Mathematical Proofs

Your Name

4 January 2022

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut ullamcorper nec magna nec aliquam. Nunc sagittis, dui nec tristique faucibus, ipsum mi tristique sapien, eu convallis ex quam accumsan urna. Curabitur commodo et elit vitae pellentesque. Maecenas id ultrices neque. Phasellus consectetur ut metus non malesuada. Duis sagittis ultricies mauris ac lobortis. Maecenas ligula magna, pellentesque eu viverra ut, venenatis et elit.

1 The Theorems

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut ullamcorper nec magna nec aliquam.

Theorem 1.1 (Lagrange's Theorem)**.** *If G is a finite group and $H \subseteq G$ is a subgroup, then*

$$|G| = [G : H] \cdot |H|.$$

In particular, $|H|$ is a divisor of $|G|$.

Theorem 1.2. *Let N, H be normal subgroups of a group G, such that $N \cap H = \{e\}$. Then*

$$NH \cong N \times H.$$

2 Results

Curabitur commodo et elit vitae pellentesque. Maecenas id ultrices neque. Phasellus consectetur ut metus non malesuada. Duis sagittis ultricies mauris ac lobortis. Maecenas ligula magna, pellentesque eu viverra ut, venenatis et elit.

Definition 2.1. For a group $(G, +)$, $H \subseteq G$ is called a subgroup of G if $(H, +)$ is a group.

Lemma 2.2. *Let G be an abelian group, and let H, K be subgroups such that $|H|, |K|$ be relatively prime. Then*

$$H + K \cong H \oplus K.$$

Proof. By Theorem 1.1,

$$H \cap K = \{0\}.$$

Since subgroups of abelian groups are *normal*, so H, K are normal subgroups of G. By Theorem 1.2, it follows that

$$H + K \cong H \oplus K.$$

□

Theorem 2.3. *Let n be a positive integer and $G \subseteq \mathbb{Z}/n\mathbb{Z}$ be a subgroup. Then G is the cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by $[d]_n$, for some divisor d of n.*

Lemma 2.4. *Let p be a prime integer and $r \geq 1$. Let G be a noncyclic abelian group of order p^{r+1}, and let $g \in G$ be an element of order p^r. Then there exists an element $h \in G, h \notin \langle g \rangle$, such that $|h| = p$.*

Proof. Denote $K := \langle g \rangle$. Let $h' \in G$, $h' \notin K$. Since G is abelian, K is normal in G and $|G/K| = p$. Therefore

$$h' \notin K \implies |h' + K| = p \implies ph' \in K.$$

Let $k = ph'$. Note that $|k|$ divides p^r. But $|k| \neq p^r$, otherwise $|h'| = p^{r+1}$ and G would be cyclic. Suppose $|k| = p^s$ for some $s < r$. By Theorem 2.3,

$$\langle k \rangle = \langle p^{r-s} g \rangle.$$

Since $s < r$, $\langle k \rangle \subseteq \langle pg \rangle$. Hence $k = mpg$ for some $m \in \mathbb{Z}$. Let $h = h' - mpg$. We then obtain $h \neq 0$ since $h' \notin K$, and

$$ph = p(h' - mg) = ph' - pmg = k - k = 0.$$

Hence $|h| = p$. □

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut ullamcorper nec magna nec aliquam. Nunc sagittis, dui nec tristique faucibus, ipsum mi tristique sapien, eu convallis ex quam accumsan urna. Curabitur commodo et elit vitae pellentesque. Maecenas id ultrices neque. Phasellus consectetur ut metus non malesuada. Duis sagittis ultricies mauris ac lobortis. Maecenas ligula magna, pellentesque eu viverra ut, venenatis et elit.