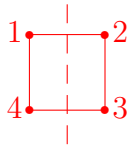
# ALGEBRA TEST #1

This exam is due Monday, October 17. Do two of the problems. You may use your book, but you may not communicate with others concerning the exam. In order to receive full credit your answer must be **complete**, **legible** and **correct**.

I have neither given nor received aid on this exam.

**Name:**_____

1. Draw a regular 4-gon and label the vertices with the numbers $1, 2, 3, 4$.




(a) Write the cycle decomposition of each element of $D_4 = \{1, r, r^2, r^3, f, rf, r^2f, r^3f\}$.

$$\begin{aligned} 1 &= 1 \\ r &= (1\ 2\ 3\ 4) \\ r^2 &= (1\ 3)(2\ 4) \\ r^3 &= (1\ 4\ 3\ 2) \end{aligned} \qquad \begin{aligned} f &= (1\ 2)(3\ 4) \\ rf &= (1\ 3) \\ r^2f &= (1\ 4)(2\ 3) \\ r^3f &= (2\ 4) \end{aligned}$$

(b) Is it possible to label the *edges* with $1, 2, 3, 4$ so that the cycle decomposition of each permutation in $D_4$ is the same as it was in (a)? (Show or explain.)

No. Depending on the axis you choose for the flip $f$, either $f$ fixes a vertex and no edge or it fixes an edge but no vertex. Either way, $f$ will have 1-cycles under one of its actions but not under the other action.

(c) For which $m$ (if any) do there exist labelings of the vertices and the edges of a regular $m$-gon with $1, \ldots, m$ so that the cycle decomposition of any permutation relative to the vertex labeling is the same as the cycle decomposition relative to the edge labeling?

If $m$ is even, then the axis of the flip $f$ either passes through two opposite vertices or pierces the middle of two opposite sides. If it passes through opposite vertices, then it fixes two vertices and no sides. If the axis pierces opposite sides, then it fixes two sides and no vertices. In either case, the number of fixed points ( = 1-cycles) of $f$ differs, so the cycle types differ.

But if $m$ is odd, then the vertices and edges can be labeled so that the cycle types of all rigid motions are the same with repect to the two labelings: just label so that each edge label matches the label on the opposite vertex.

2. If $G$ is a group and $m, n \in G$, then the *commutator of* $m$ *and* $n$ is $[m, n] := m^{-1}n^{-1}mn$. If $M$ and $N$ are subgroups, the *commutator of* $M$ *and* $N$ is subgroup generated by $\{[m, n] \mid m \in M, n \in N\}$.

(a) Show that $[M, N] = \{1\}$ iff every element of $M$ commutes with every element of $N$.

$[M, N] = \{1\}$ iff each of its generators equals 1 iff $m^{-1}n^{-1}mn = [m, n] = 1$ when $m \in M$ and $n \in N$ iff $mn = nm$ when $m \in M$ and $n \in N$.

(b) Show that a subgroup $N \leq G$ is normal iff $[G, N] \subseteq N$.

$N \triangleleft G$ iff for all $g \in G$ and $n^{-1} \in N$ it is the case that $g^{-1}n^{-1}g \in N$. But since $n, n^{-1} \in N$, we have $g^{-1}n^{-1}g \in N$ iff $g^{-1}n^{-1}gn \in N$. Thus, $N \triangleleft G$ iff $[g, n] \in N$ for all $n \in N$ and $g \in G$. The result now follows from the fact that $[G, N] \subseteq N$ iff the generators of $[G, N]$ lie in $N$.

(c) Show that if $N$ is a normal subgroup of $S_n$, then either $[S_n, N] = \{1\}$ or $N$ contains an element that is a product of exactly two transpositions. (Use the fact that $S_n$ is generated by transpositions.)

The problem should have said "exactly two distinct transpositions", otherwise the problem is trivial.

If $[S_n, N] \neq \{1\}$, then some $\tau \in S_n$ fails to commute with some $\nu \in N$. We may assume that $\tau$ is a transposition, since the transpositions generate $S_n$, and if $\nu$ commutes with a set of generators of $S_n$ it commutes with every element of $S_n$. Hence $1 \neq [\tau, \nu] \in [S_n, N] \subseteq N$, implying that $N$ contains $\tau^{-1}\nu^{-1}\tau\nu \neq 1$. But $\tau^{-1} \cdot (\nu^{-1}\tau\nu)$ is a product of two transpositions, since inverses and conjugates of transpositions are transpositions. The transpositions are distinct since their product is not 1.

