Dr. Marques Sophie
Office 519

Algebra 1

Spring Semester 2015

marques@cims.nyu.edu

Final

The grader cannot be expected to work his way through a sprawling mess of identities presented without a coherent narrative through line. If he can't make sense of it in finite time you could lose coherent narrative through line. If he can't make sense of it in finite time you could lose serious points. Coherent, readable exposition of your work is half the job in mathematics.

Problem 1 : (20 pt) Let G be a group and H a subgroup of index 2

1. **Explain what it means for a subgroup to be of index 2. Describe G/H and H/G (right and left quotient set.**
2. **Reprove then that H is a normal subgroup of G.**

Solution :

1. $|G/H| = 2$. $G/H = \{H, gH\}$ and $H \backslash G = \{H, gH\}$ where $g \notin H$.
2. Let $g \in G$. If $g \in H$ then $gH = H = Hg$. If $g \not inH$ then $gH = G \backslash - H = Hg$.

Problem 2 : (20 pt)

1. **Let $< a >$ be a cyclic group of order n. Describe all the subgroup of $< a >$ and the number of each kind. You can directly use a result seen in class without reproving it.**
2. **Let the dihedral group D_n be given by elements a of order n and b of order 2, where $ba = a^{-1}b$. Show that any subgroup of $< a >$ is normal in D_n.**

Solution :

1. For each $d|n$ there is a unique subgroup of $< a >$ of order d which is $< a^{n/d} >$.
2. As we have seen before we know that a subgroup of $< a >$ has the form $< a^k >$ where $k|n$. So we need to prove that for any $g \in D_n$ then $ga^{ik}g^{-1} \in < a^k >$. We know that any $g \in G$ is of the form $g = ba^l$ or $g = a^l$.
   If $g = a^l$ then $ga^{ik}g^{-1} = a^l a^{ik} a^{-l} = a^{ik} \in < a^k >$.
   Now, id $g = ba^l$, $ga^{ik}g^{-1} = ba^l a^{ik} a^{-l} b = ba^{ik} b$.
   Note that since $ba = a^{-1}b$ then $ba^2 = a^{-1}ba = a^{-2}b$ and thus we can prove that $ba^j = a^{-j}b$ for all j.
   So $ga^{ik}g^{-1} = ba^{ik}b = a^{-ik} \in < a^k >$.

Problem 3 : (20 pt) Let G be a simple group and suppose that $\phi : G \to H$ is a non-trivial group homomorphism.

1. **What does it means for G to be simple ?**
2. **Prove that ϕ trivial or injective.**

Solution : Suppose that $\phi : G \to H$ is a non-trivial group homomorphism. By contradiction suppose ϕ is not injective then $ker(\phi)$ is a proper normal subgroup of G indeed $ker(\phi) \neq \{e\}$ since ϕ is not injective and $ker(\phi) \neq G$ since ϕ is not the trivial homomorphism. But this is impossible since G is simple meaning it has no proper normal subgroup. Thus ϕ is injective.

Problem 4 : (30 pt)

1. **Reprove that S_4 has no normal subgroup of order 3.**
2. **How is defined A_4 in S_4 ? What is its cardinality ?**
3. **Prove that S_4 is a semi direct product of A_4 and H, where H is also a subgroup of S_4.**

Solution

1. Let H be a subgroup of order 3. Because 3 is a prime number, we know that H is cyclic thus generated by a 3-cycle, say (abc). Then $H = \{Id, (abc), (acb)\}$. But, for $d \neq a, b, c$,
$$(ad)(abc)(ad) = (bcd) \notin H$$
thus H is not normal in S_4.
2. A_4 is defined as the kernel of the signature morphism $sgn : S_n \to \{\pm 1\}$. It is a normal subgroup of S_4 of index 2 of the even permutations. Thus $|A_4| = |S_4|/2 = 12$
3. Let $< (1,2) >$ be the subgroup generated by the transposition $(1,2)$ in S_4 then $| < (1,2) > | = 2$ and $(1,2) \notin A_4$ indeed $sgn((1,2)) = -1$ thus $A_4 \cap < (1,2) >= \{Id\}$ and A_4 normal in S_4 of cardinality 12. Finally $G = A_4 < (1,2) >$ indeed $A_4 < (1,2) > \subseteq G$ and by a counting principle seen in class
$$|A_4 < (1,2) > | = |A_4|| < (1,2) > |/|A_4 \cap < (1,2) > | = 12 \times 2/1 = 24 = |G|$$
Thus since we have A_4 normal in S_4, $A_4 \cap < (1,2) >= \{Id\}$ and $G = A_4 < (1,2) >$, then G is a semi direct product of A_4 with $< (1,2) >$.

Problem 5 : (30 pt)

Let $Gl_n(\mathbb{R})$ denote the (multiplicative) group of invertible $n \times n$ matrixes with real entries. Let $SL_n(\mathbb{R})$ be the subset of matrices with determinant 1. Show that $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$ and identify the quotient group $Gl_n(\mathbb{R})$ with a group that we know.

