MAS 4301, Abstract Algebra I.

Notes of Krishna Alladi's Lecture on Wed, Mar 25, 2020

Chapter 7: Cosets and Lagrange's Theorem cont'd.

Having established properties of cosets in the Lemma, we are ready to prove

Theorem 7.1 (Lagrange).

Let G be a finite group and H a subgroup of G. Then the order of H divides the order of G, ie $|H| \mid |G|$.

Proof: Consider the sequence of all left cosets of H, namely $\{aH\}_{a\in G}$, as 'a' ranges over all elements of G in some order. Since each $a \in aH$, we clearly have

$$G = \bigcup_{a\in G} aH, \qquad (1)$$

because $G \subseteq \bigcup_{a\in G} aH$ since every $a\in G$, satisfies $a \in aH$, and $\bigcup_{a\in G} aH \subseteq G$, since $aH \subseteq G$, for each $a \in G$. An important property of cosets is that given $a, b \in G$, then

$$\text{either } aH \cap bH = \phi \quad \text{or} \quad aH = bH \qquad (2)$$

Now not all members of the sequence $\{aH\}_{a\in G}$ of left cosets are distinct as cosets. But then from (2) and (1) we see that we can extract a subsequence $\{a_i H\}_{i=1}^m$ such that

$$\left.\begin{aligned} &a_i H \cap a_j H = \phi \text{ if } i \neq j \\ \text{and } &\bigcup_{i=1}^m a_i H = G. \end{aligned}\right\} \qquad (3).$$

Thus by extracting this subsequence of pairwise non-intersecting cosets we have avoided repetition. Since the sequence of cosets $\{a_i H\}_{i=1}^m$ form a partition of G as per (3), we have

$$|G| = \sum_{i=1}^m |a_i H| \qquad (4).$$

But then we also know that any two left cosets are of the same size.

That is

$$|a_i H| = |a_j H| \quad , \quad \forall i, j \tag{5}$$

Let this common size be denoted by t. Then from (4) and (5) we deduce that

$$|G| = mt \, , \tag{6}$$

with $|H| = t$, because $H = eH$, the ~~left~~ coset generated by e. Thus ~~tt~~ by (6) we have $|H| \mid |G|$ and this proves Lagrange's theorem.

Remark: Instead of left cosets, we could have used right cosets to prove Lagrange's theorem.

Notation: Let us denote the set of distinct left cosets of H in G by $[G:H]_\ell$, and the number of distinct left cosets by $|G:H|$.

The theorem of Lagrange has a number of important consequences of which the first is

Corollary 1: Let G be a finite group and H a subgroup of G. Then

$$|G:H| = \frac{|G|}{|H|} .$$

Proof: This follows from (6) above with $|H| = t$ and $|G:H| = m$.

Further consequences of Lagrange's Theorem are:

Corollary 2: Let G be a finite group and $a \in G$. Then $|a| \mid |G|$, that is the order of an element of G divides the order of G.

Proof: Consider the cyclic group $H = \langle a \rangle$ generated by 'a'. Then by Lagrange's theorem, we know $|H| \mid |G|$. Thus $|a| = |\langle a \rangle| \mid |G|$ as claimed

Corollary 3: Every group G of prime order is cyclic.

Proof: Let G be a group and $|G| = p$ = prime. Since $p \geq 2$, pick an element $a \in G$, $a \neq e$ (identity). Consider the cyclic group $H = \langle a \rangle$. Clearly $|a| = |\langle a \rangle| > 1$. But by Cor. 1, $|a| \mid |G| = p$ = prime Hence $|a| = p$ which means $G = \langle a \rangle$. Hence G is cyclic.

Remarks (i) Since every cyclic group is Abelian, Cor 3 implies that every group of prime order is Abelian.

(ii) If G is a ~~cyclic~~ group of prime order p, we know by Cor 3 that G is cyclic. But the proof of Cor 3 shows that every non-identity element of G is a generator. The number of non-identity elements is $p-1$. We also know that if G is cyclic of order n, then G has $\varphi(n)$ generators. In the case $n=p=$ prime, we have $\varphi(p)=p-1$. (Here $\varphi(n)$ is Euler's function.).

Corollary 4: Let G be a finite group and $a \in G$. Then $a^{|G|}=e$.

Proof: Let $|a|=t$. We know by Cor 2, that $t \mid |G|$. Thus $|G|=mt$, for some $m \in \mathbb{Z}^+$. Therefore

$$a^{|G|}=a^{mt}=(a^t)^m=e^m=e.$$

This proves Corollary 4.

Corollary 5: (Fermat's Little Theorem)

For every integer 'a' and any prime p, we have

$$a^p \equiv a \pmod{p}.$$

Proof: Since we are establishing a congruence, we can replace the integer 'a' by the congruence class $[a]_p$ and by abuse of notation denote this by 'a'. Thus $a \equiv 0, 1, 2, \ldots, p-1 \pmod{p}$.

Consider the multiplicative group

$$G=\mathbb{Z}_p^{\times}=U_p=\{1,2,3,\ldots,p-1\}, \quad \text{with } |U_p|=|G|=p-1.$$

of $p-1$ elements. Then by Cor 4, we have

$$a^{p-1} \equiv 1 \pmod{p}, \quad \forall\, a \in G=U_p \qquad (7).$$

Multiply both sides of the congruence in (7) by 'a' to deduce

$$a^p \equiv a \pmod{p}, \quad \forall\, a \in U_p=\{0,1,2,\ldots,p-1\}. \qquad (8).$$

This proves Corollary 5 for all $a \not\equiv 0 \pmod{p}$. But then (8) holds trivially for $a \equiv 0 \pmod{p}$. Hence Cor 5 is proved.

Remark: Traditionally, (7) is referred to as Fermat's Little Theorem

Problems from Chapter 7

#17) Let G be a group and let $|G| = pq$, where p and q are prime. Then prove that every proper subgroup of G is cyclic.

Proof: Let $H < G$. Then $|H| < |G| = pq$, and by Lagrange's theorem, we have $|H| \mid pq$. This means that

$$|H| = 1, \ p \text{ or } q.$$

If $|H| = 1$, then $H = \{e\} = \langle e \rangle$ is cyclic. If $|H| = p$ or q, then by Cor 3, H is cyclic. This proves the assertion in # 17.

Remark: Note that the assertion and proof hold if $p = q$! So p & q need not be distinct primes.

#11) Let G be a group and H and K subgroup of G. Let $g \in G$. Then prove that the cosets $g(H \cap K)$, gH, and gK satisfy

$$g(H \cap K) = gH \cap gK. \qquad (9)$$

Proof: We know that $H \cap K$ is a subgroup of G.
Consider an element of $g(H \cap K)$. This element is of the form gh with $h \in H \cap K \Rightarrow h \in H$ & $h \in K$.
Thus

$$gh \in gH \ \& \ gh \in gK \Rightarrow gh \in gH \cap gK.$$

Hence

$$g(H \cap K) \subseteq gH \cap gK. \qquad (10)$$

Next consider an element of $gH \cap gK$. Any element of gH is of the form gh with $h \in H$. Similarly an element of gK is of the form gk, with $k \in K$. Thus the common element c of the two ~~sets~~ cosets must ~~be~~ satisfy

$$c = gh = gk, \quad \text{with } h \in H \ \& \ k \in K \qquad (11)$$

By cancelling g in (11), we conclude that $h = k$, which means $h = k \in H \cap K$. Thus $c \in g(H \cap K)$. This yields

$$gH \cap gK \subseteq g(H \cap K) \qquad (12)$$

and so ~~the~~ (9) follows from (10) and (12).