(d) Show that if $N$ is a normal subgroup of $S_n$, $n > 4$, and $N$ contains an element that is a product of exactly two transpositions, then $N$ contains a 3-cycle.

$N$ contains a product of two distinct transpositions, so contains an element whose cycle decomposition is $(a\ b)(c\ d)$ or else is $(a\ b)(b\ c) = (a\ b\ c)$. In the latter case there is nothing to prove, while in the former case we can choose $e \notin \{a, b, c, d\}$ (since $n > 4$) and form the commutator $[(d\ e), (a\ b)(c\ d)] = [(d\ e), (c\ d)] = (c\ d\ e)$ which is a 3-cycle in $N$.

3. Suppose that $N_1 \lhd G_1$ and $N_2 \lhd G_2$.

(a) Show that the composite homomorphisms $G_1 \times G_2 \xrightarrow{\pi_1} G_1 \xrightarrow{\nu_1} G_1/N_1$ and $G_1 \times G_2 \xrightarrow{\pi_2} G_2 \xrightarrow{\nu_2} G_2/N_2$ induce a homomorphism $G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$ with kernel $N_1 \times N_2$.

We have seen that the product of maps $\nu_i \circ \pi_i \colon G_1 \times G_2 \to G_i/N_i$,

$$((\nu_1 \circ \pi_2) \times (\nu_2 \circ \pi_2))(g_1, g_2) = (\nu_1(g_1), \nu_2(g_2)) = (g_1N_1, g_2N_2),$$

with a common domain is a homomorphism from the domain group $G_1 \times G_2$ into the product $(G_1/N_1) \times (G_2/N_2)$. Its kernel consists of those $(g_1, g_2) \in G_1 \times G_2$ such that $(g_1N_1, g_2N_2) \in N_1 \times N_2$, namely it is $N_1 \times N_2$.

(b) Show that the homomorphism in (a) induces an isomorphism from $(G_1 \times G_2)/(N_1 \times N_2)$ to $(G_1/N_1) \times (G_2/N_2)$.

The image of the map in (a) consists of the set of all $(g_1N_1, g_2N_2)$ with $(g_1, g_2) \in G_1 \times G_2$, namely it is $(G_1/N_1) \times (G_2/N_2)$. By the First Isomorphism Theorem we have $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$.

(c) (This part is unrelated to (a) and (b).) Explain how the universal property of products establishes $G_1 \times G_2 \cong G_2 \times G_1$.

$G_1 \times G_2$ comes equipped with projection maps; the first projection $\pi_1$ is onto $G_1$ and the second projection $\pi_2$ is onto $G_2$. $G_2 \times G_1$ Also comes equipped with projection maps; the first projection $p_1$ is onto $G_2$ and the second projection $p_2$ is onto $G_1$. The u.p. of products applied to the pair $(p_2, p_1)$ induce a map $\varphi \colon G_2 \times G_1 \to G_1 \times G_2$ such that $\pi_1 \circ \varphi = p_2$ and $\pi_2 \circ \varphi = p_1$. Similarly, the u.p. yields a map $\psi \colon G_1 \times G_2 \to G_2 \times G_1$ such that $p_1 \circ \varphi = \pi_2$ and $p_2 \circ \psi = \pi_1$.

The composition $\theta = \varphi \circ \psi \colon G_1 \times G_2 \to G_1 \times G_2$ satisfies $\pi_i \circ \theta = \pi_i$, $i = 1, 2$. The identity function $\iota \colon G_1 \times G_2 \to G_1 \times G_2$ also satisfies $\pi_i \circ \iota = \pi_i$, $i = 1, 2$. The uniqueness part of the u.p. for products implies that $\theta = \varphi \circ \psi = \iota$. Similarly, $\psi \circ \varphi$ is the identity function. Hence $\varphi$ and $\psi$ are inverse isomorphisms between $G_1 \times G_2$ and $G_2 \times G_1$.

Remark: In this problem you shold avoid using the theorem that, for groups, a homomorphism is an isomorphism iff it is bijective. The problem is about the u.p. for products, and it is true even in categories where bijective homomorphisms need not be isomorphisms. (Or even in situations where 'bijective' doesn't make sense.)

4. In a HW problem (HW IV.4) you proved that any finite abelian group is a product of groups of prime power order. These factors of prime power order are called the *primary components* of the group. (A primary component of $p$-power order is called a $p$-primary component.)

This problem investigates the structure of the primary components of a finite abelian group.

