# 15-251: Great Theoretical Ideas In Computer Science

## Recitation 12

## Definitions

- **Group.** Abuse of notation: Instead of saying $(G, \circ)$ is a group, we often say $G$ is a group under $\circ$, or just $G$ is a group (especially if the operation is unimportant or obvious from context)
- **Subgroup.** Let $G$ be a group. $H$ is a subgroup of $G$ ($H \leq G$) if $H \subseteq G$ and $H$ is a group. $H$ is a proper subgroup of $G$ if $H \subsetneq G$.
- **Field.** A field is a set $F$ equipped with two operations $+, \times$ such that $S$ forms an abelian (commutative) group under $+$, and $F \setminus \{0\}$ forms an abelian group under $\times$ where '0' is the identity of $+$ (a.k.a the additive identity). Also, multiplication should distribute over addition : $\forall x, y, z \in F$, $x \times (y + z) = x \times y + x \times z$
- **Reed-Solomon Encoding.** If Alice has a message of $d+1$ elements of field $F$, she can think of it as the coefficients of a degree-$d$ polynomial $P(X)$, and encode $P(X)$ using its values representation. To guard against at most $k$ erasures, she can send $d + k + 1$ symbols; if there are up to $k$ corruptions, she can send $d + 2k + 1$ symbols.

## GCD

Suppose $a$ and $b$ are integers, with $a = bq + r$, where $0 \leq r < b$. Prove that $\text{GCD}(a, b) = \text{GCD}(b, r)$.

## Prime Time

Let $G$ be a group of prime order $p$. Prove that $G$ has no non-trivial subgroups.

## Fields are Meta

Let $F$ be $\mathbb{Z}_7$ - this is the unique field of size 7, up to isomorphism. Let $S$ be the set of polynomials over $F$ with degree at most 2.

(a) What is the size of $S$?

(b) Verify that $S$ is a field under addition and multiplication modulo $x^3 - 2$.

## BONUS: Subgroup discussion

(a) Let $G$ be a group, and let $H_1, H_2$ be nontrivial subgroups of $G$. Prove that $H_1 \cup H_2 \neq G$

(b) Does there exist a group $G$ with proper subgroups $H_1, H_2, H_3$ such that $G = H_1 \cup H_2 \cup H_3$?