly,

$$\begin{bmatrix} 0&0&0&1\\ 1&0&0&1\\ 0&1&0&0\\ 0&0&1&0 \end{bmatrix} \begin{bmatrix} 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 0&0&0&1\\ 1&0&0&1\\ 0&1&0&1\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 0&0&0&1\\ 0&1&0&1\\ 0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 0&0&0&1\\ 0&1&0&0\\ 0&0&1&1 \end{bmatrix}$$

$$\begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 0&1&0&0\\ 1&1&0&0\\ 0&1&0&1\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 1&1&0&0\\ 0&1&1&0\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&1 \end{bmatrix}$$

$$\begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&1&1&0\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 0&1&0&0\\ 1&1&0&0\\ 0&0&0&1\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 1&1&0&0\\ 0&0&1&0\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{bmatrix}$$

[04.8] Tell a p-Sylow subgroup in $GL(3,\mathbb{F}_p)$.

To compute the order of this group in the first place, observe that an automorphism (invertible endomorphism) can take any basis to any other. Thus, letting e_1, e_2, e_3 be the standard basis, for an automorphism g the image ge_1 can be any non-zero vector, of which there are p^3-1. The image ge_2 can be anything not in the span of ge_1, of which there are $p^3 = p$. The image ge_3 can be anything not in the span

of ge_1 and ge_2, of which, because those first two were already linearly independent, there are $p^3 - p^2$. Thus, the order is

$$|GL_3(\mathbb{F}_p)| = (p^3-1)(p^3-p)(p^3-p^2)$$

The power of p that divides this is p^3. Upon reflection, a person might hit upon considering the subgroup of upper triangular *unipotent* (eigenvalues all 1) matrices

$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$

where the super-diagonal entries are all in $\mathbb{F}_p$. Thus, there would be p^3 choices for super-diagonal entries, the right number. By luck, we are done.

[04.9] Tell a 3-Sylow subgroup in $GL(3, \mathbb{F}_7)$.

As earlier, the order of the group is

$$(7^3-1)(7^3-7)(7^3-7^2) = 2^6 \cdot 3^4 \cdot 7^3 \cdot 19$$

Of course, since $\mathbb{F}_7^\times$ is cyclic, for example, it has a subgroup T of order 3. Thus, one might hit upon the subgroup

$$H = \{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} : a, b, c \in T \}$$

is a subgroup of order 3^3. Missing a factor of 3. But all the permutation matrices (with exactly one non-zero entry in each row, and in each column, and that non-zero entry is 1)

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

These normalize *all* diagonal matrices, and also the subgroup H of diagonal matrices with entries in T. The group of permutation matrices consisting of the identity and the two 3-cycles is order 3, and putting it together with H (as a semi-direct product whose structure is already described for us) gives the order 3^4 subgroup.

[04.10] Tell a 19-Sylow subgroup in $GL(3, \mathbb{F}_7)$.

Among the Stucture Theorem canonical forms for endomorphisms of $V = \mathbb{F}_7^3$, there are $\mathbb{F}_7[x]$-module structures

$$V \approx \mathbb{F}_7[x]/\langle \text{ irreducible cubic } C \rangle$$

which are *invertible* because of the irreducibility. Let α be the image of x in $\mathbb{F}_7[x]/\langle C \rangle$. Note that $\mathbb{F}_7[\alpha] = \mathbb{F}_7[x]/C$ also has a natural ring structure. Then the action of any $P(x)$ in $k[x]$ on V (via this isomorphism) is, of course,

$$P(x) \cdot Q(\alpha) = P(\alpha) \cdot Q(\alpha) = (P \cdot Q)(x) \text{mod } C(x)$$

for any $Q(x) \in \mathbb{F}_7[x]$. Since C is irreducible, there are no non-trivial zero divisors in the ring $\mathbb{F}_7[\alpha]$. Indeed, it's a field. Thus, $\mathbb{F}_7[\alpha]^\times$ *injects* to $\text{End}_{\mathbb{F}_7} V$. The point of saying this is that, therefore, if we can find an element of $\mathbb{F}_7[\alpha]^\times$ of order 19 then we have an *endomorphism* of order 19, as well. And it is arguably simpler to hunt around in side $\mathbb{F}_{7^3} = \mathbb{F}_7[\alpha]$ than in groups of matrices.

