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

Instructor: Professor Carel Faber
Duration: 180 minutes December 19, 2005

No calculators allowed **Total = 200 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. [**20** points] Let p and q be two distinct prime numbers. Let G be a group of order pq. Prove: if G is abelian, then it is cyclic.

By Cauchy's theorem, G has elements of order p and of order q. Let x be an elt. of order p and let y be an elt. of order q. Consider $z = xy$.

Then $z^p = (xy)^p \overset{G \text{ abelian}}{=} x^p y^p = y^p \neq 1$ (since $q \nmid p$)

and $z^q = (xy)^q \overset{\downarrow}{=} x^q y^q = x^q \neq 1$ (since $p \nmid q$).

So the order of z is neither p nor q nor 1. But it divides pq (by Lagrange) and the only possibility is that it equals pq. Then $\langle z \rangle$ has pq elements, so $\langle z \rangle = G$, and G is cyclic.

2. [**30** points]

(a) [**10** points] Determine the set $B = \{\, |g| \,|\, g \in S_5\}$ of orders of elements of S_5.

Each elt. $x \neq (1)$ of S_5 can be written as a product of disjoint cycles of lengths ≥ 2; then the order of x is the l.c.m. of the lengths of the cycles.

The possibilities are: (k_i for the cycle lengths; $k_i \geq 2$)

$\sum k_i \leq 5$ of course

May assume $k_1 \geq k_2 \geq \cdots \geq 2$

① $k_1 = 5$ order 5

② $k_1 = 4$ order 4

③ $k_1 = 3$ order 3

④ $k_1 = 3,\ k_2 = 2$ order 6

⑤ $k_1 = 2,\ k_2 = 2$ order 2

⑥ $k_1 = 2$ order 2

Finally, (1) has order 1. So

$$B = \{1, 2, 3, 4, 5, 6\}.$$

(b) [**10** points] Prove that S_5 does not contain abelian subgroups of order 10 or 15.

$10 = 2 \cdot 5$; $15 = 3 \cdot 5$.

By Problem 1, such groups would be cyclic. But S_5 doesn't contain elts. of orders 10 or 15. QED.

(c) [**10** points] Prove that S_5 contains abelian subgroups of order 6, but that A_5 does not contain an abelian subgroup of order 6.

$\langle (123)(45) \rangle$ is a subgroup of order 6 of S_5 which is cyclic hence abelian.

If A_5 were to contain an abelian subgroup of order 6, it would be cyclic (as we all know, or by Problem 1). But the only elements of S_5 of order 6 are the product of two disjoint cycles of lengths 3 and 2. These elements are <u>odd</u> permutations, hence not elements of A_5. QED.

3. [**30** points]

(a) [**15** points] Let $n \geq 2$ be an integer and suppose that H is a subgroup of odd order of S_n. Show that H is necessarily a subgroup of A_n.

Put $K := H \cap A_n$. If $H = K$ then $H \subseteq A_n$, so suppose $K \subsetneq H$. Let $x \in H \setminus K$: $x \in H$, $x \notin K$. Then $S_n = A_n \amalg xA_n$, hence $H = K \amalg xK$. But $|K| = |xK|$, contradiction with the fact that $|H|$ is odd. QED.

Or: each elt. of H has odd order, which is the lcm of the orders of the cycles in the disjoint cycle decomposition. So each elt. of H is a product of cycles of odd length, so a product of elts. of A_n, so H is a subgroup of A_n.

(b) [**15** points]* Prove that A_5 does not contain a subgroup of order 15. (This is rather difficult. I thought I would give you a chance to distinguish yourself. I recommend that you try the other problems first.)

Suppose that $G \subset A_5$ is a subgroup of order 15. By Cauchy, G contains elements of order 3 and order 5.

An elt. of order 5 is a 5-cycle $(a\ b\ c\ d\ e)$ with $\{a, b, c, d, e\} = \{1, 2, 3, 4, 5\}$.

If $\sigma(a) = 1$, $\sigma(b) = 2$, $\cdots$, $\sigma(e) = 5$, then

$$\sigma\,(abcde)\,\sigma^{-1} = (12345).$$

$\sigma G \sigma^{-1}$ is another (or identical) subgroup of A_5 (!) of order 15, so we may assume $(12345) \in G$.

Next, consider the 3-cycles $(f\ g\ h)$. They determine a subset $\{f, g, h\}$. There are $10 = \binom{5}{3}$ such subsets; hence A_5 has 20 3-cycles.

(3-cycles are the only elts. of order 3)

If $(fgh) \in G$, then $\tau(fgh)\tau^{-1} \in G$, for $\tau = (12345)$.
This is $(\tau(f)\tau(g)\tau(h))$, determining a different
subset: $\{\tau(f), \tau(g), \tau(h)\} \neq \{f, g, h\}$.