(a) (Cyclic subgroups of maximal order split off.) Suppose $A$ is finite, abelian, and of prime power order. Let $z \in A$ have maximal order, and let $C = \langle z \rangle$. Let $H \leq A$ be a subgroup maximal for the property that $H \cap C = \{0\}$. Show that $H$ is a complement of $C$.

The order $|z| = p^k$ must be the least power of $p$ such that $p^k A = 0$.

We have $C \cap H = \{0\}$ by choice, so if $H$ fails to be a complement of $C$ it is because $C + H \neq A$. Assume that this is the case and choose an element $a \in A - (C + H)$ of least possible order. Assuming the group is written additively, we get that $a \notin C + H$ but $pa \in C + H$, say $pa = mz + h$. Now $0 = p^{k-1}(pa) = p^{k-1}mz + p^{k-1}h$, so $p^{k-1}mz = -p^{k-1}h \in C \cap H = \{0\}$, so $p^{k-1}m$ is a multiple of the order of $z$, so $p$ divides $m$. Choose $n$ so that $pn = m$. The element $b = a - nz \in C + A$ has the following properties:

(a) $b \notin C + H$. (Since $\langle C \cup \{a\} \rangle = \langle C \cup \{b\} \rangle$ and $a \notin C + H$.)

(b) $pb = h \in H$. (Since $pb = pa - pnz = pa - mz = h$.)

(c) $H' := \langle H \cup \{b\} \rangle$ properly extends $H$, but $H' \cap C = \{0\}$. (The first part follows from $b \notin H$, proved in (a). We proceed to prove the second part:)

To prove the second part of (c), assume instead that there exist $h' \in H$, $c \in C$ and $r \in \mathbb{Z}$ such that $h' + rb = c \neq 0$. It cannot be that $p$ divides $r$, since then the left hand side belongs to $H$ and the element $c$ belongs to $C - \{0\}$, while $H \cap C = \{0\}$. Thus, $r$ is relatively prime to $p$, and we may multiply $h' + rb = c$ by some number $s$ such that $sr \equiv 1 \pmod{|A|}$ to obtain $sh' + b = sc \neq 0$. This expresses $b$ as $sc - sh' \in C + H$, contrary to (a). This contradiction completes the proof. (What we have shown is that if $C + H \neq A$, then $H$ was not truly maximal among subgroups disjoint from $C$.)

(b) Deduce from (a) that $A$ is a product of cyclic groups.

Applying the Characterization of Products to the result in (a) proves that $A \cong C \times H$. Applying the argument repeatedly allows us to further factor $H$ until we have a complete factorization of $A$ into cyclic groups.

(c) Let $A[p] = \{a \in A \mid pa = 0\}$ be the annihilator of $p$ in $A$. ($A$ is considered as an additive group.) Show that if $A \cong \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_k}}$ with $1 \leq e_1 \leq e_2 \leq \cdots \leq e_k$, then $|A[p]| = p^k$ and $A/A[p] \cong \mathbb{Z}_{p^{e_1-1}} \times \cdots \times \mathbb{Z}_{p^{e_k-1}}$.

An element in $\mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_k}}$ is annihilated by $p$ iff it is annihilated coordinatewise, so $A[p] \cong p^{e_1-1}\mathbb{Z}_{p^{e_1}} \times \cdots \times p^{e_k-1}\mathbb{Z}_{p^{e_k}} \cong \mathbb{Z}_p^k$. This shows that $|A[p]| = p^k$. By problem 2(a),

$$\begin{aligned} A/A[p] &\cong (\mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_k}})/(p^{e_1-1}\mathbb{Z}_{p^{e_1}} \times \cdots \times p^{e_k-1}\mathbb{Z}_{p^{e_k}}) \\ &\cong \mathbb{Z}_{p^{e_1-1}} \times \cdots \times \mathbb{Z}_{p^{e_k-1}}. \end{aligned}$$

(d) Deduce from (c) that if $A$ is factored into cyclic subgroups, then the number of factors of order at least $p$ is uniquely determined. Then explain why the number of factors of order at least $p^2$ is uniquely determined. Then explain why the numbers $e_i$ from (c) are uniquely determined.

As we see, the number of cyclic factors of $A \cong \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_k}}$ of order at least $p$ is $k = \log_p |A[p]|$. It is not hard to see by induction, using (c), that the number of cyclic factors of $A$ of order at least $p^{r+1}$ is $\log_p |A[p^{r+1}]| - \log_p |A[p^r]|$. These numbers are independent of any chosen factorization, since annihilators are defined without reference to any factorization, and they allow us to recover the $e_i$'s from (c), so the $e_i$'s are uniquely determined.