Algebra I
Stories From Group Theory
December 5, 2011

Instructions. The questions are interspersed with remarks so as to give a complete picture. Do NOT attempt to prove any of the remarks. NO credit will be given for work done about remarks. The marks for each question are given at its end.

1. Lagrange's Theorem.

Even though Lagrange's theorem states that the order of a subgroup divides the order of a finite group G, it follows from

(a) Let H be a subgroup of a finite group G and let xH and yH be two left cosets (or left translates) of H. Prove that they are either equal or disoint subsets of G. (4)

(b) Prove Lagrange's theorem using the first part. (2)

Therefore, strictly speaking, Lagrange's theorem is about any subset H of G with the property that any two of its left translates are either disjoint or same. Obviously, since translate of a coset is also a coset, not just a subgroup but any of its left cosets will also have this property. The following says that this is the only possibility!

(c) Let $\widetilde{H}$ be a subset of a group G such that any two of its left translates are either disjoint or same. Prove that there exists a subgroup H and an element g of G such that $\widetilde{H} = gH$. (4)

2. An Application to Number Theory.

We now give an application of cyclic groups to prove a formula about the Euler's ϕ function in elementary Number Theory. Recall that $\phi(n)$ equals the number of natural numbers not more than n that are co-prime to n.

(a) Let C be a cyclic group of order n. Prove that the number of its *generators* equals $\phi(n)$. (3)

(b) With C as above, prove that for each divisor d of n, it contains a unique subgroup of order d. (3)

(c) Prove the following property of the Euler's ϕ function:

$$\sum_{d|n} \phi(d) = n \tag{4}$$

Since the product of two cyclic groups with co-prime orders is again a cyclic group, we can also prove the *multiplicativity* of the ϕ function using Group theory. On the other hand, we can use the formula proved above to prove that any finite group having at-most one subgroup for each of the divisor of its order has to be a cyclic group. Thus, Number theory contributes to Group theory as well!

3. Index of a subgroup and normality.

(a) Let G be a finite group and H be a subgroup of index 2. Prove (without using the next part!) that H is normal in G. (2)

The following is a beautiful generalisation of the simple fact above.

(b) Let p denote the smallest prime dividing the order of G. Then, prove that any subgroup of G with index p is normal. (Hint: look at the G action on G/H) (4)

The following two parts show that this is the best possible generalisation of the first part by considering subgroups whose index is a larger prime divisor or the lowest number.

(c) Give an example of a group of order 6 and its non-normal subgroup of index 3. (2)

(d) Give an example of group such that none of its proper subgroups of smallest index is normal. (Of course, by (a), this means that it has no subgroup with index equal to smallest prime dividing its order.) (Hint: A_5 is simple!) (2)

4. A concrete example.

Let $\mathbf{Q}$ and $\mathbf{Z}$ denote the additive groups of rational numbers and integers respectively. Let G be the quotient group $\mathbf{Q}/\mathbf{Z}$. For those who like complex numbers, this group is isomorphic to the multiplicative group of all roots of unity in the complex plane $\mathbf{C}$ via the exponential map. We now prove some properties of this group.

(a) Let g be any element of G. for any natural number n, prove that n-th root of g exists in G. That is, prove that there exists $h \in G$ such that $nh = g$. (2)

(b) Prove that for any natural number d, there exists a unique subgroup of G of order d. (3)

(c) Prove that G is not cyclic. (2)

This shows that the remark after the second question about cyclicity of groups with property (b), can not be generalised to infinite groups. Of course, this group has more than one proper infinite subgroups. But if we fix a prime p and look at elements in G whose denominator is a power of p, then it does not have any proper infinite subgroup and still will not be cyclic. (This subgroup of G will be isomorphic to the one we have seen in the mid-term!) Finally, we see that:

(d) For any proper subgroup H of G, prove that there exists a proper subgroup K of G that contains H properly. (There are no *maximal* proper subgroups of G) (3)

5. Sylow's Theorems.

(a) State the three Sylow theorems. (3)

(b) Prove that an abelian group is simple if and only if its order is 1 or a prime number. (2)

The Sylow theorems are used to deny the existence of simple groups for many orders. Since classification of simple groups is a major question in finite group theory, Sylow's theorems become important in the theory of finite groups. The following example illustrates this point.

(c) Let p and q be two prime numbers. Prove that no group of order p^2q is simple. (Hint: consider three cases: $p = q$, $p < q$ and $p > q$) (5)

By no means, these are the only stories in group theory. In fact, these do not form even the tip of the iceberg that group theory is! However, it would be very nice if you can spend some time thinking about remarks in this paper and make some of your own in your holidays. Have a nice time and HAPPY NEW YEAR! in advance.