Mathematics 546 Homework, September 23, 2020

Definition 1. A ***group***, $(G, *)$ is set G with a product $*$ between pairs $(a, b) \in G \times G$ (that is for each $a, b \in G$ the product $a * b$ is also an element of G) with the properties

(i) The product is associative:
$$(a * b) * c = a * (b * c)$$
for all $a, b, c \in G$.

(ii) There is an ***identity element*** for $*$, that is an element e such that
$$a * e = e * a = a$$
for all $a \in G$. As shown below this element is necessarily unique.

(iii) Each element $a \in G$ has an ***inverse***. That is there is a b such that
$$a * b = b * a = e.4$$
$\square$

Here is the calculation showing that e is unique. Let e and e' be so that $a * e = e * a = a = a * e' = e' * a$. Then showing uniqueness means that we need to show

$$\begin{aligned} e' &= e' * e && (\text{use } a = e' \text{ in } a = a * e) \\ &= e && (\text{use } a = e \text{ in } e' * a = a). \end{aligned}$$

We also have that inverses are unique. Let b and b' both be inverses of a. Then
$$ab = b * a = a * b' = b' * a = e.$$
And we wish to show $b = b'$.

$$\begin{aligned} b' &= b' * e && (e \text{ is the identity}) \\ &= b' * (a * b) && (b \text{ is an inverse of } a) \\ &= (b' * a) * b && (\text{associative law}) \\ &= e * b && (b' \text{ is an inverse of } a) \\ &= b && (e \text{ is the identity}) > \end{aligned}$$

The importance of the identify of the associative law is that it lets us ignore parenthesis. For example there are five ways to group a product of four elements:

$$a*(b*(c*d)) \qquad a*((b*c)*d) \qquad (a*b)*(c*d) \qquad (a*(b*c))*d \qquad ((a*b)*c)*d$$

Problem 1. Use the associative law to show all of these can be reduced to $a * (b * (c * d))$. For example
$$((a * b) * c) * d = (a * (b * c)) * d = a * ((b * c) * d) = a * (b * (c * d)).$$
Now you show that all of $a * ((b * c) * d)$, $(a * b) * (c * d)$, and $(a * (b * c)) * d$ can be reduced to $a * (b * (c * d))$. $\square$

In general it holds for products of all lengths that the associative law implies that any two groupings are equal.

One very quickly gets tired of putting the $*$'s in the products and so we use the same convention we use for ordinary multiplication abbreviate $a * b$ to ab. Then the associative law looks like $a(bc) = (ab)c$. The one place where we do not use this convention is when the group operation is addition when we still use the usual $a + b$.

Also when the product $*$ is clear from context, we will refer to the group G, rather than to the group $(G, *)$.

And anther useful piece of notation is

$$a^{-1} = \text{inverse of } a.$$

Proposition 2. *If a, b are elements of the group G, then*

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Proof. We did this in class. □

Proposition 3. *Let $a_1, a_2, \ldots, a_n$ elements of the group G. Then*

$$(a_1a_2\cdots a_n)^{-1} = a_m^{-1}a_{n-1}^{-1}\cdots a_1^{-1}a_1^{-1}.$$

Problem 2. Prove this using induction. *Hint:* Here is what the induction step from $n = 3$ to $n = 4$ looks like. The induction hypothesis is that we know the result for $n = 3$, that is

$$(a_1a_2a_3)^{-1} = a_3^{-1}a_2^{-2}a_1^{-1}$$

Then

$$\begin{aligned}(a_1a_2a_3a_4)^{-1} &= ((a_1a_2a_3)a_4)^{-1} \\ &= a_4^{-1}(a_1a_2a_3)^{-1} \qquad \text{(Prop. 2 with } a = (a_1a_2a_3),\ b = a_4\text{)} \\ &= a_4^{-1}a_3^{-1}a_2^{-1}a_1^{-1} \qquad \text{(by the induction hypothesis.)}\end{aligned}$$

The general case works the same way. □

Problem 3. Show that in a group the following cancellation property holds:

$$axb = ayb$$

implies $x = y$. □

We use the natural notation for powers. That is is for $n \geq 0$,

$$\begin{aligned}
a^0 &= e \\
a^1 &= e \\
a^2 &= aa \\
a^3 &= aaa \\
a^4 &= aaaa \\
a^5 &= aaaaa \\
a^6 &= aaaaaa \\
a^7 &= aaaaaaa \\
a^8 &= aaaaaaaa
\end{aligned}$$

and in general

$$a^n = \underbrace{aa\cdots a}_{n \text{ factors}}$$

And we have the natural extension to negative exponents:

$$\begin{aligned}
a^{-1} &= a^{-1} \\
a^{-2} &= a^{-1}a^{-1} \\
a^{-3} &= a^{-1}a^{-1}a^{-1} \\
a^{-4} &= a^{-1}a^{-1}a^{-1}a^{-1} \\
a^{-5} &= a^{-1}a^{-1}a^{-1}a^{-1}a^{-1} \\
a^{-6} &= a^{-1}a^{-1}a^{-1}a^{-1}a^{-1}a^{-1} \\
a^{-7} &= a^{-1}a^{-1}a^{-1}a^{-1}a^{-1}a^{-1}a^{-1} \\
a^{-8} &= a^{-1}a^{-1}a^{-1}a^{-1}a^{-1}a^{-1}a^{-1}a^{-1}
\end{aligned}$$

and

$$a^{-n} = \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n \text{ factors}}$$