Solution : Let $det : Gl_n(\mathbb{R}) \to \mathbb{R}^\times$ be the determinant map, we know that it is an homomorphism of groups and its kernel is $Sl_n(\mathbb{R})$ thus it is a normal subgroup of $Gl_n(\mathbb{R})$. This morphism is surjective since for any $\lambda \in \mathbb{R}^\times$ take the diagonal matrix D in $Gl_n(\mathbb{R})$ with entry 1×1 λ and 1 elsewhere in the diagonal then $det(D) = \lambda$. Thus, we can apply the first isomorphism theorem, we have that $Gl_n(\mathbb{R})/Sl_n(\mathbb{R}) \simeq \mathbb{R}^\times$.

Problem 6 : (40 pt)
Let Q denote the quaternion group of order 8. Let $N = Z(Q)$ be its center, a normal subgroups of Q.

1. **Describe Q.**
2. **Find N and its index $[Q : N]$.**
3. **Find coset representatives for the left coset space Q/N.**
4. **What is the order of the quotient group Q/N ? How many groups up to isomorphism there is of this order ? Identify Q/N with one of those group ?**

Solution :

1. $Q = \{\pm 1, \pm i, \pm j, \pm k\}$, with $(-1)^2 = 1$, $i^2 = j^2 = k^2 = ijk = -1$.
2. We also have $ij = k = -ji, jk = i = -kj,$ and $ki = j = -ik$ so clearly $N = \{\pm 1\}$ and thus by Lagrange, $|Q/N| = |Q|/|N| = 4$.
3. $Q/N = \{N, iN, jN, kN\}$ thus $1, i, j, k$ are coset representative for the left coset in G/H.
4. $|Q/N| = 4$. There are two subgroup up to isomorphism which are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
   We observe that $i^2N = -N = N$, $j^2N = -N = N$ and $k^2N = -N = N$. thus the order of each non-trivial element of Q/N is 2 that implies that $Q/N \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Problem 7 : (60 pt)
Let G be a group of order p and q, where p and q are primes with $p < q$.

1. **Describe the Sylow subgroups of G.**
2. **Explain why the number of q-Sylow subgroups is coprime with q. Deduce this number and conclude about the normality of the q-Sylow subgroups.**
3. **Do the same with the the number of p-Sylows. Deduce the p-Sylow is normal when p does not divide $(q-1)$.**
4. **Prove that G is a semi-direct subgroup of q-Sylow subgroup with a p-Sylow subgroup.**
5. **If p does not divide $q-1$, show that G is the cyclic group of order pq.**
6. **Note that $U_q = \mathbb{Z}/(q-1)\mathbb{Z}$. If p divides $q-1$, show that it is a group generated by two element x and y of order q and p respectively such that $y^{-1}xy = x^{repr_{\phi(y)}}$, where $\phi : \mathbb{Z}/p\mathbb{Z} \to U_q$ is the homomorphism defining the action of H_p on H_q and $repr\phi(y)$ is some representative of the class $\phi(y)$ in $\mathbb{Z}$.**

Solution :

1. By the Sylow theorem we have p-Sylows of order $p \simeq \mathbb{Z}/p\mathbb{Z}$ and q-Sylows of order $q \simeq \mathbb{Z}/q\mathbb{Z}$.
2. By the Sylow theorem, we know that the number of q Sylow is congruent to 1 mod q thus coprime with q and divides pq but since it is coprime with q thus divides p. But since $p < q$, then the number of q-Sylows is 1 and the q-Sylow subgroup will be normal.
3. Similarly, by the Sylow theorem, we know that the number of p-Sylow subgroups n_p is congruent to 1 mod p thus coprime with p and divides pq but since it is coprime with p thus divides q. So if $n_p \neq 1$ then $n_p = q$ and $q \equiv 1 \ mod \ p$ that is $p|(q-1)$. In particular, $n_p = 1$ as soon as p does not divide $q-1$ and thus then the p-Sylow subgroup is also normal.
4. Let H_p be a p-Sylow subgroup and H_q be the q-Sylow subgroup. Then $H_p \cap H_q = \{e\}$ (Langrage and $gcd(p,q) = 1$), $G = H_pH_q$ (do counting principle again) and H_q is normal in G. Thus G is a semi-direct product of H_q and H_p.
5. If p does not divide $q-1$, then both H_p and H_q are normal subgroups and thus G is a direct product of H_p and H_q that is

$$G = H_p \times H_q \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} = \mathbb{Z}/pq\mathbb{Z}$$

6. If p does divide $q-1$, then we cannot conclude that H_p is normal. Any semi-direct product is given by an homomorphism $\psi : H_p \to Aut(H_q)$ determined by conjugation of the element of H_q by the elements of H_p which can be identified with a homormorphism $\phi : \mathbb{Z}/p\mathbb{Z} \to U_q$. By the first isomorphism theorem, $|Im(\phi)||p$ thus equals 1 or p, if it is 1 the ϕ is trivial and the product is direct isomorphic to $\mathbb{Z}/pq\mathbb{Z}$.
   Suppose now it is p, $U_q = \mathbb{Z}/(q-1)\mathbb{Z}$ and we have a unique subgroup of order p P in U_q cyclic, thus $Im(\phi) \simeq P$. For each α a generator of P we can then define a homomorphism ϕ by sending the generator to α and all the homomorphism ϕ are defined this way and we obtain the anwer.