

3.3. conjugation.

Definition 3.5. We say that a is *conjugate* to b if there exists a c so that

$$a = cbc^{-1}$$

I used the following notation. First, $a \sim b$ for “ a is conjugate to b ” and

$$\phi_c(b) := cbc^{-1}$$

The function ϕ_c is a “homomorphism” (a concept that I will explain later).

- (1) Show that conjugation is an equivalence relation, i.e., it is
 - (a) reflective: $(\forall a)a \sim a$
 - (b) symmetric: $(\forall a, b)a \sim b \Rightarrow b \sim a$
 - (c) transitive: $(\forall a, b, c)a \sim b, b \sim c \Rightarrow a \sim c$
- (2) If $\tau = (a_1, a_2, \dots, a_k)$ then find a formula for $\sigma\tau\sigma^{-1}$
- (3) Show that every permutation of n letters is conjugate to its inverse.

3.3.1. *conjugacy is an equivalence relation.* We verified in class that the three properties of an equivalence relation hold:

- (1) *reflexive:* $a \sim a$.
Just take $c = e$ (the identity). Then $a = eae^{-1} = \phi_e(a)$. So every permutation is conjugate to itself.
- (2) *symmetry:* $a \sim b \Rightarrow b \sim a$.
We are given that $a = cbc^{-1}$. Multiply both sides on the left with c^{-1} and on the right with $c = (c^{-1})^{-1}$:

$$c^{-1}ac = c^{-1}a(c^{-1})^{-1} = c^{-1}(cbc^{-1})c = ebe = b$$

So, $b = \phi_{c^{-1}}(a)$ and $b \sim a$.

- (3) *transitive:* $a \sim b, b \sim x \Rightarrow a \sim x$. (We realized that the letter c was being used too often.)

We are given that $a = cbc^{-1}$ and $b = dxd^{-1}$. Insert this formula for b into the formula for a to get:

$$a = c(dxd^{-1})c^{-1} = (cd)x(d^{-1}c^{-1}) = (cd)x(cd)^{-1} = \phi_{cd}(x)$$

Here we used the formula $(cd)^{-1} = d^{-1}c^{-1}$ from earlier.

3.3.2. *conjugate of a k -cycle.* We found the formula and proved it.

Theorem 3.6. *If σ, τ are permutations and $\tau = (a_1, a_2, \dots, a_k)$ then*

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k)).$$

Proof. Take $x = \sigma(a_i)$. Then $\sigma^{-1}(x) = a_i$ by definition of the inverse σ^{-1} as discussed earlier. So,

$$\sigma\tau\sigma^{-1}(x) = \sigma\tau(a_i) = \sigma(a_{i+1})$$

This is for $i = 1, \dots, k-1$. If $x = \sigma(a_k)$ then

$$\sigma\tau\sigma^{-1}(x) = \sigma\tau(a_k) = \sigma(a_1)$$

This almost does it. This shows that $\sigma\tau\sigma^{-1}$ moves the letters $\sigma(a_i)$ as indicated. But we also checked that the other letters are fixed. If x is not equal to any $\sigma(a_i)$ then $\sigma^{-1}(x)$ is not equal to any of the a_i which means that τ does not move it. So

$$\tau(\sigma^{-1}(x)) = \sigma^{-1}(x).$$

When you apply σ you get back x :

$$\sigma\tau(\sigma^{-1}(x)) = \sigma\sigma^{-1}(x) = x.$$

So, $\sigma\tau\sigma^{-1}$ fixes every letter not in the cycle $(\sigma(a_1), \dots, \sigma(a_k))$ which means that

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k)).$$

□

3.3.3. *every permutation of n is conjugate to its inverse.* We did this by example. Suppose that τ is a cycle. For example $\tau = (123)$. Then

$$\tau^{-1} = (321) = (132) = (213)$$

By the conjugation formula above, we just need to choose σ which changes 1, 2, 3 into the three letters in τ^{-1} . So, there are three answers:

- (1) $\sigma = (13)$
- (2) $\sigma = (23)$
- (3) $\sigma = (12)$.

Each of these will conjugate τ into its inverse.

When there is more than one cycle we have to treat each cycle separately. For example:

$$\tau = (12)(345)(8, 9, 10, 11)$$

$$\tau^{-1} = (11, 10, 9, 8)(543)(12) = (12)(543)(11, 10, 9, 8)$$

Here I used two formulas. First,

$$(abc)^{-1} = c^{-1}b^{-1}a^{-1}$$

Then, I used the fact that disjoint cycles commute.

Theorem 3.7. *If σ, τ are permutations of disjoint sets of numbers then $\sigma\tau = \tau\sigma$.*

Then you do the same thing as before. For example let

$$\sigma = (45)(8, 11)(9, 10).$$

Then

$$\sigma\tau\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\cdots \text{etc.}) = (12)(543)(11, 10, 9, 8) = \tau^{-1}.$$

This is one of those proofs that are a real pain to write down in complete detail.

3.4. definition of a group. This spilled over to Day 4 (Wednesday).

