Math 701 Homework, Edition 6

Kenneth Brown, Brian Hanson, Jing Liu
Austin Mohr, Ranil Wanigasiri, Pam Welch

February 27, 2009

Problem 21.
Prove that $\mathrm{Aut}(S_n) \cong S_n$ for every natural number n.

Proof. Let $\sigma \in S_n$ and define $f(\tau) = \sigma\tau\sigma^{-1}$ for all $\tau \in S_n$. We claim that f is an automorphism of S_n: for all $\tau, \delta \in S_n$ we have $f(\tau\delta) = \sigma\tau\delta\sigma^{-1} = (\sigma\tau\sigma^{-1})(\sigma\delta\sigma^{-1}) = f(\tau)f(\delta)$. So f is a homomorphism. Now, $f(\tau) = f(\delta) \Leftrightarrow \sigma\tau\sigma^{-1} = \sigma\delta\sigma^{-1} \Leftrightarrow \tau = \delta$ so f is one-to-one. Also, for all $\tau \in S_n$, there exists $\sigma^{-1}\tau\sigma \in S_n$, such that $f(\sigma^{-1}\tau\sigma) = \sigma(\sigma^{-1}\tau\sigma)\sigma^{-1} = \tau$. So, f is onto. Hence, f is an isomorphism from S_n to S_n; i.e. $f \in \mathrm{Aut}(S_n)$

Now, let $\Phi : S_n \to \mathrm{Aut}(S_n)$. By using $\Phi_\sigma = f$ to denote $\Phi(\sigma) = f$, we have $\Phi_\sigma(\tau) = \sigma\tau\sigma^{-1}$ for all $\tau \in S_n$. Also, Φ is a homomorphism: Let $\tau \in S_n$. Then for all $\sigma, \delta \in S_n$, we have $\Phi_{\sigma\delta}(\tau) = (\sigma\delta)\tau(\sigma\delta)^{-1} = \sigma\delta\tau\delta^{-1}\sigma^{-1} = \sigma\Phi_\delta(\tau)\sigma^{-1} = \Phi_\sigma(\Phi_\delta(\tau)) = \Phi_\sigma \circ \Phi_\delta(\tau)$.

Claim: Φ is one-to-one.

$$\begin{aligned} & \sigma \in \ker\Phi \\ \Leftrightarrow\ & \Phi_\sigma = \mathrm{Id}_{S_n} \\ \Leftrightarrow\ & \Phi_\sigma(\tau) = \mathrm{Id}(\tau)\ \ \forall\tau \in S_n \\ \Leftrightarrow\ & \sigma\tau\sigma^{-1} = \tau\ \ \forall\tau \in S_n \\ \Leftrightarrow\ & \sigma\tau = \tau\sigma\ \ \forall\tau \in S_n \end{aligned}$$

Since S_n is the group of permutations, the identity is the only element in S_n that commutes with every element in S_n. So, $\ker\Phi = \{1\}$. Therefore, Φ is one-to-one. Since both S_n and $\mathrm{Aut}(S_n)$ are finite, it follows from Φ begin one-to-one that Φ is onto. Thus Φ is an isomorphism. It follows that $\mathrm{Aut}(S_n) \cong S_n$. □

PROBLEM 22.
Let p be a prime number. Prove that if a and b are elements of the symmetric group S_p, where a has order p and b is a transposition, then $\{a, b\}$ generates S_p.

Proof. Let $a, b \in S_p$ and let b be a transposition. Without loss of generality, let $b = (0\ 1)$. As a has order p and p is prime p, we have that a is p-cycle. Therefore, $a^k = (0\ 1 \ldots)$ for some k. We can re-index the other elements so that we have $a^k = (0\ 1 \ldots p-1)$. Let $c = a^k$. Then $cbc^{-1} = (0\ 1 \ldots p-1)(0\ 1)(p-1 \ldots 0\ 1) = (0)(1\ 2)(3)...(p-1) = (1\ 2)$. By induction, we have $c^k bc^{-k} = c(c^{k-1}bc^{-k+1})c^{-1} = (k+1\ \ k+2)$. Therefore, we have that $(0\ 1), (1\ 2), ..., (p-2\ \ p-1)$ are generated by $\{a, b\}$. Let (xy) be a transposition. Then $(x\ \ x+1)(x+1\ \ x+2) \cdots (y-1\ \ y) = (x\ \ y)$ and $(x\ \ y)$ is also generated by $\{a, b\}$. As every permutation can be decomposed into transpositions we conclude that $\{a, b\}$ generates S_p. □

PROBLEM 23.
Let $H \leq G$. Prove that $N_G(H)/C_G(H)$ is embeddable into $\mathrm{Aut}(H)$.

Proof. We begin by recalling the definitions of $N_G(H)$ and $C_G(H)$.

$$\begin{aligned} N_G(H) &= \{g \in G \mid gH = Hg\} \\ &= \{g \in G \mid H = gHg^{-1}\} \end{aligned}$$

$$\begin{aligned} C_G(H) &= \{g \in G \mid gh = hg \text{ for all } h \in H\} \\ &= \{g \in G \mid h = ghg^{-1} \text{ for all } h \in H\} \end{aligned}$$

Now, define a map $h : N_G(H) \to \mathrm{Aut}(H)$ by $h(n) = \varphi_n$ for each $n \in N_G(H)$, where we have $\varphi_n(h) = nhn^{-1}$ for $h \in H$. Since φ_n acts on H by conjugation, we see that $\varphi_n \in \mathrm{Aut}(H)$.
Claim: $h : N_G(H) \to \mathrm{Aut}(H)$ is a homomorphism. Let $a, b \in N_G(H)$. We have

$$\begin{aligned} h(ab) &= \varphi_{ab} \\ &= \varphi_a \varphi_b \\ &= h(a)h(b) \end{aligned}$$

Claim: $\ker h = C_G(H)$. We have

$$\begin{aligned} \ker h &= \{n \mid \varphi_n(h) = h \text{ for all } h \in H\} \\ &= \{n \mid nhn^{-1} = h \text{ for all } h \in H\} \\ &= C_G(H) \end{aligned}$$

By the isomorphism theorems, we now have $N_G(H)/C_G(H) \cong \text{im } h \leq \text{Aut}(H)$ which is what we wanted to establish. $\square$

Problem 24.
Let G be a group of order n. Define $\varphi : G \to G$ by $\varphi(a) = a^{n^2+3n+1}$ for all $a \in G$. Prove that φ is an automorphism of G.

Proof. First, we show that $a^n = 1$, for all $a \in G$. Let $a \in G$ and $|\langle a \rangle| = m$. By Lagrange's Theorem, $|\langle a \rangle|$ divides $|G|$, i.e. $m \mid n$. Let $n = mq$ for some $q \in \mathbb{N}$. Then $a^n = a^{mq} = (a^m)^q = 1$. Now, $\varphi(a) = a^{n^2+3n+1} = a^{n^2+3n} \cdot a = (a^n)^{n+3} \cdot a = 1 \cdot a = a$, for all $a \in G$. Therefore, φ is the identity map from G to G. So, φ is an automorphism of G. $\square$