Peter Cholak and Juan Migliore Math 222 - Exam 2 Wednesday, April 25

Except where noted, be sure to show all your work.

(4 points each for a total of 20 points) **Define** the following terms:

a) *irreducible polynomial.*

b) $GF(p, P(x))$, where $P(x)$ is irreducible and p is prime.

c) an *even permutation.*

d) a *group.*

e) The *symmetric group* S_n.

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

a) The dihedral group D_4 is not abelian.

b) The order of $(\mathbb{Z}_n, +)$ is n.

c) The set of *primitive* 8th roots of unity in $\mathbb{Z}_{17}$ is a group (under multiplication).

d) Let p be a prime number. The multiplicative group $(\mathbb{Z}_p \backslash \{0\}, \cdot)$ has at least one element of order p. (Notice this says p and not $p - 1$.)

e) Let p be a prime number and let $P(x)$ be a polynomial of degree d that is irreducible over $\mathbb{Z}_p$. Let $G = (GF(p, P(x)) \backslash \{0\}, \cdot)$, the multiplicative group of $GF(p, P(x))$. Then there must exist an element x of G satisfying $|G| = o(x)$.

(15 points) Work over $\mathbb{Z}_5$. For each $a \in \mathbb{Z}_5$, state whether $x^2 - a$ is irreducible and if not factor $x^2 - a$ into irreducible factors.

(10 points) Consider the Galois field $F = GF(11, x-1)$.

a. How many elements does F have?

b. Find *one* primitive element of F.

c. In terms of powers of the element you found in part (b), find *all* primitive elements of F.

(10 points) Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$$

a. Write σ as a product of disjoint cycles.

b. Write σ as a product of 3-cycles.

c. What is $\sigma^{1234567}$?

(15 points) Consider the dihedral group D_3 (the symmetries of an equilateral triangle).

a. What is the order of D_3?

b. Let R denote clockwise rotation of 120 degrees and let F denote a flip about the vertical axis. Describe all the elements of D_3 and write them down in terms of R, F and the identity.

c. For each integer k between 1 and 6 (inclusive) list the elements of D_3 of order k, or else state that no such element exists.

order 1:
order 2:
order 3:
order 4:
order 5:
order 6:

(10 points) 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.

(10 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 exactly p^3 elements.