Definition 3.8. A *group* is a set G with a binary operation (for all $a, b \in G$ there is a product $ab \in G$) satisfying three properties:

- (1) (*associative*) $(ab)c = a(bc)$ for all $a, b, c \in G$.
- (2) (*identity*) G has an identity element e so that $ae = ea = a$ for all $a \in G$. (Think: $e = 1$.)
- (3) (*inverse*) Every element $x \in G$ has an inverse x^{-1} which is also an element of G so that

$$xx^{-1} = x^{-1}x = e.$$

The discussion from Monday proves the following.

Theorem 3.9. *Permutations of X forms a group, i.e., the set of all permutations of X is a group.*

Problem: Show that the set of 2×2 integer matrices with determinant ± 1 forms a group under matrix multiplication. Thus

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = \pm 1$$

and $a, b, c, d \in \mathbb{Z}$.

- (1) (*associative*) We skipped the boring proof that matrix multiplication is associative.
- (2) (*identity*) The identity is the matrix

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

This satisfies the equation $I_2X = X = XI_2$ for any 2×2 matrix X .

- (3) (*inverse*) The inverse of a 2×2 matrix A is

$$A^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

When $ad - bc = \pm 1$ this matrix also has integer entries. Liz pointed out that we also need to check that the determinant of

the new matrix A^{-1} is ± 1 because the definition of a group says the inverse needs to be an element of G . But this is a simple calculation:

$$\det \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{(ad-bc)^2} (ad-bc) = \frac{1}{ad-bc} = \frac{1}{\pm 1} = \pm 1$$

(Why does the scalar become squared in the determinant?)

I said that there is a general formula

$$\det(AB) = \det A \det B$$

So,

$$\det(AA^{-1}) = \det I_2 = 1 = \det A \det A^{-1}$$

which implies that

$$\det A^{-1} = \frac{1}{\det A}$$

3.5. permutation matrices.

Definition 3.10. If σ is a permutation of n letters, the *permutation matrix* $M(\sigma)$ is defined to be the matrix with entries p_{ij} where

$$p_{ij} = \begin{cases} 1 & \text{if } \sigma(j) = i \\ 0 & \text{if not} \end{cases}$$

For example, if $\sigma = (123)$ then

$$M(\sigma) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Questions:

- (1) Show that $M(\sigma)M(\tau) = M(\sigma\tau)$
- (2) Describe $M(\sigma)X$, i.e., what happens to X when you multiply on the left by $M(\sigma)$?
- (3) What is $\det M(\sigma)$?

I think we did the last question first:

$$\det M(\sigma) = \pm 1.$$

You can prove this by induction. This will be homework.

To do question (2) we did the example of $\sigma = (123)$:

$$M(\sigma)X = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} g & h & i \\ a & b & c \\ d & e & f \end{pmatrix}$$

Thus multiplication by $M(\sigma)$ on the left moves the numbers in the first row into the second row, the second row moves to the third and the third row moves to the first.

Theorem 3.11. *Multiplication of a matrix X on the left by a permutation matrix $M(\sigma)$ permutes the rows of X by the permutation σ .*

Proof. Here is a formal proof. By definition of matrix multiplication,

$$(M(\sigma)X)_{ik} = \sum_{j=1}^n p_{ij}x_{jk}$$

But $p_{ij} = 1$ when $i = \sigma(j)$ or $j = \sigma^{-1}(i)$ and $p_{ij} = 0$ otherwise. This means that only one term in the sum is nonzero:

$$(M(\sigma)X)_{ik} = p_{ij}x_{jk} \quad \text{where } i = \sigma(j)$$

In other words, the (j, k) entry of X moves to the $(\sigma(j), k)$ position. Since this happens for every k , the entire j -th row of X moves to the $\sigma(j)$ -th row. \square

Students were surprised to figure out that the multiplication on the right has a different rule:

Theorem 3.12. *Multiplication of a matrix X on the right by a permutation matrix $M(\sigma)$ permutes the columns of X by the permutation σ^{-1} .*

With this rule we can figure out the proof for the 1st statement. Take a matrix X .

Lemma 3.13.

$$M(\sigma)M(\tau)X = M(\sigma\tau)X$$

Proof. By associativity, $(M(\sigma)M(\tau))X = M(\sigma)(M(\tau)X)$. But, by the previous discussion, this does the following. In $M(\tau)X$ the rows of X are permuted by τ . In $M(\sigma)(M(\tau)X)$ the rows are then permuted by σ . But, this is the permutation $\sigma\tau$ applied to the rows of X which is $M(\sigma\tau)X$. \square

Theorem 3.14.

$$M(\sigma)M(\tau) = M(\sigma\tau)$$

Proof. Multiply by the inverse of X :

$$M(\sigma)M(\tau) \underbrace{XX^{-1}}_{I_n} = M(\sigma\tau) \underbrace{XX^{-1}}_{I_n}$$

$$M(\sigma)M(\tau) = M(\sigma\tau).$$

\square