Chris Bendel and Peter Cholak Math 222 - Sample Exam 2 Wednesday, April 14

The exam will cover sections 6.1-6.3, 7.1-7.3, 8.2, 8.4, 9.1, 9.2 and will have format as outlined below.

(4 points each) **Define** the following terms:

a) *relatively prime* polynomials

b) *field*

c) *Gauss imaginary*

d) *transposition*

(2 points each) Answer **True** or **False** - no work required:

a) The polynomial $P(x) = 2x^3 + x^2 + 3$ is irreducible over $\mathbb{Z}_5$.

b) $GF(3, x^5 + 2x + 1)$ contains 242 elements.

c) The negative real numbers under multiplication is a group.

d) The permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 7 & 1 & 8 & 2 & 9 & 5 & 4 \end{pmatrix}$ is even.

Part III: Computational Problems - there will be a few problems something *like* the following for a total of 45 points.

Completely factor $P(x) = x^3 + 2x + 3$ over $\mathbb{Z}_5$.

Find a greatest common divisor of $P(x) = x^5 + 4x^3 + 3x^2 + 4x + 1$ and $Q(x) = x^4 + x^3 + 2x + 1$ over $\mathbb{Z}_5$.

Find the remainder when dividing x^{51} by $x + 4$ over $\mathbb{Z}_7$.

For which $a \in \mathbb{Z}_5$ is $P(x) = x^3 + x + a$ irreducible over $\mathbb{Z}_5$?

Find the inverse of the element $1 + 2\beta$ in $GF(3, x^2 + x + 2)$, where β is the associated Galois imaginary.

Let $f(x) = x^3 + x + 1$ and α be the associated Galois imaginary in $GF(2, f(x))$. Find all integers i such that $f(\alpha^i) = 0$.

Find all primitive elements in $GF(2, x^4 + x + 1)$.

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 7 & 1 & 8 & 2 & 9 & 5 & 4 \end{pmatrix}$ and $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 9 & 8 & 7 & 6 & 5 & 4 \end{pmatrix}$.

a) Express both σ and τ in disjoint cycle notation and as a product of transpositions.

b) Express σ^{-1} and $\sigma\tau$ in disjoint cycle notation.

c) Find the orders and parity of σ, τ, and $\sigma\tau$.

Let $G = \mathbb{Q}^*$ be the nonzero rational numbers and consider the following multiplication on G: $x * y \equiv 2xy$ where multiplication is as usual on the right hand side. This forms a group.

a) Find the identity element, 1_G, of G.

b) Find the inverse of 3 in G.

Consider the following hypothetical multiplication table for a group G:

G	e	a	b
e	e	a	b
a	a	e	a
b	b	a	e

The table defines a multiplication, but the nature of the table should suggest that G is in fact *not* a group. Which of the properties of a group fail? Which hold. Explain.

Consider the following set of matrices:

$$G \equiv GL_2(\mathbb{R}) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ and } \det(A) \neq 0\}$$

G is a group under matrix multiplication - called the general linear group of 2 by 2 invertible matrices over the real numbers. Why is G closed under multiplication? What is the identity element? Why? Why does each matrix have an inverse? What is the inverse of the element $\begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix}$?

How many elements of order 2 are there in D_{125}? Explain.

Part IV: Proofs - *exactly* two of the following problems will appear. They'll be worth 15 points each.

Let a and b be two elements of a field. Prove that $a \cdot b = 0$ in F if and only if a or b is zero.

Let p be a prime number and suppose that $\mathbb{Z}_p$ contains an element c which is not a cube (in $\mathbb{Z}_p$). Show that there exists a field with p^3-elements.

Let p be a prime number and $P(x)$ be an irreducible polynomial of degree ν over $\mathbb{Z}_p$. Suppose that n is a positive integer relatively prime to $p^\nu - 1$. Prove that there is exactly one nth root of unity in $GF(p, P(x))$.

Let $\alpha \in GF(p, P(x))$ be primitive. Show that α^2 is primitive if and only if $p = 2$.

Let a, b, c be elements of a group G. Prove that if $a \cdot b = a \cdot c$, then $b = c$. Can we make the same conclusion if $b \cdot a = a \cdot c$? Why or why not?

Let a and b be elements of a group G. Prove that if $(a \cdot b)^2 = a^2 \cdot b^2$, then $a \cdot b = b \cdot a$.

Let G be a group. Prove that if $x^2 = 1$ for each $x \in G$, then G is abelian.

Let G be a group. Prove that if $a \cdot b = 1_G$ for some $a, b \in G$, then $b = a^{-1}$.