SYLOW THEOREM

Cosets

Author
Tom Jeong

October 21, 2024

Contents

1 Sylow **3**

1.1 Exmaples of Sylow Theorems 4

1 Sylow

Proof of the first sylow theorem:

Proof. Let $S = \{X \subseteq G||X| = p^r\}$ Define $\alpha : G \times S \to S$ group action.

$$\alpha(g, X) = \{gx|x \in X\}$$

Since multiplication by g is a bijection, $\alpha(g, X) \in S$ $\square$

Exercise: Check that α is a group action. Observe that the number of subsets, X of G with $|X| = p^r$ is

$$|S| = \binom{p^r m}{p^r}$$

Exercise: The highest power of p dividing $p^r - i$ is the highest power of p dividing $p^r m - i$ for $i = 0, 1, \cdot p^r - 1$
show that p doens't deivide the size of s

By proposition (2,19.5 - 2) The set of G orbits partitions S so $\exists$ orbit $G \cdot X, X \in S$ such that $p \nmid |G \cdot X|$ because if $p \mid |G \cdot X| \forall X \in S$ then $p \mid |S|$
By Lagrnage's theorem and Proposition 2.10.2 (3)

$$|G| = |G \cdot X||G_X|$$

where G_X (is the stabilizer) $= \{g \in G|gX = X\}$
So $p^r \mid |G_X|$ since $p \nmid |G \cdot X|$
Claim: $|G_X| = p^r$ and profe of claim $G_X \circlearrowright X$ and orbit are right cosets. $G_X \cdot g$ (each coset has $|G_X|$ elements)

$|G_X| = |G_X|$

since orbits partition X

$|G_X| \mid |X|$

so $|G_X| \mid p^r$

hence $|G_X| = p^r$, so G_X is the desired Sylow p-subgroup of G.

See textbook for proofs of 2nd and 3rd Sylow Theorems.

1.1 Exmaples of Sylow Theorems

Example: prove that any group G of order 35 is isomprhic to $\mathbb{Z}/35\mathbb{Z}$ PF: since 35 = 5 x 7 the third sylo theorem implies:

$$
\begin{aligned}
&|Syl_7(G)| = \{1, 5\} \\
&|Syl_5(G)| = \{1, 7\} \\
&|Syl_7(G)| \equiv 1 \text{ mod } 7 \\
&|Syl_5(G)| \equiv 1 \text{ mod } 5 \\
&\text{ so } \exists! \text{ Sylow 7-Subgroup P of G} \\
&\exists! \text{ Sylow 5-Subgroup Q of G}
\end{aligned}
$$

Hence by Corollary to 2nd Sylow Theorem. P and Q are normal in G.
BY Lemma 2.3.6, PQ is a subgroup of G contaninig P and Q as subgroups, Ten $|PQ| = 35$
$|P| = 7$ divides $|PQ|$
$|Q| = 5$ divides $|PQ|$
Hence $PQ = G$ and Since $P \cap Q$ is a propeor subgroup of Q, we have that $P \cap Q = \{e\}$ by Lagrange. Tehn by lemma 2.8.11

$$
\begin{aligned}
&\Pi : P \times Q \to PQ = G \\
&\pi(p, q) = pq
\end{aligned}
$$

is an isomorphism. SO $G \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and by proposition 2.8.2,
beginalign* $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/35\mathbb{Z}$

Rings

Q: What would happen if a set had two different operations on it? EX: we know $(\mathbb{Z}, +)$ are a group mltiplication is a binary operation on Z. $a \cdot (b + c) = a \cdot b + a \cdot c$ ObserveL $(\mathbb{Z}, \cdot)$ is not a group no inverse

Definition 1.1. Deifine a ring is an abelian group $(R, +)$ with an additional binary operation.

$$\cdot : R \times R \to R$$

called multiplication. Multiplication satisfies the follwoing $\forall x, y, z \in \mathbb{R}$:

1. multilpication is associative
2. there exists a multiplcative identity
3. Multi. distributes over addition $x(y + z) = xzxy$

(some books dont require an identity and its call this a ring with unity)

Notes for $x \in R$ there is always an additive inverse -x.
There might not be a multiplicative invers. nOtation.

1. we will generally write xy for x $\cdot$ y.
2. we will write 0 for the additive identity

exercise: provet htat $0 \cdot x = x \cdot 0 = 0 \forall x \in \mathbb{R}$ ex.r
Ringss $(\mathbb{Z}, +, \cdot), (\mathbb{Z}/n\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$

Definition 1.2. Let R be a ring.

1. A subset $S \subset R$ is called a subring of R S is a subgroup of $(R, +)$ and
   (a) $1 \in S$
   (b) if $x, y \in S$ then $x \cdot y \in S$
2. An element $x \in R \backslash \{0\}$ is called a zero divisor if $\exists y \in \mathbb{R} \backslash \{0\}$
3. An element $x \in R$ is called a unit if $\exists y \in R$ such that $xy = 1 = yx$ we denote y by x^{-1} and y is called the multiplicative inverse of x. The set of units in R is denoted R^*
4. We say R commutative ring if $xy = yx \forall x, y \in R$

From now on we will restrit oursekves to commutative rings for the rest of the semester.