

Math 122, Solution Set No. 1

1 Chapter 1.1 Problem 16

Let A be nilpotent, i.e. $A^k = 0$ for some $k > 0$. Then I claim

$$I - A + A^2 - A^3 + \cdots + A^{k-1} = (I + A)^{-1}.$$

This is because right-multiplying by this matrix gives:

$$\begin{aligned}(I + A)(I - A + A^2 - A^3 + \cdots + A^{k-1}) &= I + A - A + \cdots + A^{k-1} - A^{k-1} + A^k \\ &= I + A^k \\ &= I\end{aligned}$$

because $A^k = 0$. similarly, left-multiplication yields:

$$(I - A + A^2 - A^3 + \cdots + A^{k-1})(I + A) = I$$

therefore $I - A + A^2 - A^3 + \cdots + A^{k-1} = (I + A)^{-1}$, i.e. $(I + A)$ is invertible \diamond

Note: I deducted points if you did not show the inverse was two-sided.

2 Chapter 2.1 Problem 1(b)

The multiplication table for S_3

\times	e	(12)	(23)	(13)	(123)	(132)
e	e	(12)	(23)	(13)	(123)	(132)
(12)	(12)	e	(123)	(132)	(23)	(13)
(23)	(23)	(132)	e	(123)	(13)	(12)
(13)	(13)	(123)	(132)	e	(12)	(23)
(123)	(123)	(13)	(12)	(23)	(132)	e
(132)	(132)	(23)	(13)	(12)	e	(123)

All multiplication tables are read (as in Artin) with the entry in row u and column v being the product $u \circ v$. \diamond

3 Chapter 2.1 Problem 8

This problem asks for an example of 2×2 matrices such that $A^{-1}B \neq B^{-1}A$. Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

and $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$. Then $A^2 = B^2 = I$, i.e. $A = A^{-1}$ and $B = B^{-1}$. So $A^{-1}B = AB =$

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ but } B^{-1}A = BA = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \neq A^{-1}B.$$

4 Chapter 2.2 Problem 2

Let a, b be elements of a group G , such that a has order 5 and $a^3b = ba^3$. Left-multiplying by a^3 gives $a^3(a^3b) = a^3ba^3$. But $a^3a^3 = a^6 = a$, because $a^5 = 1$. So $ab = a^3ba^3$, and recalling the original condition gives $ab = ba^3a^3 = ba^6 = ba$. \diamond

5 Chapter 2.2 Problem 3

- (a) Yes. The identity is real, and since $GL_n(\mathbb{R})$ is a group, it is closed and contains inverses.
(b) Yes. This was covered in class on 9/18.
(c) No. 1 is a positive integer, but -1 , its inverse, is not.
(d) Yes. The identity 1 is positive, and the product of positive reals is positive implies that this set is closed. The multiplicative inverse of a positive number is likewise positive.
(e) No. The set of all matrices of the form: $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ does not include the identity element of $GL_n(\mathbb{R})$! \diamond

6 Chapter 2.2 Problem 4

Assume that $\forall x, y \in H, xy^{-1} \in H$. If $H \neq \emptyset$, then $\exists x \in H$. So by assumption, $e = xx^{-1} \in H$. Then $e, x \in H \Rightarrow x^{-1} = ex^{-1} \in H$. Finally, if $x, y \in H$, we now know that $y^{-1} \in H$ which means $xy = x(y^{-1})^{-1} \in H$, i.e. H is closed. This proves H is a subgroup. \diamond

7 Chapter 2.2 Problem 14

Lemma: Every subgroup of a cyclic group is cyclic.

Proof: Let $G = \langle x \rangle$ and $H \leq G$. Let n be the smallest positive integer such that $x^n \in H$. Since H is closed, $\langle x^n \rangle \leq H$. Assume $\exists x^m \in H$ such that $x^m \notin \langle x^n \rangle$. Then $m = an + b$ with $0 \leq b < n$, and $x^b \in H$. Therefore $b = 0$, i.e. $x^m \in \langle x^n \rangle$. So $H = \langle x^n \rangle$, which means H is cyclic.