If $\{f,g,h\} = \{1,2,3\}$, we get the 5 subsets

$\{1,2,3\}$, $\{2,3,4\}$, $\{3,4,5\}$, $\{4,5,1\}$, $\{5,1,2\}$; (A)

if $\{f,g,h\} = \{1,2,4\}$, we get the 5 subsets

$\{1,2,4\}$, $\{2,3,5\}$, $\{3,4,1\}$, $\{4,5,2\}$, $\{5,1,3\}$. (B)

These are all 10 possible subsets.

We conclude: 5 of the 10 subsets, either (A) or (B), occur; hence G contains 10 elements of order 3 (with (fgh) also (hgf), etc.).

We have found all elts. of G !

10 of order 3; 1 of order 1; and $\tau, \tau^2, \tau^3, \tau^4$ of order 5. (Total $15 = |G|$.)

Finally we obtain our contradiction:

Case (A): $(123) \in G$, $(234) \in G$; then $(123)(234) \in G$, but $(123)(234) = (12)(34)$, ↯;

Case (B): $(124), (235) \in G$; then $(124)(235) \in G$, but $(124)(235) = (12354)$ is not a power of τ, ↯.

QED.

4. [**30** points] Let $G = \mathbb{Z}_{13}^* = \mathbb{Z}_{13} - \{0\}$ be the multiplicative group of the field $\mathbb{Z}_{13}$. We know that G is a cyclic group.

(a) [**6** points] Determine a generator for G. Note: $|G| = 12$.

Let's try: $2^2 = 4$, $2^3 = 8$, $2^4 = 16 = 3$, $2^6 = 64 = 12$; then the order of 2 must be 12, and $\langle 2 \rangle = G$.

(b) [**6** points] How many elements of G are generators of G?

G is cyclic of order 12, hence $G \cong \mathbb{Z}_{12}$ (group with addition). The generators of $\mathbb{Z}_{12}$ are $\bar{a}$, $1 \leq a \leq 12$, such that $\gcd(a, 12) = 1$. Their number equals $\varphi(12)$ (Euler's φ-function). $\varphi(12) = \varphi(3)\varphi(4) = 2 \cdot 2 = 4$. (since $\gcd(3,4)=1$)

Answer: 4.

(c) [**6** points] Find all generators of G. The generators of $\mathbb{Z}_{12}$ are $\bar{1}, \bar{5}, \bar{7}, \bar{11}$. The generators of G are $2 = 2^1$, $2^5 = 32 = 6$ (mod 13!), $2^7 = 4 \cdot 2^5 = 4 \cdot 6 = 24 = 11$, and $2^{11} = 2^{-1} = \frac{1}{2} = \frac{14}{2} = 7$.

Answer: 2, 6, 7, and 11.

(d) [**6** points] Determine the set $B = \{\, |g| \mid g \in G \,\}$ of orders of elements of G.

Easy: all divisors of 12.

$B = \{1, 2, 3, 4, 6, 12\}$.

(e) [**6** points] For each element b of B, find an element g of G of order b.

$b = 12$ $\quad g = 2$

$b = 6 = \frac{12}{2}$ $\quad g = 2^2 = 4$

$b = 4 = \frac{12}{3}$ $\quad g = 2^3 = 8$

$b = 3 = \frac{12}{4}$ $\quad g = 2^4 = 16 = 3$

$b = 2 = \frac{12}{6}$ $\quad g = 2^6 = 64 = 12 \ (= -1)$

$b = 1$ $\quad g = 1$

5. [**30** points] Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ of degree 4.

(a) [**15** points] Let p and q be two distinct prime numbers. Let $f_p(x) \in \mathbb{Z}_p[x]$ be the reduction of $f(x)$ modulo p and let $f_q(x) \in \mathbb{Z}_q[x]$ be the reduction of $f(x)$ modulo q. Suppose that $f_p(x)$ is the product of two irreducible polynomials in $\mathbb{Z}_p[x]$ of degree 2 and that $f_q(x)$ is the product of two irreducible polynomials in $\mathbb{Z}_q[x]$ of degrees 1 and 3 respectively. Prove that $f(x)$ does not admit a proper factorization in $\mathbb{Z}[x]$.

In $\mathbb{Q}[x]$, $f(x)$ factors as a product of monic irreducible polynomials. Their degrees form a so-called partition of 4:

4 ; 3+1 ; 2+2 ; 2+1+1 ; 1+1+1+1

are the five possibilities.

By Gauss's Lemma, a factorization in $\mathbb{Q}[x]$ yields a (proper) factorization in $\mathbb{Z}[x]$ (and the degrees of the factors don't change).

A factorization in $\mathbb{Z}[x]$ may be assumed to be a factorization in monic polynomials, since $f(x)$ is monic.

Reducing it modulo a prime gives a similar factorization (but the factors are not necessarily irreducible).

Modulo p, we find "2+2". Hence in $\mathbb{Z}[x]$ we have "2+2" or "4" as the only possibilities.

Modulo q, we find "3+1". Hence in $\mathbb{Z}[x]$ we have "3+1" or "4" as the only possibilities.

Combine the two statements: "4" is the only possibility, so $f(x)$ does not admit a proper factorization in $\mathbb{Z}[x]$.

