Abstract Algebra in Theoretical Computer Science

Final Exam - Practice

Lecturer: Gil Cohen

Problem 1

Prove or disprove each of the following claims:

1. For every abelian group G and $N \triangleleft G$ it holds that $G \cong N \times (G/N)$.
2. If $G = H_1 \times H_2$ is a group with $|H_1| \geq 2$, $|H_2| \geq 2$ then G cannot by cylic.

Problem 2

Let R, S be commutative rings and $\phi\colon R \to S$ a ring homomorphism. Prove or disprove each of the following claims:

1. If P be a prime ideal in S then $\phi^{-1}(P)$ is a prime ideal in R.
2. If M be a maximal ideal in S then $\phi^{-1}(M)$ is a maximal ideal in R.

Problem 3

Prove or disprove: Let R be a ring and P, Q nonzero prime ideals in R. Then, $P \subseteq Q$ implies $P = Q$.

Problem 4

Let R be a commutative ring. An ideal $I \neq R$ in R is called *primary* if for every $x, y \in R$ the following holds: if $xy \in I$ then $x \in I$ or $y \in \sqrt{I}$.

1. Prove that every prime ideal is primary.
2. Prove that the radical of a primary ideal is prime.
3. Find all primary ideals in $\mathbb{Z}$.

An element $r \in R$ is called nilpotent if there exists an integer $n \geq 1$ such that $r^n = 0$.

4. Prove that an ideal I in R is primary if and only if every zero divisor in R/I is nilpotent.

Problem 5

Let K/F be a field extension. Let $a \in K$ be an algebraic element over F with odd degree. Prove or disprove: $F(a) = F(a^2)$.

Problem 6

Let p be a prime power and $q = p^2$. Define

$$H = \{(x, y, z) \in \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \mid y^p + y = x^{p+1} \text{ and } z^p + z = y^{p+1}\}.$$

What is $|H|$? Prove your answer.

Problem 7

Let $\mathbb{F}_{125}$ be the field of 125 elements. Consider the function $f\colon \mathbb{F}_{125} \to \mathbb{F}_{125}$ that is given by $f(x) = x^{31}$. What is the image of f? Prove your answer.

Problem 8

Let p be a prime number. Prove that there are exactly $(2^p - 2)/p$ degree p irreducible polynomials over $\mathbb{F}_2$.

Problem 9

Let p be an odd prime and $\mathbb{F}_p$ be the field of size p. A nonzero element $a \in \mathbb{F}_p$ is a *quadaric residue (modulo p)* if there exists $b \in \mathbb{F}_p$ such that $a = b^2$. We define the function $\chi_p\colon \mathbb{F}_p^* \to \{\pm 1\}$ by $\chi_p(a) = 1$ if a is a quadratic residue and -1 otherwise. Note that $\chi_p(ab) = \chi_p(a)\chi_p(b)$.

You can easily conveience yourself that exactly half the elements of $\mathbb{F}_p^*$ are quadartic residues, that is, $\mathbf{E}_{x \sim \mathbb{F}_p^*}[\chi_p(x)] = 0$. This readily implies that for any $a, b \in \mathbb{F}_p$, $a \neq 0$, $\mathbf{E}_{x \sim \mathbb{F}_p^*}[\chi_p(ax + b)] = 0$. That is, exactly half of the points on every line in $\mathbb{F}_p \times \mathbb{F}_p$ are quadratic residues.

A famous result of Weil gives a bound on the discrepancy of quadratic residues and quadratic nonresidues on the image of degree $d > 1$ polynomials. The result states that if $f(x) \in \mathbb{F}_p[x]$ is a degree d polynomial that is not a square of another polynomial then

$$\left| \sum_{x \in \mathbb{F}_p^*} \chi_p(f(x)) \right| \leq (d-1)\sqrt{p}.$$

You are going to construct a small-bias set based on this result. Given n, ε, wisely choose a prime number $p = p(n, \varepsilon)$. Define the set $S = \{s_1, \ldots, s_m\} \subseteq \{0,1\}^n$ such that the jth entry of s_i is given by

$$(s_i)_j = \frac{1 - \chi_p(i + j)}{2}.$$

Prove that for an appropriate choice of a prime number p, S is an ε-biased set of size $O(n^2/\varepsilon^2)$.