Now let G have order n and r be an integer that divides n . Then $H = \langle x^{n/r} \rangle$ is a subgroup of G having order r . Assume H is not unique, i.e. $H' \leq G$ and $|H'| = r$. Then by the Lemma, $H' = \langle x^m \rangle$ for some m , and let m be the smallest positive integer such that $H' = \langle x^m \rangle$. If $m \nmid n$ then we can write $n = qm + s$ with $0 < s < m$. Then we have $x^{(q+1)m} = x^{m-s} \in H'$. But $m - s < m$ is a contradiction, so $m \mid n$ and thus $|H'| = n/m$. But we already had $|H'| = r$, which tells us that $m = n/r$ and $H' = \langle x^{n/r} \rangle = H$. Therefore H is unique. \diamond (Note:) In a cyclic group of order n , $x^{ar} = x^{br} \Rightarrow ar \equiv br \pmod{n}$ but it does not imply $a = b$, even mod n .

8 Chapter 2.2 Problem 20

- (a) Let $a, b \in G$, an abelian group, with orders m, n respectively.

Claim: The order of ab divides the least common multiple of m, n .

Proof: Let r be the least common multiple of m, n . Then $r = zm = yn$ for some integers y, z . So we have

$$(ab)^r = a^r b^r = (a^m)^z (b^n)^y = e^z e^y = e$$

Since $(ab)^r = e$, The order of ab must divide r .

Note: The order of ab is not in general equal to the least common multiple of m, n : For example, let $G = C_4 = \langle x \rangle$ with $a = x$ and $b = x^3$, in which case ab has order 1. \diamond

(b) Let $G = GL_2(\mathbb{R})$ and consider the matrices $A = \begin{bmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 3 \\ \frac{1}{3} & 0 \end{bmatrix}$. Then we have $A^2 = B^2 = I$, that is, A and B have order 2, which is finite. However, $AB = \begin{bmatrix} 2/3 & 0 \\ 0 & 3/2 \end{bmatrix}$ which has the startling property that $(AB)^n = \begin{bmatrix} (2/3)^n & 0 \\ 0 & (3/2)^n \end{bmatrix}$ which is never equal to the identity for $n \neq 0$, i.e. AB has infinite order. \diamond

9 Chapter 2.3 Problem 1

Construct the map $\varphi : \mathbb{R}^+ \rightarrow P$ defined by $\varphi(x) = 2^x$.

$$\varphi(x+y) = 2^{x+y} = 2^x 2^y = \varphi(x)\varphi(y)$$

So φ is a homomorphism. Furthermore, $2^x = 1$ iff $x = 0$. So $\text{Ker}(\varphi) = 0$, i.e. φ is injective. Finally, if $x \in P$, $\varphi(\log_2(x)) = x$. So φ is surjective. Thus φ is an isomorphism, i.e. $\mathbb{R}^+ \cong P$. \diamond

10 Chapter 2.3 Problem 7

Define $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Furthermore define the permutation matrix $D \in GL_2(\mathbb{R})$ by $P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Then $D = D^{-1}$ and $DAD^{-1} = B$, i.e. A and B are conjugate in $GL_2(\mathbb{R})$.

Suppose that $\exists C \in SL_2(\mathbb{R})$ such that $CAC^{-1} = B$. Then

$$CAC^{-1} = DAD^{-1} \Rightarrow (D^{-1}C)A = A(D^{-1}C)$$

So $D^{-1}C$ commutes with A . Write the general form of a 2×2 matrix, and we have:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix} = \begin{bmatrix} a & a+b \\ c & c+d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

So $c = 0$ and $a = d$. This says $\det(D^{-1}C) = a^2 > 0$. But $\det(D^{-1}C) = (\det D^{-1})(\det C) = -1 \cdot 1 < 0$, a contradiction. Therefore A and B must not be conjugate in $SL_2(\mathbb{R})$. \diamond

11 Chapter 2.3 Problem 12

(a) φ is surjective because $\varphi(x^{-1}) = x, \forall x \in G$. The identity is the inverse only of itself, so $\ker(\varphi) = e$, i.e. φ is injective.

(b) Let φ be an automorphism, which means φ is a homomorphism. Let $x, y \in G$. Then

$$xy = (y^{-1}x^{-1})^{-1} = \varphi(y^{-1}x^{-1}) = \varphi(y^{-1})\varphi(x^{-1}) = yx$$

and so G is abelian. If G is abelian, then

$$\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y)$$

and so φ is a bijective homomorphism, i.e. an automorphism. Thus φ is an automorphism if and only if G is abelian. \diamond