THE JOHNS HOPKINS UNIVERSITY
Krieger School of Arts and Sciences
MIDTERM EXAM - FALL 2005
110.401 – ADVANCED ALGEBRA I

Instructor: Professor Carel Faber
Duration: 50 minutes November 2, 2005

No calculators allowed

Total = 100 points

NAME: Carel Faber

ETHICS PLEDGE:

I agree to complete this examination without unauthorized assistance from any person, materials, or device.

SIGNATURE:

DATE:

Motivate your answers!

1. [**15** points] Write the following element of S_7 as a product of (one or more) disjoint cycles of length at least two:

$$(1\,3\,5\,7)(2\,3\,6\,1\,4\,5)(7\,5\,3\,1).$$

ⓐ
$$\begin{array}{ll} 1\ 2\ 3\ 4\ 5\ 6\ 7 & \\ \downarrow & \text{first } (7531) \\ 7\ 2\ 1\ 4\ 3\ 6\ 5 & \\ \downarrow & \text{then } (236145) \\ 7\ 3\ 4\ 5\ 6\ 1\ 2 & \\ \downarrow & \text{then } (1357) \\ 1\ 5\ 4\ 7\ 6\ 3\ 2 & \end{array}$$

i.e. $\mapsto 1$, $2 \to 5 \to 6 \to 3 \to 4 \to 7 \to 2$.

Answer: $(1)(2\,5\,6\,3\,4\,7) = (2\,5\,6\,3\,4\,7)$.

ⓑ Like above, but "by hand":

$(1357)\ (236145)\ (7531)$

$1 \leftarrow 7 \longleftarrow 7 \longleftarrow 1$ so $1 \to 1$

$5 \leftarrow 3 \longleftarrow 2 \longleftarrow 2$ so $2 \to 5$, etc.

ⓒ of the form $\sigma \tau \sigma^{-1}$;
if $\tau = (a_1 a_2 \cdots a_k)$, then
$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2) \cdots \sigma(a_k))$.
Here: $\sigma\,(2\,3\,6\,1\,4\,5)$
$= (\sigma(2)\ \sigma(3) \cdots \sigma(5))$
$= (2\,5\,6\,3\,4\,7)$.

2. [**15** points] Determine the inverse of $\overline{12}$ in $\mathbb{Z}_{31}^*$.

Do the Euclidean algorithm & then use it backwards. $\mathbb{Z}_{31}^*$ = multiplicative group of units in $\mathbb{Z}_{31}$. By now we know that $\mathbb{Z}_{31}$ is a field, so $|\mathbb{Z}_{31}^*| = 31 - 1 = 30$. (We also know that $\mathbb{Z}_{31}^*$ is cyclic of order 30, but we don't need that of course.)

In any case, $\overline{12} \in \mathbb{Z}_{31}^*$ is a unit hence has an inverse.

Gcd, Eucl. algorithm: (we know already that $\gcd(31, 12) = 1$ but the point is to do the algorithm backwards!):

$\underline{31} = 2 \cdot \underline{12} + \underline{7}$
$\underline{12} = 1 \cdot \underline{7} + \underline{5}$
$\underline{7} = 1 \cdot \underline{5} + \underline{2}$
$\underline{5} = 2 \cdot \underline{2} + \underline{1} \leftarrow \gcd$
$\underline{2} = 2 \cdot \underline{1} + 0$

$\left.\begin{array}{l} 1 = \underline{5} - 2 \cdot \underline{2} \\ 2 = \underline{7} - \underline{5} \end{array}\right\}$ $1 = \underline{5} - 2(\underline{7} - \underline{5}) = 3 \cdot \underline{5} - 2 \cdot \underline{7}$ $(= 15 - 14, ✓)$

I underline the "important" numbers ....

$\underline{5} = \underline{12} - \underline{7} \Rightarrow 1 = 3(\underline{12} - \underline{7}) - 2 \cdot \underline{7} = 3 \cdot \underline{12} - 5 \cdot \underline{7}$ $(= 36 - 35, ✓)$

$\underline{7} = \underline{31} - 2 \cdot \underline{12} \Rightarrow 1 = 3 \cdot \underline{12} - 5 \cdot (\underline{31} - 2 \cdot \underline{12})$
$= 13 \cdot \underline{12} - 5 \cdot \underline{31}$ $(= 156 - 155, ✓)$

So: $1 \equiv 13 \cdot 12 \mod 31$
$\bar{1} = \overline{13} \cdot \overline{12}$ in $\mathbb{Z}_{31} \Rightarrow \overline{12}^{-1} = \overline{13}$ in $\mathbb{Z}_{31}^*$.

3. [**25** points] Let G be a group.

(a) [**4** points] Give the definition of an **automorphism** of G.

An automorphism of G is a homomorphism from G to itself that is a bijection.

So: $\overset{\text{mapping}}{\varphi}: G \to G$, φ is one-to-one (or injective) and onto (or surjective), and

$$\varphi(a * b) = \varphi(a) * \varphi(b),$$

if $*$ is the binary operation in G.

