MAS 4301, Abstract Algebra I

Notes of Krishna Alladi's Lecture, Fri, Mar 27, 2020

Chapter 7: Cosets & Lagrange's theorem cont'd.

Problems from Chapter 7:

#25, p. 151: Let G be an Abelian group of odd order. Prove that the product of all elements of G is the identity e.

Proof: First note that since G is Abelian, it does not matter in which order the factors (terms) in the product occur. So consider

$$\prod_{a\in G} a \qquad (1)$$

in some order.

Since G has odd order, by Lagrange's theorem we deduce that no element of G can have order 2. This means that

$$\text{if } a\in G,\ a\neq e, \text{ then } a^2\neq e \Leftrightarrow a\neq a^{-1} \qquad (2)$$

Since $|G|$ is odd, there are an even number of non-identity elements in G. These non-identity elements can be paired as (a, a^{-1}) because of (2). Thus by rewriting the product in (1) as

$$\prod_{a\in G} a = \prod_{a\in G,\, a\neq e} a, \qquad (3)$$

we can pair the terms of the product (on the right) in (3) as $a\cdot a^{-1}$ and each $a\cdot a^{-1} = e$. Thus the product in (1) will have value e.

#26, p. 151: We will split this problem into two parts as follows: Let G be a group with more than one element, and having no non-trivial proper subgroups. Then show that

(i) G is cyclic of finite order

(ii) $|G| = p$ prime.

Proof: A proper subgroup $H < G$ satisfies $|H| < |G|$. The subgroup $\{e\}$ is the trivial proper subgroup. Otherwise H is non-trivial.

Since $|G| > 2$, it has non-identity elements. So pick $a \in G$, $a \neq e$. (2)

Consider the cyclic subgroup H generated by 'a'. ie $H = \langle a \rangle$.
Clearly $|H| \geq 2$, so H is not the trivial subgroup. Since G has no non-trivial proper subgroups, we must have $H = \langle a \rangle = G$, Thus G is cyclic.

If $G = \langle a \rangle$ and $|G| = \infty$, then $H = \langle a^2 \rangle$ is a proper subgroup of G, and H is not trivial. But we are given that G has no non-trivial proper subgroups. Hence $|G| = \infty$ is not possible. Thus $|G| < \infty$, which proves (i)

Next let $|G| = n$, G cyclic, and n composite. This means there exist $d \mid n$, $1 < d < n$. Since G is cyclic, there is a cyclic subgroup of order d. This subgroup will be a non-trivial proper subgroup - contradicting the hypothesis. Thus n composite is not possible. Hence $|G| = p$ prime and this proves (ii).

---

problem 27, p.152: Let G be a group and $|G| = 15$. Suppose G has only one subgroup ~~H~~ of order 3 and only one subgroup of order 5. Prove that G is cyclic.

Proof: Since H and K are of prime order, both are cyclic. Let $H = \langle a \rangle$, and $K = \langle b \rangle$. Consider now the element $ab \in G$. Clearly $ab \neq e$, because $ab = e$ would imply that $b = a^{-1}$ and so we would have $|a| = |b| = |a^{-1}| = 3$, but $|b| = 5$. Thus $ab \neq e$.

Next note that $ab \notin H$, for $ab \in H$ and $a \in H$ would imply $b \in H$. This is a contradiction because $|b| = 5$ & $|H| = 3$. Thus $ab \notin H$. Similarly $ab \notin K$, because $ab \in K$ together with $b \in K$ would imply $a \in K$. This is a contradiction to a corollary of Lagrange's theorem since $|a| = 3$, $|K| = 5$ & $3 \nmid 5$. Thus $ab \notin K$.

Again by Lagrange's theorem $|ab| = 1, 3, 5,$ or 7. Let $L = \langle ab \rangle$, the cyclic subgroup generated by ab. Then we see that since H is the only subgroup of order 3, and K is the only subgroup of order 5, and $L \neq H$ (because $ab \in L$ & $ab \notin H$), and $L \neq K$ (because $ab \in L$ and $ab \notin K$), and $ab \neq e$, we see that

$$|L| \neq 1, 3, \text{ or } 5.$$

Thus $|L| = 15$ & $L = \langle ab \rangle$. Since $|G| = 15$, we deduce that $G = \langle ab \rangle$. Hence G is cyclic.

Remarks: The above argument only uses the property that 3 and 5 are distinct primes. So the assertion would hold if $|G| = pq$ with any pair of distinct primes p and q.

---

problem 44, p. 152 : Prove that every subgroup of D_{2n} of odd order is cyclic

Proof: We know that $|D_{2n}| = 2n$, and that R_n ~~the~~ is a subgroup of order n where R_n is the set of rotations. Thus $D_{2n} - R_n$ is the set of reflections and $|D_{2n} - R_n| = n$. We know that R_n is a cyclic group of order n.

Now let $H < D_{2n}$ with $|H| =$ odd. Since every reflection has order 2, we see by Lagrange's theorem that H cannot have any reflections. Thus $H \leq R_n$ and R_n is cyclic. Since every subgroup of a cyclic group is cyclic, we conclude that H is cyclic.

---

problem 29, p 152 : Let G be a group of order 33. Prove that G has an element of order 3.

Proof: If G is cyclic of order 33, it must have an element of order 3 since there are elements of order d for each $d \mid |G|$. So we need only prove the claim now in the case G being not cyclic.

By Lagrange's theorem, the possible orders of elements of G are 1, 3, 11 and 33. Since G is not cyclic, order 33 is not possible. Only the identity has order 1. Thus there are 32 non-identity elements of G whose orders will be either 3 or 11.

Suppose G has no element of order 3. Then all 32 non-iden elements will have order 11. But then $\varphi(11) = 10$, and we know that the number of elements of order 11 is a multiple of $\varphi(11) = 10$. Note that $32 \not\equiv 0 \pmod{10}$. Thus the assumption the G has no elements of order 3 leads to a contradiction. So G must have an element of order 3, as claimed.

Remark: If $a \in G$ and $|a| = 3$, then $|a^2| = 3$ as well & $a \neq a^2$.

problem 46, p. 153: Prove that every group of order 12 has an element of order 2.

Proof: Let G be group and $|G| = 12$. Then by Lagrange's theorem, the possible orders of the elements of G are

$$1, 2, 3, 4, 6 \text{ and } 12,$$

—namely, the divisors of 12. There are 11 non-identity elements of order > 1.

If $a \in G$, and $|a| = n$ with $n = 2, 4, 6$ or 12 (all even), then $|\langle a \rangle| = 2, 4, 6, 12$. Now 2 divides each of the numbers 2, 4, 6, 12 and so this cyclic subgroup will have an element of order 2.

So we need only show now that not all non-identity elements of G can have order 3. Note that $\varphi(3) = 2$, and the number of elements of order 3 must be a multiple of $\varphi(3) = 2$, But if all non-identity elements have order 3, we would have $2 \mid 11$ — which is a contradiction. Hence the proof.