10/3/16 Fall 2016, Intro to Modern Algebra I Test I Solutions Sitaraman

EACH PROBLEM 20 POINTS

1. State clearly Lagrange's Theorem and use it to prove that for any element in a group its order divides the order of the group.

Solution: This is theorem 2.4.4 in Herstein.

2. Prove by induction on n that $n^p - n$ is always divisible by p if p is a prime. Show that Fermat's little theorem follows from this.

You may need the Binomial Theorem to expand $(n+1)^p$:

$$(x+y)^m = x^m + \binom{m}{1}x^{m-1}y + \binom{m}{2}x^{m-2}y^2 + ... + \binom{m}{m-2}x^2y^{m-2} + \binom{m}{m-1}xy^{m-1} + y^m \text{ where } \binom{m}{k} = \frac{m!}{(m-k)!k!}.$$

Solution: For $n = 1$ it is clearly true.

Assuming for n we need to prove for $n+1$: That $(n+1)^p - (n+1)$ is divisible by p.

On expansion using binomial theorem we get

$$(n+1)^p - (n+1) = \left(n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + ... + \binom{p}{p-2}n^2 + \binom{p}{p-1}n + 1^p\right) - (n+1)$$

$$= (n^p - n) + \left(\binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + ... + \binom{p}{p-2}n^2 + \binom{p}{p-1}n\right).$$

Now using $\binom{n}{k} = \frac{n!}{(n-k)!k!}$ we have for any $k = 1, 2, ...p-1$, $\binom{p}{k} = \frac{p!}{(p-k)!k!} = \frac{p.p-1...p-k+1}{k.k-1....3.2.1}$. Clearly none of the numbers in the denominator divide p because they are all smaller than p. So that means all of the coefficients $\binom{p}{k}$ are divisible by p. Since by induction assumption $n^p - n$ is divisible by p we see that all of the RHS of the expression for $(n+1)^p - (n+1)$ is divisible by p. Therefore $(n+1)^p - (n+1)$ is divisible by p.

Fermat's last theorem follows from this because, if p does not divide then we can divide n out of $n^p - n$ (in other words n is invertible mod p and can be "canceled out") and the quotient $n^{p-1} - 1$ will also be divisible by p. So $n^{p-1} \equiv 1$ modulo p.

3. Give an example of a G and a subgroup H where $[G : H]$ is infinite. Describe the cosets. [Hint: Think of a group and an equivalence relation on it that results in an infinite number of equivalence classes. Alternately think of an infinite group with a finite subgroup].

Solution: The easiest example is the subgroup $\{1, -1\}$ in $\mathbb{R}^*$ under multiplication where $\mathbb{R}^* = \mathbb{R} - \{0\}$. Its cosets are the sets of the form $\{r, -r\}$ where r is any real number. So you get one coset for each positive real number. These are the same as the equivalence classes for the relation $a \sim b$ if $|a| = |b|$. In fact, if $H = \{1, -1\}$ then this equivalence relation is the same as the one defined by the cosets of the subgroup, namely $a \sim b \iff Ha = Hb \iff ab^{-1} \in H$.

The above equivalence relation can also be generalized to $\mathbb{C}^*$ and in that case $H = \{z \in \mathbb{C}^* \mid |z| = 1\}$. The equivalence classes (hence the cosets) will be all the circles with center at the origin.

Another example, also discussed in class, is the finite subgroup of $\mathbb{C}^*$ under multiplication given by $\{x \in \mathbb{C}^* \mid x^n = 1\}$ for any natural number n. These are just the n^{th}roots of unity. For example the fourth roots of unity are $1, -1, i, -i$. The cosets in this case are sets of the form $\{z, -z, iz, -iz\}$ where z is a non-zero complex number.

4. Describe all the subgroups of integers modulo 12 under addition (the remainders modulo 12). The subgroups are the following: Subgroup of order 6 generated by 2 namely ({2,4,6,8,10,0}) ; Subgroup of order 4 generated by 3 ; Subgroup of order 3 generated by 4 ; Subgroup of order 2 generated by 6 ; The trivial subgroups, namely { 0 } and the group itself.

5. Given a subgroup $H < G$ show that $aHa^{-1} = \{aha^{-1} | h \in H\}$ is also a subgroup for any fixed $a \in G$.

Solution: Need only to prove that if $x, y \in aHa^{-1}$ then $xy^{-1} \in aHa^{-1}$.
Let $x = ah_1a^{-1}, y = ah_2a^{-1}$, with $h_1, h_2 \in H$.
Then $xy^{-1} = ah_1a^{-1}\left(ah_2a^{-1}\right)^{-1} = ah_1a^{-1}(a^{-1})^{-1}h_2^{-1}a^{-1} = ah_1a^{-1}ah_2^{-1}a^{-1} = a(h_1h_2^{-1})a^{-1} \in aHa^{-1}$.