Proposition 4. *With this notation the usual rules for exponents hold:*

$$\begin{aligned}
a^n a^m &= a^{m+n} \\
(a^{-1})^n &= a^{-n} = (a^n)^{-1} \\
(a^m)^n &= a^{mn}.
\end{aligned}$$

Proof. The proof is the same as the argument you used in elementary algebra. $\square$

Problem 4. Let G be a group and let $a \in G$ satisfy $a^4 = e$. Then we can compute a^{91} as follows. Divide 4 into 91 using the division algorithm to get $91 = 88 + 3 = 22(4) + 3$. Then

$$a^{91} = a^{22(4)+3} = (a^4)^{22}a^3 = e^{22}a^3 = a^3.$$

Using this idea do the following

(a) If $b^5 = 1$ simplify b^{147}, where here by simplify we mean write $b^{145} = b^r$ where $0 \le r \le 4$.
(b) If $c^7 = 1$ simplify c^{-33}, that is write $c^{-33} = c^r$ where $0 \le r \le 6$.
(c) Assume s is a group element with $s^k = e$ for some positive integer k. Can you come up with a rule for simplifying s^n? $\square$

Definition 5. A group, G, is ***Abelian*** or ***commutative*** if and only if $ab = ba$ for all $a, b \in G$. $\square$

Problem 5. In light of Proposition 4 and your experience with elementary algebra it might be tempting to conjecture that $(ab)^n = a^n b^n$ for all n. Here we show this is not the case. Prove that if a, b are elements of a group and $(ab)^2 = a^2b^2$, then $ab = ba$. There are examples of groups with elements with $ab \neq ba$, For example see Problem 9.

Problem 6. Let G be a group where $x^2 = e$ for all $x \in G$. Then show G is Abelian. *Hint:* Let $x = ab$ and use $x^2 = xx = e$. $\square$

Problem 7. Show that a group with just two elements is Abelian. *Hint:* As G has only two elements, $G = \{e, a\}$, That is G is just the identity and one other element $a \neq e$. Then $a^2 = e$ or $a^2 = a$. Show that $a^2 = a$ implies $a = e$, which is not the case. Thus $a^2 = e$. $\square$

We extend our examples of groups using matrices. Recall that a 2×2 matrix is a square array

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

and we multiple two matrices by the rule

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax + bz & ay + bd \\ cx + dz & cy + dw \end{bmatrix}$$

Proposition 6. *Matrix multiplication is associative, that is if A, B, and C are 2 matrices then*

$$(AB)C = A(BC).$$

Proof. This can be done by brute force, but I will refer to your linear algebra course or if, you can not stand not seeing why this is true, you can find a nice presentation of the proof for for the 2×2 case at this page at the Kahn Acadmey. $\square$

Proposition 7. *The matrix*

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

is an identity for 2×2 matrix multiplication. That is for any 2×2 matrix A,

$$AI = IA = A$$

Proof. This is easy to check using the definition of matrix multiplication. $\square$

Problem 8. Let A and B be the matrices

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad B = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

and define the ***determinant*** of A to be

$$\det(A) = ad - bc.$$

Show

$$AB = BA = \det(A)I.$$

$\square$

Proposition 8. *Let A be a 2×2 matrix with $\det A \neq 0$. Then A has an inverse. If*

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

it is given by

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

Proof. Using the notation of Problem 8 we have that

$$\left(\frac{1}{\det(A)}B\right) A = A\left(\frac{1}{\det(A)}B\right) = \frac{1}{\det(A)}AB = \frac{1}{\det(A)}\det(A)I = I$$

which shows that $\frac{1}{\det(A)}B$ is the inverse of A. Thus

$$A^{-1} = \frac{1}{\det(A)}B = \frac{1}{ad - bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

and we are done. $\square$

Proposition 9. *Let $\mathbb{F}$ be either $\mathbb{Q}$ (the rational numbers) of $\mathbb{R}$ (the real numbers) and set*

$$\mathrm{GL}(\mathbb{F}, 2) = \textit{The set of } 2 \times 2 \textit{ matrices } A \textit{ with } \det(A) \neq 0.$$

Then $\mathrm{GL}(2, \mathbb{F})$ using matrix multiplication as product is a group.

Proof. The product is associative by 6. It has the matrix I as identity by Proposition 7 and has inverses by Proposition 8 $\square$

Problem 9. Let $A, B \in \mathrm{GL}(2, \mathbb{Q})$ be the elements

$$A = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \qquad B = \begin{bmatrix} -1 & 0 \\ -2 & 1 \end{bmatrix}$$

(a) Show

$$A^3 = B^2 = I$$

(b) Compute A^{431} and B^{103}.

(c) Show
$$AB \neq BA$$
which shows the group $\mathrm{GL}(2, \mathbf{Q})$ is nonAbelian. $\square$