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

Be sure to carefully write up your answers. Be sure to explain your answers.

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

a) *irreducible* polynomial.

b) $GF(p, P(x))$ where $P(x)$ is an irreducible polynomial of degree ν over $\mathbb{Z}_p$.

c) *order* of an element in a group.

d) *primitive* element in a finite field with p^ν elements.

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

a) The polynomial $x^4 + 2x^2 + 1$ is irreducible over $\mathbb{Z}_3$.

b) The order the number 2 in the group $(\mathbb{Z}_3, +)$ is 2.

c) The set of 10th roots of unity in $\mathbb{C}$ is a group (under multiplication).

d) Each element $\zeta \neq 0, 1$ in $GF(2, x^5 + x^2 + 1)$ is primitive.

(10 points) Find the remainder when x^{73} is divided by $x + 2$ in $\mathbb{Z}_5$.

(15 points) Consider the field $GF(2, x^4 + x + 1)$. Let β be the associated Galois imaginary. β is primitive. Why? Find the inverse of $\beta^2 + \beta$ as a power of β.

(10 points) Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 8 & 1 & 4 & 2 & 9 & 3 & 7 \end{pmatrix}$.

a) Write σ^{67} in disjoint cycle notation.

b) Is σ^{35} even or odd? Why?

(10 points) The set $G = \{4, 8, 16\}$ is a group under multiplication modulo 28.

a) Find the identity element of G.

b) Find the inverses of the remaining elements in G.

(15 points) 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.

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