Math 312/ AMS 351 (Spring' 20)

Final Exam

May 14, 2020

Name:

ID:

- Time: 11:15–12:45
- If possible, print the exam. If not, solve each question (1-5) on a separate page.
- Scan the exam and e-mail it to me (radu.laza@stonybrook.edu) by **1pm EST (May 14, 2020)**

1. Consider the permutation

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

i) Decompose σ into disjoint cycles.

ii) What is the order of σ? (Add a brief explanation, e.g. *the order of a cycle is* $\ldots$*, and then for the product of* $\ldots$ *cycles, the order is* $\ldots$)

iii) What is the signature of σ? (Add a brief explanation.)

iv) Pick the correct answer: σ *can be written as product of*

$*$ 8 transpositions,

$*$ 9 transpositions.

Explain.

2. i) Give an example of
   - ∗ a cyclic group of order 8
   - ∗ a non-abelian group of order 8
   - ∗ an abelian, but not cyclic group of order 8

ii) Consider the following 3 abelian groups of order 90:
   - ∗ $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{15}$;
   - ∗ $\mathbb{Z}_2 \times \mathbb{Z}_{45}$;
   - ∗ $\mathbb{Z}_3 \times \mathbb{Z}_{30}$.

   Two of them are isomorphic. Which ones?

iii) State the result that you have used in the previous item (Chinese remainder Theorem):

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \ldots\ldots$$

iv) Use Lagrange theorem to deduce that any group of order 10 contains an element of order 5.

3. i) Use Euclid Algorithm to compute the gcd of the following polynomials in $\mathbb{Z}_3[x]$:

$$\begin{aligned} f(x) &= x^4 + x^3 + 2x + 2 \\ g(x) &= x^3 + x^2 + x \end{aligned}$$

ii) Decompose in irreducible factors f and g

iii) Use the result from ii) above to compute $\gcd(f, g)$ (and thus check your answer to the first item) and $\operatorname{lcm}(f, g)$.

4. Consider the polynomials

$$f = x^3 + x + 1 \in \mathbb{Z}_2[x]$$

i) Prove that f is an irreducible polynomial in $\mathbb{Z}_2[x]$.

ii) Write down the 8 elements of the field $\mathbb{Z}_2[x]/\langle f(x)\rangle$.

iii) In $\mathbb{Z}_2[x]/\langle f(x)\rangle$, compute

$$(x^2 + 1) + (x^2 + x + 1) = \dots$$

and

$$(x^2 + 1) \cdot (x^2 + x + 1) = \dots$$

iv) In $\mathbb{Z}_2[x]/\langle f(x)\rangle$, compute the inverse of x.

5. True/False

(1) Any group of order 3 is cyclic.

(2) Any group of order 4 is cyclic.

(3) The possible order of elements in a group of order 24 are: 1, 2, 3, 4, 5, 6, 8, 9, 12, 24.

(4) Let $(R, +, *)$ be a ring. Then $*$ is always commutative.

(5) Any field contains an identity element (call it 1) for multiplication.

(6) Any degree 1 polynomial over $\mathbb{Z}_3$ is irreducible.

(7) Any degree 2 polynomial over $\mathbb{Z}_3$ is irreducible.

(8) Any degree 2 polynomial over $\mathbb{R}$ is reducible.

(9) Let $f \in \mathbb{Z}[x]$ be a monic polynomial with integer coefficients, and $\bar{f} \in \mathbb{Z}_p[x]$ be its reduction mod p. *If $\bar{f}$ is reducible in $\mathbb{Z}_p[x]$, then f is reducible in $\mathbb{Z}[x]$.*

(10) Let $f \in \mathbb{Z}[x]$ be a monic polynomial with integer coefficients, and $\bar{f} \in \mathbb{Z}_p[x]$ be its reduction mod p. *If $\bar{f}$ is irreducible in $\mathbb{Z}_p[x]$, then f is irreducible in $\mathbb{Z}[x]$.*