$f(x) :=$

(b) [**15** points] Prove that $x^4 - 2x^3 + x^2 + 2x + 3$ does not admit a proper factorization in $\mathbb{Z}[x]$.

We try our luck:

$p = 2$: $f_2(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2$, (in $\mathbb{Z}_2[x]$)

type "2+2", since $x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

$q = 3$: $f_3(x) = x^4 + x^3 + x^2 + 2x$

$= x(x^3 + x^2 + x + 2)$.

Put $g_3(x) = x^3 + x^2 + x + 2$. Then

$g_3(0) = 2$, $g_3(1) = 2$, $g_3(-1) = 1$.

Hence g_3 is irreducible (of degree 3 w/o zeroes), so f_3 has type "3+1".

Part (a) applies and we obtain the desired conclusion.

10

6. [**30** points] Let $f(x) \in \mathbb{Z}_5[x]$ be the polynomial $x^2 + 2x + 3$.

(a) [**10** points] Prove that $f(x)$ is irreducible in $\mathbb{Z}_5[x]$.

$f(0) = 3$, $f(1) = 6 = 1$, $f(2) = 11 = 1$,

$f(3) = 9 + 6 + 3 = 18 = 3$, $f(4) = 16 + 8 + 3 = 27 = 2$.

$f(x)$ has no zeroes, deg. 2 : irreducible.

(b) [**10** points] Let E be the field $\mathbb{Z}_5[x]/(f(x))$ (the factor ring of $\mathbb{Z}_5[x]$ by the ideal generated by $f(x)$). Denote the element $x + (f(x))$ of E by t. Determine the order of t as an element of the multiplicative group E^*.

E is a field with 25 elements ($a + bt$, $a, b \in \mathbb{Z}_5$).

E^* is a cyclic group with 24 elements.

The possible orders of t are the divisors of 24:

$1, 2, 3, 4, 6, 8, 12, 24$.

$t \neq 1$; $t^2 = 3t + 2 \neq 1$; $t^3 = 3t^2 + 2t = 9t + 6 + 2t$

$= 11t + 6 = t + 1 \neq 1$; $t^4 = t(t^3) = t(t+1) = t^2 + t$

$= 4t + 2 \neq 1$; $t^6 = (t+1)^2 = t^2 + 2t + 1 = 3t + 2 + 2t + 1$

$= 5t + 3 = 3$; $t^8 = t^6 \cdot t^2 = 3(3t + 2) = 9t + 6 = 4t + 1 \neq 1$;

$\neq 1$

$t^{12} = (t^6)^2 = 3^2 = 9 = 4 \neq 1$; So order$(t) = 24$.

(t happens to be a generator of E^*).

(c) [**10** points] Find an element of order 3 of E^*.

t^8 has order 3.

$t^8 = 4t+1 = -t+1$ has order 3.

Check: $(-t+1)^3 = -t^3+3t^2-3t+1$

$= -t-1+9t+6-3t+1 = 5t+6 = 1$

(and $-t+1 \neq 1$). ✓

7. [**30** points]

(a) [**20** points] Determine the greatest common divisor of x^2+1 and x^3+1 in $\mathbb{Q}[x]$ and write it as a linear combination of these two polynomials with coefficients in $\mathbb{Q}[x]$.

$$\begin{array}{r|l} x^2+1 & x^3+1 \\ & x^3+x \\ \hline & -x+1 \end{array} \qquad x^3+1 = x(x^2+1) - (x-1)$$

$$x^2+1 = (x+1)(x-1) + 2$$

Hence the gcd will be the monic constant polynomial 1.

To "save fractions", let's work with 2 for the moment:

$$\begin{array}{r|l} x-1 & x^2+1 \\ & x^2-x \\ \hline & x+1 \\ & x-1 \\ \hline & 2 \end{array}$$

$$2 = -(x+1)(x-1) + (x^2+1) =$$

$$= (x+1)\left((x^3+1) - x(x^2+1)\right) + (x^2+1)$$

$$= (x+1)(x^3+1) + (1-x^2-x)(x^2+1)$$

$$= (x+1)(x^3+1) - (x^2+x-1)(x^2+1). \quad \text{(check!)}$$

So $1 = \frac{1}{2}(x+1)(x^3+1) - \frac{1}{2}(x^2+x-1)(x^2+1)$. (Answer)

(b) [**10** points] Determine the greatest common divisor of x^2+1 and x^3+1 in $\mathbb{Z}_2[x]$ and write it as a linear combination of these two polynomials with coefficients in $\mathbb{Z}_2[x]$.

$$
\begin{array}{r|l}
x^2+1 & x^3+1 \\
 & x^3+x \\
\hline
 & x+1
\end{array}
\qquad x
$$

and $x^2+1 = (x+1)^2$.

So the gcd will be $x+1$.

And $x^3+1 = x(x^2+1) + x+1$

So $x+1 = (x^3+1) - x(x^2+1)$

$= (x^3+1) + x(x^2+1)$ (answer).