HW 9 Selected solutions

Prof. Shahed Sharif

2.78 If the two elements are τ_1, τ_2, define $\sigma = \tau_1\tau_2$ and set $\tau = \tau_1$. Since G is finite, σ has finite order; call this order n. Now I just need to show that σ, τ satisfy the same relations as D_{2n}, and then by definition G will "be" D_{2n}. Since $\tau_2 = \tau^{-1}\sigma$, we have $\tau_2 \in \langle \tau, \sigma \rangle$, and so $\langle \tau, \sigma \rangle \supset \langle \tau_1, \tau_2 \rangle = G$. Therefore σ and τ generate G. We already have $\sigma^n = e$ and $\tau^2 = e$. We have

$$\begin{aligned} \tau\sigma &= \tau_1\tau_1\tau_2 \\ &= \tau_2 \end{aligned}$$

while

$$\begin{aligned} \sigma^{-1}\tau &= (\tau_1\tau_2)^{-1}\tau_1 \\ &= \tau_2\tau_1\tau_1 \\ &= \tau_2. \end{aligned}$$

Thus $\tau\sigma = \sigma^{-1}\tau$. The claim follows.

2.79 Use Prop 2.95 and the proof of Prop 2.97.

2.85 These can be done by table. Alternatively, the first one can be done in a similar way as last week's A.

2.86 Straightforward from the definitions.

2.90 For $g \in G$, if $\pi(g) = \prod_i^n x_i^{\varepsilon_i}$ (for some n, $\varepsilon_i = \pm 1$), show that $g^{-1} \prod g_{x_i}^{\varepsilon_i} \in T$.

2.97 Suppose $x, y \in G_m$. Then $mx = my = 0$, so $m(x + y) = mx + my = 0$, and hence $x + y \in G_m$. As the order of $-x$ is the same as that of x, we see that G_m is closed under inversion. Clearly $0 \in G_m$. Thus G_m is a subgroup. A similar argument holds for G_n.

Certainly $0 \in G_m \cap G_n$. Let $x \in G_m \cap G_n$. Then the order of x divides both m and n. But $\gcd(m, n) = 1$, so $\text{order}(x) = 1$, and hence $x = 0$. Therefore $G_m \cap G_n = \{0\}$.

We have $G_m + G_n \subset G$. Let $g \in G$. By the corollary to Lagrange's theorem, mn is a period of g, so $mng = 0$. By the Euclidean algorithm, $\exists a, b \in \mathbb{Z}$ such that $am + bn = 1$. Let $g_1 = bng$ and $g_2 = amg$. I claim that $g_1 \in G_m$, $g_2 \in G_n$, and $g_1 + g_2 = g$. We have $mg_1 = b(mng) = 0$, so $g_1 \in G_m$; a similar argument shows that $g_2 \in G_n$. Finally,

$$\begin{aligned} g_1 + g_2 &= bng + amg \\ &= (am + bn)g \\ &= 1 \cdot g \\ &= g. \end{aligned}$$

Therefore $G \subset G_m + G_n$, and so we have equality.

Finally, define $\varphi : G_m \times G_n \to G$ by $\varphi(g_1, g_2) = g_1 + g_2$. This is a homomorphism; the proof is straightforward, and omitted. By the previous part, φ is surjective. Finally, suppose $(g_1, g_2) \in \ker(\varphi)$. Then $g_1 + g_2 = 0$, so $g_2 = -g_1 \in G_m$, and hence $g_2 \in G_m \cap G_n$. By the first part, $g_2 = 0$, and so $g_1 = 0$ too. This shows that $\ker(\varphi)$ is trivial, and so φ is injective. It follows that φ is an isomorphism.

A. Direct computation.

B. Actually, the problem is incorrect as written: we need $n \geq 3$. Once we have that, observe that $(2\,3) \in H$, but

$$(1\,2)(2\,3)(1\,2)^{-1} = (1\,3) \notin H,$$

which shows that H is not normal. If $\sigma \in H$, then σ restricted to $\{2, 3, \ldots, n\}$ is a permutation, and is determined by this permutation. Therefore $\#H = (n-1)!$. By Lagrange's Theorem, there are $\#S_n/\#H = n!/(n-1)! = n$ cosets. I claim that for $i = 1, \ldots, n$, $(1\,i)$ is a complete system of representatives (where $(1\,1)$ means the identity). Since there are n elements in my list, it suffices to show that no two are in the same coset. For assume $i \neq j$. Without loss of generality $j \neq 1$. Then we have

$$\begin{aligned}(1\,i)^{-1}(1\,j)(1) &= (1\,j\,i)(1) \\ &= j \neq 1\end{aligned}$$

and therefore $(1\,i)^{-1}(1\,j) \notin H$, and so are in different cosets.

C. Recall the definition of union.