Homework

due on Friday, November 16

Read sections 2.4, 2.5, 2.6, 2.7, 2.8 in Lauritzen's book and sections 3.2.1, 3.2.2, 3.2.3, 3.3.1, 3.3.2, 3.3.3 in Cameron's book.

Solve problem 3.20 in Cameron's book and the following problems.

Problem 1. a) Let G be a group. For any element $g \in G$, let c_g be the conjugation by g map defined by $c_g(x) = gcg^{-1}$. Show that c_g is an automorphism of G. (It is called the **inner automorphism** induced by the element g.)

b) Show that the set $\{c_g : g \in G\}$ is a subgroup of Aut$G$. (This subgroup is called the **inner automorphism group** of G, denoted Inn$G$.)

c) Show that the map $g \mapsto c_g$ is a homomorphism from G to Aut$G$, whose image is the inner automorphism group Inn$G$ and whose kernel is the center $Z(G)$. Deduce that Inn$G \cong G/Z(G)$.

d) Show that Inn$G$ is a normal subgroup of Aut$G$. (By definition, the factor group Aut$G$/Inn$G$ is the **outer automorphism group** of G, denoted Out$G$.)

Solution: a) Since

$$c_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = c_g(x)c_g(y),$$

we see that c_g is a homomorphism. Note that $c_{g^{-1}}c_g$ and $c_gc_{g^{-1}}$ are both equal to the identity:

$$(c_gc_{g^{-1}})(x) = c_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x$$

and similarly for $c_{g^{-1}}c_g$. Thus c_g is a bijection, hence an automorphism of G.

b) This will follow from c) since the image of a homomorphism is a subgroup (you can verify it directly though).

c) Note that

$$c_{ab}(x) = (ab)x(ab)^{-1} = abxb^{-1}a^{-1} = a(bxb^{-1})a^{-1} = c_a(c_b(x)) = (c_ac_b)(x).$$

Thus $c_{ab} = c_ac_b$ so our map is a homomorphism. Its image is Inn$G$ by the very definition of Inn$G$. The kernel of this homomorphism is

$$\{a \in G : c_a \text{ is the identity}\} = \{a \in G : c_a(x) = x \text{ for all } x \in G\} =$$

$$= \{a \in G : axa^{-1} = x \text{ for all } x \in G\} = Z(G).$$

By the first isomorphism theorem, we have $\mathrm{Inn}G \cong G/Z(G)$.

d) Let $\phi \in \mathrm{Aut}G$ and $c_a \in \mathrm{Inn}G$. We need to prove that $\phi c_a \phi^{-1} \in \mathrm{Inn}G$. Note that

$$(\phi c_a \phi^{-1})(x) = \phi(a\phi^{-1}(x)a^{-1}) = \phi(a)\phi(\phi^{-1}(x))\phi(a^{-1}) = \phi(a)x\phi(a)^{-1} = c_{\phi(a)}(x)$$

so $\phi c_a \phi^{-1} = c_{\phi(a)} \in \mathrm{Inn}G$. This shows that $\mathrm{Inn}G \lhd \mathrm{Aut}G$.

Problem 2. Let G be a group and let H be a subgroup of G. Define the **normalizer** of H in G as $N_G(H) = \{a \in G : aH = Ha\}$.

a) Prove that $a \in N_G(H)$ iff $c_a(H) = H$, where c_a is the conjugation by a.

b) Prove that $N_G(H)$ is a subgroup of G and that $H \subseteq N_G(H)$ and the center $Z(G) \subseteq N_G(H)$.

c) Prove that H is a normal subgroup of $N_G(H)$. Conculde that $H \lhd G$ iff $N_G(H) = G$.

d) Let $G = D_8$, $H = \{I, S\}$. Find $N_G(H)$.

Solutiuon: Suppose that $a \in N_G(H)$. Then $aH = Ha$. If $h \in H$ then $ah = h_1 a$ for some $h_1 \in H$. We see that $c_a(h) = aha^{-1} = h_1 aa^{-1} = h_1 \in H$, so $c_a(H) \subseteq H$. Conversely, for any $h \in H$ we have $ha = ah_2$ for some $h_2 \in H$. Then $h = ah_2a^{-1} = c_a(h_2) \in c_a(H)$, so $H \subseteq c_a(H)$. Consequently, $c_a(H) = H$.