To compute anything explicitly in $\mathbb{F}_{7^3}$ we need an irreducible cubic. Luckily, $7 = 1 \text{mod } 3$, so there are many non-cubes mod 7. In particular, there are only 2 non-zero cubes mod 7, ± 1. Thus, $x^3 - 2$ has no linear factor

in $\mathbb{F}_7[x]$, so is irreducible. The *sparseness* (having not so many non-zero coefficients) of this polynomial will be convenient when computing, subsequently.

Now we must find an element of order 19 in $\mathbb{F}_7[x]/\langle x^3-2\rangle$. There seems to be no simple algorithm for choosing such a thing, but there is a reasonable probabilistic approach: since $\mathbb{F}_{7^3}^\times$ is cyclic of order $7^3-1 = 19\cdot 18$, if we pick an element g at random the probability is $(19-1)/19$ that its order will be *divisible* by 19. Then, whatever its order is, g^{18} will have order either 19 or 1. That is, if g^{18} is not 1, then it is the desired thing. (Generally, in a cyclic group of order $p\cdot m$ with prime p and p not dividing m, a random element g has probability $(p-1)/p$ of having order divisible by p, and in any case g^m will be either 1 or will have order p.)

Since elements of the ground field $\mathbb{F}_7^\times$ are all of order 6, these would be bad guesses for the random g. Also, the image of x has cube which is 2, which has order 6, so x itself has order 18, which is not what we want. What to guess next? Uh, maybe $g = x+1$? Can only try. Compute

$$(x+1)^{18} = (((x+1)^3)^2)^3 \bmod x^3-2$$

reducing modulo x^3-2 at intermediate stages to simplify things. So

$$g^3 = x^3+3x^2+3x+1 = 3x^2+3x+3 \bmod x^3-2 = 3\cdot(x^2+x+1)$$

A minor piece of luck, as far as computational simplicity goes. Then, in $\mathbb{F}_7[x]$,

$$g^6 = 3^2\cdot(x^2+x+1)^2 = 2\cdot(x^4+2x^3+3x^2+2x+1) = 2\cdot(2x+2\cdot 2+3x^2+2x+1)$$

$$= 2\cdot(3x^2+4x+5) = 6x^2+x+3 \bmod x^3-2$$

Finally,

$$g^{18} = (g^6)^3 = (6x^2+x+3)^3 \bmod x^3-2$$

$$= 6^3\cdot x^6 + (3\cdot 6^2\cdot 1)x^5 + (3\cdot 6^2\cdot 3 + 3\cdot 6\cdot 1^2)x^4 + (6\cdot 6\cdot 1\cdot 3 + 1^3)x^3 + (3\cdot 6\cdot 3^2 + 3\cdot 1^2\cdot 3)x^2 + (3\cdot 1\cdot 3^2)x + 3^3$$

$$= 6x^6+3x^5+6x^4+4x^3+3x^2+6x+6 = 6\cdot 4+3\cdot 2\cdot x^2+6\cdot 2x+4\cdot 2+3x^2+6x+6 = 2x^2+4x+3$$

Thus, if we've not made a computational error, the endomorphism given by multiplication by $2x^2+4x+3$ in $\mathbb{F}_7[x]/\langle x^3-2\rangle$ is of order 19.

To get a matrix, use (rational canonical form) basis $e_1 = 1$, $e_2 = x$, $e_3 = x^2$. Then the matrix of the endomorphism is

$$M = \begin{pmatrix} 3 & 4 & 1 \\ 4 & 3 & 4 \\ 2 & 4 & 3 \end{pmatrix}$$

Pretending to be brave, we check by computing the 19^{th} power of this matrix, modulo 7. Squaring repeatedly, we have (with determinants computed along the way as a sort of parity-check, which in reality did discover a computational error on each step, which was corrected before proceeding)

$$M^2 = \begin{pmatrix} 1 & 0 & 6 \\ 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} \quad M^4 = \begin{pmatrix} 6 & 3 & 2 \\ 1 & 6 & 3 \\ 5 & 1 & 6 \end{pmatrix} \quad M^8 = \begin{pmatrix} 0 & 4 & 2 \\ 1 & 0 & 4 \\ 2 & 1 & 0 \end{pmatrix} \quad M^{16} = \begin{pmatrix} 6 & 5 & 5 \\ 6 & 6 & 5 \\ 6 & 6 & 6 \end{pmatrix}$$

Then

$$M^{18} = M^2\cdot M^{16} = \begin{pmatrix} 1 & 0 & 6 \\ 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}\cdot M^{16} = \begin{pmatrix} 6 & 5 & 5 \\ 6 & 6 & 5 \\ 6 & 6 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 4 & 0 & 1 \\ 4 & 4 & 0 \end{pmatrix}$$

$$M^{19} = M\cdot M^{18} = \begin{pmatrix} 3 & 4 & 1 \\ 4 & 3 & 4 \\ 2 & 4 & 3 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 & 1 \\ 4 & 0 & 1 \\ 4 & 4 & 0 \end{pmatrix} = \text{ the identity}$$

Thus, indeed, we have the order 19 element.