(↑usually written "$\cdot$"; or "$+$" sometimes when G is abelian).

We know that the automorphisms of G form a group under composition. We denote this group by $\mathrm{Aut}(G)$.

(b) [**8** points] For all $a \in G$, define $\sigma_a : G \to G$ by $\sigma_a(g) = aga^{-1}$. Show that $\sigma_a \in \mathrm{Aut}(G)$ for all $a \in G$.

⓪ σ_a is a mapping from G to G

① σ_a a homomorphism?

$$\sigma_a(gh) = agha^{-1} = ag\underbrace{a^{-1}a}_{=1}ha^{-1} = \sigma_a(g)\,\sigma_a(h), \text{ yes!}$$

② σ_a one-to-one?

$$\sigma_a(g) = \sigma_a(h) \Longleftrightarrow aga^{-1} = aha^{-1} \underset{(\text{in fact } \Leftrightarrow)}{\overset{\cdot a}{\Longrightarrow}} ag = ah \underset{(\Leftrightarrow)}{\overset{a^{-1}\cdot}{\Longrightarrow}} g = h, \text{ yes!}$$

③ σ_a onto? I.e., $\forall g \in G$, $\exists ?\, h \in G$: $\sigma_a(h) = g$?

Yes: $aha^{-1} = g \underset{\cdot a}{\Longrightarrow} ah = ga \underset{a^{-1}\cdot}{\Longrightarrow} h = a^{-1}ga$

and indeed $\sigma_a(a^{-1}ga) = a(a^{-1}ga)a^{-1} = g$.

Hence $\sigma_a \in \mathrm{Aut}(G)$, $\forall a \in G$. QED.

(c) [**5** points] For a, $b \in G$, show that $\sigma_a\sigma_b = \sigma_{ab}$. Show also that σ_1 equals the identity map 1_G and that $(\sigma_a)^{-1} = \sigma_{a^{-1}}$ for $a \in G$. Conclude that $\{\sigma_a | a \in G\}$ is a subgroup of $\mathrm{Aut}(G)$.

Get it straight!

$\sigma_a \sigma_b$ is multiplication in Aut(G), where the group operation is <u>composition</u>.

So: $(\sigma_a\sigma_b)(g) = \sigma_a(\sigma_b(g)) = \sigma_a(bgb^{-1}) = a(bgb^{-1})a^{-1}$

$= abgb^{-1}a^{-1} = (ab)g(ab)^{-1} = \sigma_{ab}(g)$, $\forall a,b,g \in G$;

So $\sigma_a\sigma_b = \sigma_{ab}$.

Then $\sigma_a\sigma_{a^{-1}} = \sigma_{aa^{-1}} = \sigma_1 = \sigma_{a^{-1}a} = \sigma_{a^{-1}}\sigma_a$

and $\sigma_1(g) = 1g1^{-1} = g$, so $\sigma_1 = 1_G \in \mathrm{Aut}(G)$,

and $(\sigma_a)^{-1}$, the inverse mapping of σ_a, is $\sigma_{a^{-1}}$ (check!).

$\{\sigma_a | a \in G\}$ fulfills all the criteria for the subgroup test, so it is a subgroup of Aut(G).

We denote this subgroup by $\mathrm{Inn}(G)$, the subgroup of inner automorphisms of G.

(d) [**8** points] For $\tau \in \mathrm{Aut}(G)$ and $a \in G$, show that

$$\tau\sigma_a\tau^{-1} = \sigma_{\tau(a)}\,.$$

Conclude that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

Again, use the <u>composition</u> as group operation:

$(\tau\sigma_a\tau^{-1})(g) = (\tau\sigma_a)(\tau^{-1}(g)) = \tau(\sigma_a(\tau^{-1}(g)))$

$= \tau(a\tau^{-1}(g)a^{-1}) = \tau(a)\,\tau(\tau^{-1}(g))\,\tau(a^{-1})$

$= \tau(a)\,g\,\tau(a^{-1})$. But $\tau \in \mathrm{Aut}(G)$, so $\tau(a^{-1}) = (\tau(a))^{-1}$.

So: $= \tau(a)\,g\,(\tau(a))^{-1} = \sigma_{\tau(a)}(g)$, so $\boxed{\tau\sigma_a\tau^{-1} = \sigma_{\tau(a)}}$.

But $\forall \tau \in \mathrm{Aut}(G)$, $\forall x \in \mathrm{Inn}(G)$:

$\tau x \tau^{-1} \in \mathrm{Inn}(G)$! So Inn(G) is a normal subgroup of Aut(G).

4. [**45** points] Let $p > 2$ be an odd prime number and let G be a group of order $2p$.

(a) [**5** points] List the possible orders of elements of G.

All (positive) divisors of $2p$: $1, 2, p$, and $2p$.

(Of course the only elt. of G of order 1 is the identity elt. of G.)

(b) [**5** points] State Cauchy's theorem and conclude from it that G has an element of order 2 and an element of order p.

