Homework 6

Anthony Jones

1a) Every element of S_n can be written as a unique product of disjoint cycles,

Luckily, for S_7, this is easy to find:
(Recall that the order of an element of S_n is the lcm of the lengths of disjoint cycles)

	type of cycles	order	# of perm
	()	1	$1 = 1$
	(12)	2	$\binom{7}{2}\left(\frac{2!}{2}\right) = 21$
	(123)	3	$\binom{7}{3}\left(\frac{3!}{3}\right) = 70$
	(1234)	4	$\binom{7}{4}\cdot\left(\frac{4!}{4}\right) = 210$
	(12345)	5	$\binom{7}{5}\cdot\left(\frac{5!}{5}\right) = 504$
	(123456)	6	$\binom{7}{6}\cdot\left(\frac{6!}{6}\right) = 840$
	(1234567)	7	$\frac{7!}{7} = 720$
~~(2,2)~~	(12)(34)	2	$\binom{7}{2}\frac{2!}{2}\cdot\binom{5}{2}\frac{2!}{2}\cdot\frac{1}{2!} = 105$
(2,3)	(12)(345)	6	$\binom{7}{2}\frac{2!}{2}\cdot\binom{5}{3}\frac{3!}{3} = 420$
~~(2,4)~~	(12)(3456)	4	$\binom{7}{2}\frac{2!}{2}\cdot\binom{5}{4}\frac{4!}{4} = 630$
~~(2,5)~~	(12)(34567)	10	$\binom{7}{2}\frac{2!}{2}\cdot\frac{5!}{5} = 504$
~~(3,3)~~	(123)(456)	3	$\binom{7}{3}\frac{3!}{3}\cdot\binom{4}{3}\frac{3!}{3}\cdot\frac{1}{2!} = 280$
~~(3,4)~~	(123)(4567)	12	$\binom{7}{3}\frac{3!}{3}\cdot\left(\frac{4!}{4}\right) = 420$
~~(2,2,2)~~	(12)(34)(56)	2	$\binom{7}{2}\frac{2!}{2}\cdot\binom{5}{2}\frac{2!}{2}\cdot\binom{3}{2}\frac{2!}{2}\cdot\frac{1}{3!} = 105$
~~(2,2,3)~~	(12)(34)(567)	6	$\binom{7}{2}\frac{2!}{2}\cdot\binom{5}{2}\frac{2!}{2}\cdot\binom{3}{3}\frac{3!}{3}\cdot\frac{1}{2!} = 210$

* Note: repeating cycles n times has $\frac{1}{n!}$ times as many elements fewer as (ab)(cd) = (cd)(ab); cycles can be arranged n! times...

Therefore the possible values of k are
k=1 with 1 element, k=2 with 231 elements, k=3 with 350 elements, k=4 with 840 elements, k=5 with 504 elements, k=6 with 1470, k=7 with 720, k=10 with 504, and k=12 with 420.

Homework 6

Anthony Jones

2b) As mentioned before, the orders of elements in S_n are equal to the lcm of the lengths of disjoint cycles of that element. Therefore any element $a \in S_p$ with $|a| = p$ must have a disjoint cycle of length p, as p is prime and hence no smaller lengths multiply to p.

Furthermore, as the set forming S_p has p elements, a disjoint cycle of length p uses all elements of A. Therefore any element $a \in S_p$ with $|a| = p$ is a single cycle with length p.

There are $\left(\frac{p!}{p}\right)$ possible such elements; $p!$ possible choices, but for each choice there are p permutations that are cyclically the same element $[(abc) = (cab) = (bca)]$.

Thus $\frac{p!}{p}$ elements of order p are in S_p.

Homework 6

Anthony Jones

1c) I claim there are $\frac{(p-1)!}{p-1}$ subgroups with order p in S_p.

Pf: Let $H \leq S_p$ with $|H| = p$. Then, by Lagrange's Thm, there are <u>no</u> proper, non-trivial subgroups of H as the only divisors of p are 1 and p.

Let $h \in H$ where $h \neq e$.

Observe that $|h|$ must equal p, as if not, then $\langle h \rangle \leq H$ would be a proper subgroup with $|\langle h \rangle| \neq p$. Thus all non-identity elements of H have order p and $\langle h \rangle = H$ (as $|\langle h \rangle| = |H|$).

Furthermore, because H is shown to be cyclicly defined by elements of order p, we can count the number of subgroups H by counting all subgroups cyclicly generated by elements in S_p with order p:

$\frac{!p}{p} = (p-1)!$ total elements with order p;

$(p-1)$ different elements with order p that generate the same subgroup within $\langle h \rangle$,

and therefore $\frac{(p-1)!}{p-1}$ different subgroups.

Homework 6

AJ

2) Let $f: G \to \text{Inn}(G)$ be defined by $f(g) = \phi_g$ where $\phi_g(x) = g^{-1}xg$.

Then for $g \in G$, $h \in G$

$$f(gh)(x) = \phi_{gh}(x)$$
$$= (gh)^{-1} x (gh)$$
$$= h^{-1}g^{-1} x gh$$
$$= h^{-1} \phi_g(x) h$$
$$= \phi_h \phi_g(x)$$
$$= [f(g) f(h)](x).$$

Therefore f is a homomorphism.
Recall $\text{Ker}(f) = \{g \in G \mid f(g) = \phi_e\}$.