Note that, in reality, without some alternative means to verify that we really found an element of order 19, we could easily be suspicious that the numbers were wrong.

[04.11] Classify the conjugacy classes in S_n (the *symmetric group* of bijections of $\{1, \ldots, n\}$ to itself).

Given $g \in S_n$, the cyclic subgroup $\langle g \rangle$ generated by g certainly acts on $X = \{1, \ldots, n\}$ and therefore decomposes X into *orbits*

$$O_x = \{g^i x : i \in \mathbb{Z}\}$$

for choices of orbit representatives $x_i \in X$. We claim that the (unordered!) *list of sizes* of the (disjoint!) orbits of g on X uniquely determines the conjugacy class of g, and vice-versa. (An unordered list that allows the same thing to appear more than once is a **multiset**. It is not simply a *set*!)

To verify this, first suppose that $g = tht^{-1}$. Then $\langle g \rangle$ orbits and $\langle h \rangle$ orbits are related by

$$\langle g \rangle\text{-orbit } O_{tx} \leftrightarrow \langle h \rangle\text{-orbit } O_x$$

Indeed,

$$g^\ell \cdot (tx) = (tht^{-1})^\ell \cdot (tx) = t(h^\ell \cdot x)$$

Thus, if g and h are conjugate the unordered lists of sizes of their orbits must be the same.

On the other hand, suppose that the unordered lists of sizes of the orbits of g and h are the same. Choose an ordering of orbits of the two such that the cardinalities match up:

$$|O_{x_i}^{(g)}| = |O_{y_i}^{(h)}| \quad (\text{for } i = 1, \ldots, m)$$

where $O_{x_i}^{(g)}$ is the $\langle g \rangle$-orbit containing x_i and $O_{y_i}^{(h)}$ is the $\langle g \rangle$-orbit containing y_i. Fix representatives as indicated for the orbits. Let p be a permutation such that, for each index i, p bijects $O_{x_i}^{(g)}$ to $O_{x_i}^{(g)}$ by

$$p(g^\ell x_i) = h^\ell y_i$$

The only slightly serious point is that this map is well-defined, since there are many exponents ℓ which may give the same element. And, indeed, it is at this point that we use the fact that the two orbits have the same cardinality: we have

$$O_{x_i}^{(g)} \leftrightarrow \langle g \rangle / \langle g \rangle_{x_i} \quad (\text{by } g^\ell \langle g \rangle_{x_i} \leftrightarrow g^\ell x_i)$$

where $\langle g \rangle_{x_i}$ is the isotropy subgroup of x_i. Since $\langle g \rangle$ is cyclic, $\langle g \rangle_{x_i}$ is necessarily $\langle g^N \rangle$ where N is the number of elements in the orbit. The same is true for h, with the same N. That is, $g^\ell x_i$ depends exactly on $\ell \bmod N$, and $h^\ell y_i$ likewise depends exactly on $\ell \bmod N$. Thus, the map p is well-defined.

Then claim that g and h are conjugate. Indeed, given $x \in X$, take $O_{x_i}^{(g)}$ containing $x = g^\ell x_i$ and $O_{y_i}^{(h)}$ containing $px = h^\ell y_i$. The fact that the exponents of g and h are the same is due to the definition of p. Then

$$p(gx) = p(g \cdot g^\ell x_i) = h^{1+\ell}\, y_i = h \cdot h^\ell\, y_i = h \cdot p(g^\ell\, x_i) = h(px)$$

Thus, for all $x \in X$

$$(p \circ g)(x) = (h \circ p)(x)$$

Therefore,

$$p \circ g = h \circ p$$

or

$$pgp^{-1} = h$$

(Yes, there are usually many different choices of p which accomplish this. And we could also have tried to say all this using the more explicit cycle notation, but it's not clear that this would have been a wise choice.)

