Math 30810 Honors Algebra 3
Homework 3

Andrei Jorza

Due Thursday, September 15

Do any 8 of the following 10 questions. Artin a.b.c means chapter a, section b, exercise c.

1. Artin 2.4.3

   Proof. If $(ab)^k = 1$ it follows that $1 = (ab)^k = a(ba)^{k-1}b$ and so $(ba)^{k-1} = a^{-1}b^{-1} = (ba)^{-1}$ which immediately implies that $(ba)^k = 1$. The reciprocal is also true and therefore $(ab)^k = 1$ iff $(ba)^k = 1$ and so ab and ba have the same order. □

2. Artin 2.4.7

   Proof. It suffices to check that H is stable under multiplication and inversion. But $x^{-1} = x$, $y^{-1} = y$ and $(xy)^{-1} = xy$ from the assumption that each of these elements has order 2. To check that H is closed under multiplication we look at the multiplication table (the entry on row a and column b is the product ab)

	1	x	y	xy
1	1	x	y	xy
x	x	x^2	xy	x^2y
y	y	yx	y^2	yxy
xy	xy	xyx	xy^2	$(xy)^2$

   and we need that every entry in the table is in H. Each of x, y, xy has order 2 so that takes care of the squares. Moreover, since $(xy)^2 = 1$ it follows that $xyxy = 1$ and so $yx = x^2yxy^2 = x(xyxy)y = xy$ so x and y commute. By inspection every entry is now in H. □

3. Artin 2.6.2

   Proof. Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a homomorphism of (additive) groups. Then $f(1) = a \in \mathbb{Z}$. From class we know that $f(n) = nf(1)$ for all integers $n \in \mathbb{Z}$ and so $f(n) = na$ for all $n \in \mathbb{Z}$. Moreover, given a the map f_a sending n to na is a homomorphism.

   The map f_a is injective whenever $a \neq 0$. It is surjective if and only if $1 \in \operatorname{Im} f_a = a\mathbb{Z}$ and so if and only if $a \in \{-1, 1\}$. □

4. For a matrix $A \in M_{n\times n}(\mathbb{C})$ define $e^A = I_n + A + A^2/2! + A^3/3! + \cdots$. You may assume that this expression always converges to a matrix $e^A \in M_{n\times n}(\mathbb{C})$. If $S \in \mathrm{GL}_n(\mathbb{C})$ show that $e^{SAS^{-1}} = Se^AS^{-1}$.

Proof. Note that $(SAS^{-1})^n = SAS^{-1}SAS^{-1}\cdots SAS^{-1} = SA^nS^{-1}$ and so

$$e^{SAS^{-1}} = \sum_{n\geq 0} \frac{(SAS^{-1})^n}{n!} = \sum \frac{SA^nS^{-1}}{n!} = Se^AS^{-1}$$

□

5. In the context of the previous exercise show that if A is upper triangular with $a_1, \ldots, a_n$ on the diagonal then e^A is upper triangular with $e^{a_1}, \ldots, e^{a_n}$ on the diagonal and conclude that $\det(e^A) = e^{\mathrm{Tr}(A)}$. As an optional exercise show that for any matrix A, $\det(e^A) = e^{\mathrm{Tr}(A)}$ and deduce that e^A is always invertible. [Hint: You may use the following standard fact from linear algebra, that for every matrix A you can find an invertible matrix S such that SAS^{-1} is upper triangular.]

Proof. Remember from last homework that if you multiply two upper triangular matrices the result is also upper triangular and the diagonal entries are simply the products of the diagonal entries of the two matrices. Therefore if A is upper triangular with diagonal entries $(a_{11}, \ldots, a_{nn})$ then A^k is upper triangular with diagonal entries $(a_{11}^k, \ldots, a_{nn}^k)$. We deduce that e^A is upper triangular with diagonal entries

$$(\sum_{k\geq 0} \frac{a_{11}^k}{k!}, \ldots, \sum_{k\geq 0} \frac{a_{nn}^k}{k!}) = (e^{a_{11}}, \ldots, e^{a_{nn}})$$