Observe that $f(g) = \phi_g = \phi_e$ then

$$g^{-1}xg = x, \ \forall x \in G.$$

$(\phi_g(x) = \phi_e(x)$ for $\forall x \in G)$

Therefore if $g \in \text{Ker}(f)$ then

$$xg = gx, \ \forall x \in G \iff g \in Z(G)$$

And by the First Isomorphism Thrm,
$$G/Z(G) \cong \text{Inn}(G).$$

* 2(a) Observe that f is onto as for any $\phi_g \in \mathrm{Inn}(G)$ we have $g \in G$ where

$$f(g) = \phi_g \quad \text{(by definition)}.$$

Therefore $\mathrm{im}(f) = \mathrm{Inn}(G)$.

Homework 6 AJ

3a) Let $g \in G$ and $h \in H$ were H is characteristic in G.

Let $\phi_g : G \to G$ be defined as an inner automorphism $\phi_g(x) = g^{-1}xg \; \forall x \in G$.

Observe that $\phi_g \in \mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$, so therefore $\phi_g(H) \subseteq H$.

This means $g^{-1}hg \in H$ for $\forall h \in H$, or in other words, $H \trianglelefteq G$.

3b) Let $\phi|_H : H \to G$ be defined as the function $\phi|_H(x) = \phi(x) \; \forall x \in H$, where ϕ is some arbitrary element in $\mathrm{Aut}(G)$.

Observe that since H is characteristic, $\phi(H) \subseteq H$ and therefore $\phi|_H(x) \in H$ for any element $x \in H$.

Thus $\phi|_H : H \to H \leq G$.

Furthermore, $\phi|_H$ is a homomorphism as

$$\phi|_H(xy) = \phi(xy) = \phi(x)\phi(y)$$
$$= \phi|_H(x)\,\phi|_H(y),$$

$\phi|H$ is surjective as any $h \in H$ is also $h \in G$, and thus $h = \phi(x) = \phi|_H(x)$ for $x \in H$.

Finally, $\phi|_H$ is injective as $\phi|_H(x) = \phi(x)$, which being $\in \mathrm{Aut}(G)$ is 1-to-1. Thus $\phi|_H \in$

3b) Thus $\phi|_H \in \mathrm{Aut}(H)$ as

it is an isomorphism that maps to itself.

3c) $(\mathbb{Z},+) \trianglelefteq (\mathbb{R},+)$.

Let $\emptyset : \mathbb{R} \to \mathbb{R}$ be the automorphism defined by $\emptyset(r) = r + \pi$.

$\emptyset(\mathbb{Z},+)$ is not contained in $(\mathbb{Z},+)$ as for any element $z \in \mathbb{Z}$, $z + \pi \notin \mathbb{Z}$.

Therefore $(\mathbb{Z},+)$ is not characteristic to $(\mathbb{R},+)$.

3d) Yes ~ difficult proof

Homework 6

Anthony Jones

4) Assume G is abelian.

We know from Cauchy's Theorem that there exists elements $x, y \in G$

$$|x| = 2$$

$$|y| = p$$

As 2 and p are factors of $|G|$. Consider the element xy. We know from Corollary 4.2.5 of Lagranges Theorem that $|xy| \mid |G|$, meaning $|xy| = 1, 2, p, 2p$.

→ $|xy| \neq 1$ as this implies that $x = y^{-1}$, but $|x| \neq |y| = |y^{-1}|$, so it is false.

→ $|xy| \neq 2$ as (given G is abelian) this implies $(xy)^2 = x^2y^2 = y^2 = e$, which is false as $|y| = p$ where p is odd.

→ $|xy| \neq p$ as (similarly) this implies $(xy)^p = x^py^p = x^{2n+1} = (x^2)^n x = x = e$, for $p = 2n+1$, which is false as $|x| = 2$.

Therefore $|xy| = 2p$, meaning $\langle xy \rangle = G$ is cyclic as $|\langle xy \rangle| = |G|$ and every $a \in \langle xy \rangle$ is also $a \in G$. Hence from Theorem 3.2.5, we know the cyclic group

$$\mathbb{Z}_{2p} \cong G \text{ is isomorphic to } G.$$

Homework 6

Anthony Jones

Now

4(cont) Assume G is non-abelian.

Using Cauchy's Theorem as in before, we know $r, s \in G$

$|r| = p$
$|s| = 2.$

Because G is strickly non-abelian, $sr = gs \iff r \neq g$.

Observe that $[G : \langle r \rangle] = \frac{|G|}{|r|} = 2$, which we know from HW that means $\langle r \rangle \trianglelefteq G$. Therefore $g^{-1}hg \in \langle r \rangle$ for any $g \in G$ and $h \in \langle r \rangle$.

Also observe that $|s| = 2 \iff s = s^{-1}$ as $s^2 = e = s \cdot s^{-1}$.

Finally consider $srs \in G$. We know (given $r \in \langle r \rangle$) that $srs \in \langle r \rangle$, shown

$s^{-1}rs = r^n$

Now consider exponentiating by n:

$$(r^n)^n = (s^{-1}rs)^n = s^{-n}r^ns^n = s^{-n-1}rs^{n+1}$$
$$= (s^{-n-1}s^{n+1})r(s^{n+1}s^{-n-1}) = r.$$

Therefore $r^{(n^2)} = r$ and so $r^n = r^{-1}$.

Thus $G = \langle r, s \mid r^p = s^2 = e,\ s^{-1}rs = srs = r^{-1} \rangle$ and there for $G \cong D_p$ is clearly shown.

4) * $r^{n^2} = r \iff$ $n=1$ or $n=-1$.

If $n=1$ then $srs = r^n = r$ and therefore $sr = rs$. However, G is strictly non-abelian and therefore $n=-1$. *