Suppose now that $c_a(H) = H$. Note that for any $h \in H$ we have $ah = (aha^{-1})a = c_a(h)a \in Ha$. Thus $aH \subseteq Ha$. Also, any $h \in H$ is of the form $c_a(h_1)$ for some $h_1 \in H$ so $ha = c_a(h_1)a = ah_1a^{-1}a = ah_1 \in aH$, which proves that $Ha \subseteq aH$. Thus $aH = Ha$.

b) Suppose that $a, b \in N_G(H)$. Then $c_a(H) = H = c_b(H)$ by a). Thus $c_{ab}(H) = c_a(c_b(H)) = c_a(H) = H$ and therefore $ab \in N_G(H)$ by a) again. Since $c_a(H) = H$ and c_a is a bijection, we have $c_a^{-1}(H) = H$. But $c_a^{-1} = c_{a^{-1}}$, so $a^{-1} \in N_G(H)$ by a). Finally, if $a \in H$ then $aH = H = Ha$, so $a \in N_G(H)$. Thus $H \subseteq N_G(H)$.

Recall now that $a \in Z(G)$ iff c_a is the identity map. But the identity map maps H onto itself, so $Z(G) \subseteq N_G(H)$ by a).

c) H is a subgroup of $N_G(H)$ by b). By definition of $N_G(H)$, $aH = Ha$ for all $a \in N_G(H)$. Thus $H \lhd N_G(H)$. It follows that if $N_G(H) = G$ then $H \lhd G$. Conversely, if $H \lhd G$ then $aH = Ha$ for every $a \in G$ so $N_G(H) = G$.

d) One way to solve this problem is to compute aH and Ha for every element a of G and see explicitely which a are in $N_G(H)$. We will use a more conceptual approach though. Recall that $Z(D_8) = \{I, T^2\}$. By b), we have $H \subseteq N_G(H)$ and $Z(G) \subseteq N_G(H)$. Since $N_G(H)$ is a subgroup, we have $\{I, T^2, S, ST^2\} \subseteq N_G(H)$. Note that $TH \neq HT$, so $T \notin N_G(H)$. Thus $N_G(H)$ is a proper subgroup of D_8, so it has 1, 2 or 4 elements by Lagranges theorem. But we have already found 4 elements in $N_G(H)$ so we must have $N_G(H) = \{I, T^2, S, ST^2\}$.

Problem 3. Let G be a finite group and let H be a subgroup of G. Let m be the smallest positive integer such that $a^m \in H$. Prove that $< a^m >= H\cap < a >$ and that m divides the order of a. **Hint:** Prove first that $\{k \in \mathbb{Z} : a^k \in H\}$ is a subgroup of $\mathbb{Z}$.

Solution: Consider the set $J = \{k \in \mathbb{Z} : a^k \in H\}$. If $s, t \in J$ then $a^s \in H$ and $a^t \in H$. Since H is a group, we have $a^{s+t} = a^s a^t \in H$ and $a^{-s} = (a^s)^{-1} \in H$. Thus $s + t$ and $-s$ are both in J. This shows that J is a subgrpup of $\mathbb{Z}$ (clearly, $0 \in \mathbb{Z}$). Since G is finite, the order of a is finite. Call it n. Thus $a^n = e \in H$, so $n \in J$. Recall now that every non-trivial subgroup of $\mathbb{Z}$ is of the form $d\mathbb{Z}$, where d is the smallest positive element of the subgroup. Since, by its definition, m is the smallest positive element of J, we have $J = m\mathbb{Z}$. Since $n \in J$, we have $m|n$. Finally $a^t \in H$ iff $t \in J$ iff $m|t$. It follows that $H\cap < a >= \{a^t : m|t\} =< a^m >$.

Problem 4. Let G be a group and let M, N be normal subgroups of G. Suppose that G/M and G/N are abelian. Prove that $G/(M \cap N)$ is also abelian.

Solution: Consider two elements $x, y \in G/(M \cap N)$. Thus $x = a(M \cap N)$, $y = b(M \cap N)$ for some $a, b \in G$. We want to prove that $xy = yx$, i.e. that $(ab)(M \cap N) = (ba)(M \cap N)$. This holds iff $(ba)^{-1}(ba) \in M \cap N$.

Since G/M is abelian, we have $(aM)(bM) = (bM)(aM)$, i.e. $(ab)M = (ba)M$. Thus $(ba)^{-1}(ab) \in M$. The same argument applied to G/N shows that $(ba)^{-1}(ab) \in N$. Thus $(ba)^{-1}(ba) \in M \cap N$, which is exactly what is needed to show that $xy = yx$. This proves that $G/(M \cap N)$ is abelian.