Since the determinant of an upper triangular matrix is the product of the diagonal entries we deduce that

$$\det e^A = \prod e^{a_{ii}} = e^{\sum a_{ii}} = e^{\mathrm{Tr}\, A}$$

For the optional part for any matrix A there exists an invertible matrix S and an upper triangular B such that $A = SBS^{-1}$. In fact B can be chosen to be the Jordan canonical form with entries only on the diagonal and off diagonal. Then the previous problem implies that

$$\det e^A = \det e^{SBS^{-1}} = \det Se^BS^{-1} = \det e^B = e^{\mathrm{Tr}\, B} = e^{\mathrm{Tr}\, S^{-1}AS} = e^{\mathrm{Tr}\, A}$$

where we used that det is multiplicative and $\mathrm{Tr}(S^{-1}AS) = \mathrm{Tr}\, A$. □

6. Let G be a group with subgroups H and K. Show that $H \cup K$ is a group if and only if one of H and K contains the other.

Proof. Suppose that $H \not\subset K$. Then there exists $h \in H - K$. For any $k \in K$ we have $h, k \in H \cup K$ and since $H \cup K$ is a group it follows that $hk \in H \cup K$. If $hk \in K$ it follows that $h \in K \cdot k^{-1} = K$ which is impossible by choice of h. Therefore $hk \in H$ and so $k \in h^{-1} \cdot H = H$ and so we deduce that $K \subset H$. □

7. Show that every cyclic group is abelian.

Proof. This is easy. Note that $x^m \cdot x^n = x^{m+n} = x^n \cdot x^m$. □

8. Let G be a group and $g \in G$. Show directly that g and g^{-1} have the same order.

Proof. Remember from class that for $h \in G$, $S_h = \{n \in \mathbb{Z} \mid h^n = 1\}$ is a subgroup of $\mathbb{Z}$ and is of the form $\mathrm{ord}(h)\mathbb{Z}$ where $\mathrm{ord}(h) > 0$, unless $S_h = \{0\}$ in which case $\mathrm{ord}(h) = \infty$. Therefore $\mathrm{ord}(h)$ is completely determined by S_h.

Since $g^n = 1$ iff $g^{-n} = (g^{-1})^n = 1$ it follows that $S_g = S_{g^{-1}}$ so g and g^{-1} have the same order. □

9. Prove that every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle x \rangle$ be a cyclic group and $H \subset G$ a subgroup. Let $S = \{n \in \mathbb{Z} \mid x^n \in H\}$. Since H is closed under division it follows that S is closed under subtraction and therefore $S \subset \mathbb{Z}$ is a subgroup. But then $S = a\mathbb{Z}$ for an integer a in which case $H = \langle x^a \rangle$ as desired. □

10. Let $n \geq 2$ be an integer. To a permutation $\sigma \in S_n$ attach the matrix $P(\sigma) = (a_{ij})$ such that for every i, $a_{\sigma(i),i} = 1$ and $a_{i,j} = 0$ if $i \neq \sigma(j)$. Show that P is a homomorphism $P : S_n \to \mathrm{GL}_n(\mathbb{R})$.

Proof. Let $\sigma, \tau \in S_n$. We need to verify that $P(\sigma)P(\tau) = P(\sigma\tau)$. In that case $P(\sigma)P(\sigma^{-1}) = P(1) = I_n$ and so $P(\sigma)$ is automatically invertible.

Suppose $P(\sigma) = (a_{ij})$ with $a_{\sigma(i),i} = 1$ for all i and $a_{i,j} = 0$ whenever $i \neq \sigma(j)$ and suppose that $P(\tau) = (b_{ij})$ with $b_{\tau(i),i} = 1$ for all i and $b_{i,j} = 0$ whenever $i \neq \tau(j)$. Let's compute $P(\sigma)P(\tau) = (c_{ij})$:

$$c_{ij} = \sum_k a_{ik} b_{kj}$$

As $b_{kj} = 0$ unless $k = \tau(j)$ we can simplify this to $c_{ij} = a_{i,\tau(j)} b_{\tau(j),j}$. But this is 0 unless $i = \sigma(\tau(j))$, in which case is it 1. Therefore $P(\sigma)P(\tau) = P(\sigma\tau)$ as desired. □