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.*

An irreducible polynomial is a polynomial f which cannot be factored as $f = gh$ where g and h are polynomials and $0 < \deg(g) < \deg(f)$.

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

Let v be the degree of $P(x)$ and α be a Galois imaginary of $P(x)$. Then $GF(p, P(x))$ is the Galois field consisting of all the elements of the form $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{v-1}\alpha^{v-1}$ with $a_i \in \mathbb{Z}_p$, whose addition and multiplication are defined as those for polynomials in one variable modulo the relation $P(\alpha) = 0$.

c) an *even permutation.*

An even permutation is a permutation which can be written as a product of even number of transpositions.

d) a *group.*

A group is a non-empty set G with a binary operation $\cdot$ on its elements satisfying:

(1) $a \cdot b \in G$ for any $a, b \in G$.

(2) There is $1_G \in G$ such that $a \cdot 1_G = 1_G \cdot a = a$ for $a \in G$.

(3) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for $a, b, c \in G$.

(4) For every $a \in G$, there is $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1_G$ (a^{-1} is written as $a^{\#}$ by the book) .

e) The *symmetric group* S_n.

The symmetric group S_n is a permutation group consisting of all the permutations on the set $\{1, 2, \cdots, n\}$, where the binary operation for the group is composition of permutations.

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

a) The dihedral group D_4 is not abelian.

True.

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

True. $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$, containing exactly n elements.

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

False. This set contains no identity element. Also, it is not closed under the 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 $p - 1$.)

False. Fermat's theorem says that $x^p \equiv_p x$ for all $x \in \mathbb{Z}_p$, so the only candidate is $x = 1$. But 1 has order 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 $|G| = o(x)$.

True since every Galois field contains a primitive element.

(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.

- $a = 0$: $x^2 - 0 = (x)(x)$.
- $a = 1$: $x^2 - 1 = (x + 1)(x + 4) = (x + 1)(x - 1)$.
- $a = 2$: $x^2 - 2$ is irreducible.
- $a = 3$: $x^2 - 3$ is irreducible.
- $a = 4$: $x^2 - 4 = (x - 2)(x - 3) = (x + 3)(x + 2)$.

a. Write σ as a product of disjoint cycles.

b. Write σ as a product of 3-cycles.

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

a. $\sigma = (1\ 3)(2\ 5)$
b. $\sigma = (1\ 3\ 5)(3\ 5\ 2)$
c. The order of σ is 2 and 1,234,567 is odd, so $\sigma^{1234567} = \sigma$.
(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:

a. 6
b. identity, R, R^2, F, RF, R^2F.
c. Order 1: identity. Order 2: F, RF, R^2F. Order 3: R, R^2. No others exist.
(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.

Proof. ($\Leftarrow$) is clear.
($\Rightarrow$) If $a = 0$ then we are done. If $a \neq 0$ then $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$.
(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.

Proof. Let $P(x) = x^3 - c$. Since c is not a cube in $\mathbb{Z}_p$, the cubic polynomial $P(x)$ is irreducible over $\mathbb{Z}_p$. The Galois field $\mathrm{GF}(p, P(x))$ contains exactly p^3 elements.