Cauchy: if G is a finite group, and q is a prime number dividing the order of G, then G has an element of order q. (How beautiful!)

Here: Take $q = 2$; G has an elt. of order 2.

Take $q = p$: G has an elt. of order p.

(c) [**5** points] If G is abelian, show that G is in fact cyclic. (Hint: consider the product of an element of order 2 and an element of order p.)

If x has order 2 and y has order p, then what is the order of xy?

$$(xy)^2 = xyxy \underset{G \text{ abelian}}{=} x^2y^2 = y^2 \neq 1 \quad (\text{since } p > 2).$$

So the order of xy is not 1 or 2.

$$(xy)^p = \cdots \underset{G \text{ abelian}}{=} x^p y^p = x^p \underset{\substack{\uparrow \\ p \text{ odd}}}{=} x \neq 1 \quad (\text{since } x \text{ has } \underline{\text{order}} \ 2).$$

So the order of xy is not (1 or) p.

By (a), the order of xy is then $2p$. That means: if G is abelian, then G is cyclic!

(d) [**5** points] Let b and c be two elements of G of order p. Show that $\langle b\rangle = \langle c\rangle$ or $\langle b\rangle \cap \langle c\rangle = \{1\}$.

$\langle b\rangle$ = the subgroup generated by p.

$|\langle b\rangle|$ = order of b $= p$.

So $\langle b\rangle$ and $\langle c\rangle$ are two subgroups of G of order p.

Let $H = \langle b\rangle \cap \langle c\rangle$ be their intersection.

It is also a subgroup of G! And of $\langle b\rangle$ and of $\langle c\rangle$.

So its order is 1 or p:

if $|H| = 1$, then $\langle b\rangle \cap \langle c\rangle = \{1\}$;

if $|H| = p$, then $\langle b\rangle \cap \langle c\rangle = \langle b\rangle$ (both of order p)

and $\langle b\rangle \cap \langle c\rangle = \langle c\rangle$, (" " " ")

So $\langle b\rangle = \langle b\rangle \cap \langle c\rangle = \langle c\rangle$.

(e) [**5** points] Use (d) to show that the number of elements of G of order p is a multiple of $p-1$. Hence it is $p-1$ or $2p-2$.

If x has order p, then $\langle x\rangle$ has order p, and contains exactly $p-1$ elements of order p.

So elts. of order p come in "clumps" of size $p-1$, according to the subgroup of order p of G that they generate.

So their number is a multiple of $p-1$ (since the intersection of two distinct subgroups of order p equals $\{1\}$, so no elt. of order p lives in two distinct subgroups of order p).

So $p-1$, or $2p-2$, or $3p-3$, ...

But $3p-3$ is already too much!

in G, of order $2p$, have an elt. of order 1, and an elt. of order 2, so at most $2p-2$ elts. of order p.

So either $p-1$ or $2p-2$ elts. of order p.

In fact, we are going to show that G has exactly $p-1$ elements of order p: assuming that G has $2p-2$ elements of order p, we will arrive at a contradiction. So assume from now on that G has $2p-2$ elements of order p.

(f) [**5** points] Show that G has then a unique element of order 2.

As above: $2p-2$ elts of order p

$\exists$ elt. of order 1 (unique in fact)

$\exists$ elt. of order 2 (unique ???)

$\geqslant 2p$ elts.

But we have $2p$ elts., so the elt. of order 2 is unique (and the elt. of order 1 is unique as well, but we knew that already).

(g) [**5** points] Show that the unique element of order 2 is central in G.

$x \in G$ Central $\Leftrightarrow \forall y \in G: \ xy = yx$

$\Leftrightarrow \forall y \in G: \ yxy^{-1} = x$.

But if x has order 2, then yxy^{-1} has order 2 (reason: $g \mapsto ygy^{-1}$ is an automorphism of G, so "all structure is preserved", so orders of elts. are preserved, so $\text{order}(g) = \text{order}(ygy^{-1})$).

But x was unique of order 2, so $x = yxy^{-1} \ \forall y \in G$,

QED.

Recall the following result: let K be a subgroup of the center $Z(H)$ of a group H. If H/K is cyclic, then H is abelian.

(h) [**5** points] Use this result to show that G is abelian.

Take $K = \langle x \rangle$, for x of order 2, then K of order 2, and $K = \{1, x\}$, so $K \leq Z(G)$ (so K is normal).

G/K is then of order p; so G/K is cyclic.

↖ a group

By the result above, G is abelian.

(i) [**5** points] Derive a contradiction by using (c).

If G is abelian, then it is cyclic, so there is an elt. of order $2p$.

But there is no room for that anymore!

$2p-2$ of order p

1 of order 1

1 of order 2

$2p$, no room for an elt. of order $2p$.

↯

Conclusion: A nonabelian group G of order $2p$ has $p-1$ elements of order p and p elements of order 2.

Right! Exactly $p-1$ of order p, 1 of order 1, so the rest (p elements) must be order 2 (since if it was $2p$, then G cyclic, hence abelian).