[04.12] The **projective linear group** $PGL_n(k)$ is the group $GL_n(k)$ modulo its center k, which is the collection of scalar matrices. Prove that $PGL_2(\mathbb{F}_3)$ is isomorphic to S_4, the group of permutations of 4 things. (*Hint:* Let $PGL_2(\mathbb{F}_3)$ act on **lines** in $\mathbb{F}_3^2$, that is, on one-dimensional $\mathbb{F}_3$-subspaces in $\mathbb{F}_3^2$.)

The group $PGL_2(\mathbb{F}_3)$ acts by permutations on the set X of lines in $\mathbb{F}_3^2$, because $GL_2(\mathbb{F}_3)$ acts on non-zero vectors in $\mathbb{F}_3^2$. The scalar matrices in $GL_2(\mathbb{F}_3)$ certainly stabilize every line (since they act by scalars), so act trivially on the set X.

On the other hand, any non-scalar matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ acts non-trivially on some line. Indeed, if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} * \\ 0 \end{pmatrix} = \begin{pmatrix} * \\ 0 \end{pmatrix}$$

then $c = 0$. Similarly, if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ * \end{pmatrix} = \begin{pmatrix} 0 \\ * \end{pmatrix}$$

then $b = 0$. And if

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \lambda \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

for some λ then $a = d$, so the matrix is scalar.

Thus, the map from $GL_2(\mathbb{F}_3)$ to permutations $\mathrm{Aut}_{\mathrm{set}}(X)$ of X has kernel consisting exactly of scalar matrices, so *factors through* (that is, is well defined on) the quotient $PGL_2(\mathbb{F}_3)$, and is *injective* on that quotient. (Since $PGL_2(\mathbb{F}_3)$ is the quotient of $GL_2(\mathbb{F}_3)$ by the kernel of the homomorphism to $\mathrm{Aut}_{\mathrm{set}}(X)$, the kernel of the mapping induced on $PGL_2(\mathbb{F}_3)$ is trivial.)

Computing the order of $PGL_2(\mathbb{F}_3)$ gives

$$|PGL_2(\mathbb{F}_3)| = |GL_2(\mathbb{F}_3)|/|\text{scalar matrices}| = \frac{(3^2-1)(3^2-3)}{3-1} = (3+1)(3^2-3) = 24$$

(The order of $GL_n(\mathbb{F}_q)$ is computed, as usual, by viewing this group as automorphisms of $\mathbb{F}_q^n$.)

This number is the same as the order of S_4, and, thus, an injective homomorphism must be surjective, hence, an isomorphism.

(One might want to verify that the center of $GL_n(\mathbb{F}_q)$ is exactly the scalar matrices, but that's not strinctly necessary for this question.)

[04.13] An automorphism of a group G is **inner** if it is of the form $g \to xgx^{-1}$ for fixed $x \in G$. Otherwise it is an **outer automorphism**. Show that every automorphism of the permutation group S_3 on 3 things is *inner*. (*Hint:* Compare the action of S_3 on the set of 2-cycles by conjugation.)

Let G be the group of automorphisms, and X the set of 2-cycles. We note that an automorphism must send order-2 elements to order-2 elements, and that the 2-cycles are exactly the order-2 elements in S_3. Further, since the 2-cycles *generate* S_3, if an automorphism is trivial on all 2-cycles it is the trivial automorphism. Thus, G *injects* to $\mathrm{Aut}_{\mathrm{set}}(X)$, which is permutations of 3 things (since there are three 2-cycles).

On the other hand, the conjugation action of S_3 on itself stabilizes X, and, thus, gives a group homomorphism $f : S_3 \to \mathrm{Aut}_{\mathrm{set}}(X)$. The kernel of this homomorphism is trivial: if a non-trivial permutation p conjugates the two-cycle $t = (1\ 2)$ to itself, then

$$(ptp^{-1})(3) = t(3) = 3$$

so $tp^{-1}(3) = p^{-1}(3)$. That is, t fixes the image $p^{-1}(3)$, which therefore is 3. A symmetrical argument shows that $p^{-1}(i) = i$ for all i, so p is trivial. Thus, S_3 injects to permutations of X.

In summary, we have group homomorphisms

$$S_3 \to \mathrm{Aut}_{\mathrm{group}}(S_3) \to \mathrm{Aut}_{\mathrm{set}}(X)$$

where the map of automorphisms of S_3 to permutations of X is an isomorphism, and the composite map of S_3 to permutations of X is surjective. Thus, the map of S_3 to its own automorphism group is necessarily surjective.

[04.14] Identify the element of S_n requiring the maximal number of adjacent transpositions to express it, and prove that it is unique.

