Final Exam, Math 4107

April 28, 2008

NO CALCULATORS ARE ALLOWED FOR THIS EXAM!

Instructions. Work any 8 of the following 10 problems.

1. Find integers x and y such that

a. $76x + 47y = 1$.

b. $68x \equiv 1 \pmod{109}$.

2.

a. Determine the number of permutations of the set $X = \{A, B, C, D, E, F\}$.

b. Let $Y = \{G, H, I, J, K, L\}$. Let $\varphi : X \to Y$ be given by

$$\varphi = \begin{pmatrix} A & B & C & D & E & F \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ G & H & I & J & K & L \end{pmatrix}.$$

Show that every bijection $\psi : X \to Y$ can be written as

$$\Psi = \theta \circ \varphi, \text{ where } \theta \in S_Y.$$

c. Determine the number of surjections

$$\psi : X \to Y.$$

d. Determine the number of injections

$$\psi : X \to Y.$$

3. Suppose that G is a group that acts on the set

$$S \ := \ \{1,\ 2,\ 3\}.$$

Suppose that there is at least one element of G that acts non-trivially on S (i.e. there is an element $g \in G$ that doesn't just map $1 \to 1$, $2 \to 2$ and $3 \to 3$). Show that if

$$|G| \ > \ 6,$$

then G is non-simple. Justify all the steps in your proof.

4.

a. Consider the permutation

$$(1\ 2\ 3\ 4\ 5\ 6) \ \in \ S_{100}.$$

Explain why it cannot be written as a product of 3-cycles.

b. Write it as a product of transpositions.

c. Explain why $(1\ 2\ 3\ 4\ 5)$ is conjugate to the product of cycles

$$(50\ 49)(49\ 51)(51\ 53)(53\ 48).$$

d. Give an example of a pair of elements x and y belonging to a finite group, such that each has order 2, and yet their product has order 5.

5. Suppose that φ is a homomorphism from a finite group G to itself.

a. If $\varphi(x) = x^2$, show that G is abelian.

b. Show that the set of elements $y \in G$ that commute with some fixed $x \in G$, form a subgroup of G.

c. Show that if $\varphi(x) = x^2$ for more than 75% of the elements $x \in G$, then G is abelian. Hint: To prove this, first show that for every $x \in G$, more than $|G|/2$ of the $y \in G$ satisfy both

$$\varphi(y) \ = \ y^2 \ \text{ and } \varphi(xy) \ = \ (xy)^2.$$

Now think about what this means in light of part b (and Lagrange's theorem...).

6. a. State the Sylow Theorems.

b. State the First Isomorphism Theorem for groups.

c. State Lagrange's Theorem.

d. State Cayley's Theorem for groups.
e. State the Orbit-Stabilizer Theorem.

7. Suppose that G is a group of order 33. Show that G is abelian. Justify every step, and quote all the relevant theorems you use.

8.

a. Show that every finite Integral Domain is a field.
b. Find an example of an infinite Integral Domain that is not a field.
c. Show that if R is a ring containing a zero divisor, then $R[x]$ does not have the unique factorization property (Hint: Cook up an example of a polynomial that factors in two different ways as a product of irreducibles.)

9. Given a polynomial $f(x) \in \mathbb{Z}[x]$, we let $\overline{f}(x)$ be its image under the mod p homomorphism

$$\varphi \; : \; \mathbb{Z}[x] \; \longrightarrow \; (\mathbb{Z}/p\mathbb{Z})[x].$$

a. Show that if $f(x)$ is monic, and if $\overline{f}(x)$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.
b. Give an example of a polynomial $f(x) \in \mathbb{Z}[x]$ such that $\overline{f}(x)$ is irreducible in $(\mathbb{Z}/3\mathbb{Z})[x]$, and yet $f(x)$ is reducible in $\mathbb{Z}[x]$.

10.

a. Show that if α is a prime element of an integral domain R (here α is said to be a prime element if when $\alpha|\beta\gamma$, we have that either $\alpha|\beta$ or $\alpha|\gamma$), then α is irreducible (here α is said to be irreducible if when $\alpha = bc$, we have that either b or c is a unit).
b. Observe that $x^2 - 2$ is irreducible in $\mathbb{Z}[x]$. Yet show that the ideal $I = (x^2 - 2)$ is not a maximal ideal. Hint: One way to show this is to construct a larger ideal $J \neq \mathbb{Z}[x]$ containing I (think about the example in class showing that $\mathbb{Z}[x]$ is not a PID); however, there are other, less direct ways to show this as well.