Math 332 HW 4

14.10 $\mathbb{Z}_{34}$ is abelian, and D_{17} is not.

14.21 Any automorphism of $\mathbb{Z}$ must send 1 to another generator. There are only two generators: ± 1. So that gives two automorphisms: $1 \mapsto 1$ and $1 \mapsto -1$, and $\mathrm{Aut}(\mathbb{Z}) \cong \{\pm 1\} \cong \mathbb{Z}_2$.

14.23 $U_7 = \{1,2,3,4,5,6\}$ is cyclic with two elements of order 6, namely 3 and 5. So there are two automorphisms again, determined by $3 \mapsto 3$ and $3 \mapsto 5$, and $\mathrm{Aut}(U_7) \cong \mathbb{Z}_2$.

$x \mapsto x$ $\quad$ $x \mapsto x^{-1}$

15.11 (a) $G_x = \mathrm{Stab}(x) = \{g \in G : gx = x\}$. First note that $e \in G_x$; so $G_x \neq \emptyset$. Next suppose $g, h \in G_x$. Then $(gh)(x) = g(hx) = gx = x \Rightarrow gh \in G_x$ and $hx = x \Rightarrow h^{-1}(hx) = h^{-1}x \Rightarrow (h^{-1}h)x = h^{-1}x \Rightarrow ex = h^{-1}x \Rightarrow x = h^{-1}x \Rightarrow h^{-1} \in G_x$. $\square$

(b) Suppose $z \in \mathrm{Orb}(x) \cap \mathrm{Orb}(y)$, say $z = gx \overset{*}{=} hy$.

To show $\mathrm{Orb}(x) \subseteq \mathrm{Orb}(y)$, take an arbitrary $fx \in \mathrm{Orb}(x)$ (with $f \in G$). By $(*)$, $x = g^{-1}hy$. So $fx = fg^{-1}hy \in \mathrm{Orb}(y)$.

Similarly, $\mathrm{Orb}(y) \subseteq \mathrm{Orb}(x)$. $\square$

16.14 (a) The group G is generated by G, itself, which is finite.

(b) If a has order mp, then a^m has order p.

(c) If $|\langle a_1, \dots, a_n \rangle| = k$, we know $a_i^k = 1$ for $i = 1, \dots, n$ by corollary 16.7 (essentially, by Lagrange's thm.). Thus, k divides $|a_i|$ $\forall i$, which means k is divisible by $\mathrm{lcm}(|a_1|, \dots, |a_n|)$.

(d) We prove this by induction on n. The case $n=1$ holds since $|\langle a_1 \rangle| = |a_1|$.

Let $H_{n-1} = \langle a_1, \dots, a_{n-1} \rangle$ and $H_n = \langle a_1, \dots, a_n \rangle$ and assume an integer k s.t.

$k|H_{n-1}| = |a_1| \cdots |a_{n-1}|.$ (1) Consider the cosets $H_{n-1}, a_n H_{n-1}, a_n^2 H_{n-1}, \dots$

of H_{n-1} in H_n. Let ℓ be the smallest positive integer s.t. $a_n^\ell H_{n-1} = H_{n-1}$.

Then the number of cosets of H_{n-1} is ℓ, and $|H_n| = \ell |H_{n-1}|$ (2)

Claim: ℓ divides $|a_n|$. Once we prove this claim, we have $|a_n| = m\ell$ (3) for some integer m. Hence, $km|H_n| \overset{(2)}{=} km\ell |H_{n-1}| \overset{(3)}{=} |a_n| k |H_{n-1}|$

$\overset{(1)}{=} |a_1| \cdots |a_n|$, as required.

Pf of claim / Let $s = \gcd(\ell, |a_n|)$. By the Euclidean algorithm,

$s = p\ell + q|a_n|$ for some integers p, q. So $a_n^s = a_n^{p\ell + q|a_n|} = (a_n^\ell)^p$

But ℓ is the smallest positive integer s.t. $a^\ell \in H_{n-1}$, and $a_n^s = (a_n^\ell)^p \in H_{n-1}$

$\Rightarrow s = \ell$. Thus, $\ell = \gcd(\ell, |a_n|)$, which says ℓ divides $|a_n|$. ☒

(e) Let $G = \{a_1, \dots, a_n\}$. If no a_i has order divisible by p, then $|G| = |\langle a_1, \dots, a_n \rangle|$, which is a factor of $|a_1| \cdots |a_n|$, is not divisible by p. But we are given that $|G| = kp$ for some k. Hence, $\exists\, a_i \in G$ with order $|a_i| = mp$. By part (a), we get an element of order p, namely a_i^m. ☐

1. $U_8 = \{1, 3, 5, 7\}$ Left multiplication gives permutations of U_8:

$$\ell_1 : \begin{array}{c} 1 \to 1 \\ 3 \to 3 \\ 5 \to 5 \\ 7 \to 7 \end{array}, \quad \ell_3 : \begin{array}{c} 1 \to 3 \\ 3 \to 1 \\ 5 \to 7 \\ 7 \to 5 \end{array}, \quad \ell_5 : \begin{array}{c} 1 \to 5 \\ 3 \to 7 \\ 5 \to 1 \\ 7 \to 3 \end{array}, \quad \ell_7 : \begin{array}{c} 1 \to 7 \\ 3 \to 5 \\ 5 \to 3 \\ 7 \to 1 \end{array}$$

2. (16.13) (a) $aH = H \iff a \in H$

Pf/ $(\Rightarrow)$ $a \in aH$ since $e \in H$. Thus, $aH = H \Rightarrow a \in H$

$(\Leftarrow)$ Conversely, suppose $a \in H$. Since H is a group, it follows that $ah \in H$ $\forall h \in H$. Thus, $aH \subseteq H$. On the other hand, $a \in H \Rightarrow$ $a^{-1} \in H \Rightarrow$ if $h \in H$, then $a^{-1}h \in H \Rightarrow h = a(a^{-1}h) \in aH$.

(b) $aH = bH \iff H = a^{-1}bH$.

Pf/ ($\Rightarrow$) Suppose $aH = bH$. Then, since $b \in bH \overset{=}{} aH$, there exists $h \in H$ s.t. $b = ah$. Thus, $a^{-1}b = h \in H$. By part (a), we have $H = a^{-1}bH$.

($\Leftarrow$) Suppose $H = a^{-1}bH$, and let $ah \in aH$. Since $e \in H = a^{-1}bH$, $\exists h' \in H$ s.t. $e = a^{-1}bh'$, and thus, $a = bh'$. So $ah = b(h'h) \in bH$ since $h'h \in H$. So $aH \subseteq bH$. On the other hand, take $bh \in bH$. Then $e \in H \Rightarrow a^{-1}b \in a^{-1}bH = H \Rightarrow a^{-1}b = h''$ for some $h'' \in H \Rightarrow b = ah'' \Rightarrow bh = a(h''h) \in aH$ since $hh'' \in H$. Thus, $bH \subseteq aH$. $\square$

3. For each $1 < k \leq n$, S_n has the k-cycle $(1,2,\ldots,k)$, and $x \mapsto x^k$ takes this k-cycle to the identity $()$. It also takes $()$ to itself. So $x \mapsto x^k$ can never be a permutation of S_n.

(I meant to ask about cyclic groups!)