We claim that the permutation that takes $i \to n-i+1$ is the unique element requiring $n(n-1)/2$ elements, and that this is the maximum number.

For an ordered listing $(t_1, \ldots, t_n)$ of $\{1, \ldots, n\}$, let

$$d_o(t_1, \ldots, t_n) = \text{ number of indices } i < j \text{ such that } t_i > t_j$$

and for a permutation p let

$$d(p) = d_o(p(1), \ldots, p(n))$$

Note that if $t_i < t_j$ for all $i < j$, then the ordering is $(1, \ldots, n)$. Also, given a configuration $(t_1, \ldots, t_n)$ with *some* $t_i > t_j$ for $i < j$, necessarily this inequality holds for some *adjacent* indices (or else the opposite inequality would hold for *all* indices, by transitivity!). Thus, if the ordering is *not* the default $(1, \ldots, n)$, then there is an index i such that $t_i > t_{i+1}$. Then application of the adjacent transposition s_i of $i, i+1$ reduces by exactly 1 the value of the function $d_o()$.

Thus, for a permutation p with $d(p) = \ell$ we can find a product q of exactly ℓ adjacent transpositions such that $q \circ p = 1$. That is, we need *at most* $d(p) = \ell$ adjacent transpositions to express p. (This does not preclude *less efficient* expressions.)

On the other hand, we want to be sure that $d(p) = \ell$ is the *minimum* number of adjacent transpositions needed to express p. Indeed, application of s_i only affects the comparison of $p(i)$ and $p(i+1)$. Thus, it can decrease $d(p)$ by at most 1. That is,

$$d(s_i \circ p) \geq d(p) - 1$$

and possibly $d(s_i \circ p) = d(p)$. This shows that we do need *at least* $d(p)$ adjacent transpositions to express p.

Then the permutation w_o that sends i to $n-i+1$ has the effect that $w_o(i) > w_o(j)$ for *all* $i < j$, so it has the maximum possible $d(w_o) = n(n-1)/2$. For uniqueness, suppose $p(i) > p(j)$ for all $i < j$. Evidently, we must claim that $p = w_o$. And, indeed, the inequalities

$$p(n) < p(n-1) < p(n-2) < \ldots < p(2) < p(1)$$

leave no alternative (assigning distinct values in $\{1, \ldots, n\}$) but

$$p(n) = 1 < p(n-1) = 2 < \ldots < p(2) = n-1 < p(1) = n$$

(One might want to exercise one's technique by giving a more careful inductive proof of this.)

[04.15] Let the permutation group S_n on n things act on the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ by $\mathbb{Z}$-algebra homomorphisms defined by $p(x_i) = x_{p(i)}$ for $p \in S_n$. (The universal mapping property of the polynomial ring allows us to define the images of the indeterminates x_i to be whatever we want, and at the same time guarantees that this determines the $\mathbb{Z}$-algebra homomorphism completely.) Verify that this is a group homomorphism

$$S_n \to \mathrm{Aut}_{\mathbb{Z}-\mathrm{alg}}(\mathbb{Z}[x_1, \ldots, x_n])$$

Consider

$$D = \prod_{i<j} (x_i - x_j)$$

Show that for any $p \in S_n$

$$p(D) = \sigma(p) \cdot D$$

where $\sigma(p) = \pm 1$. Infer that σ is a (non-trivial) group homomorphism, the **sign** homomorphism on S_n.

Since these polynomial algebras are *free* on the indeterminates, we check that the permutation group *acts* (in the technical sense) on the set of indeterminates. That is, we show associativity and that the identity of the group acts trivially. The latter is clear. For the former, let p, q be two permutations. Then

$$(pq)(x_i) = x_{(pq)(i)}$$

while

$$p(q(x_i)) = p(x_{q(i)} = x_{p(q(i))}$$

Since $p(q(i)) = (pq)(i)$, each $p \in S_n$ gives an automorphism of the ring of polynomials. (The endomorphisms are invertible since the group has inverses, for example.)

Any permutation merely permutes the factors of D, up to sign. Since the group *acts* in the technical sense,

$$(pq)(D) = p(q(D))$$

That is, since the automorphisms given by elements of S_n are $\mathbb{Z}$-linear,

$$\sigma(pq) \cdot D = p(\sigma(q) \cdot D) = \sigma(q)p(D) = \sigma(q) \cdot \sigma(p) \cdot D$$

Thus,

$$\sigma(pq) = \sigma(p) \cdot \sigma(q)$$

which is the homomorphism property of σ. ///
