HW 1 Selected solutions

DF 1.1

#17. Suppose $|x| = n$. Then $x^n = e$, by definition of order.

So $x(x^{n-1}) = x^n = e$ and $x^{n-1} \cdot x = x^n = e$

this shows that x^{n-1} is the inverse of x.

#22 (hint: use induction to show $(g^{-1}xg)^n = g^{-1}x^n g$.

Now suppose $|x| = m$.

Then $(g^{-1}xg)^m = g^{-1}eg = e$

If for any d, we have

$g^{-1}x^d g = e$, then we would have

$x^d = geg^{-1} = e$

Thus, $g^{-1}x^d g \neq e$ for any $d < m$.)

#25.

Suppose $x^2 = 1$ for all $x \in G$.

Let $a, b \in G$. Then $a^2 = 1$, $b^2 = 1$ and $(ab)^2 = 1$

So $1 = (ab)^2 = a^2 b^2$

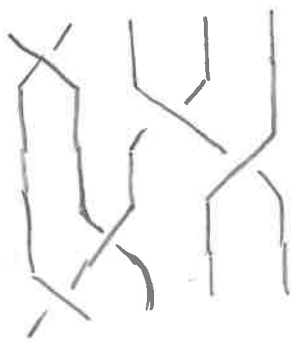
This implies that $abab = aabb$

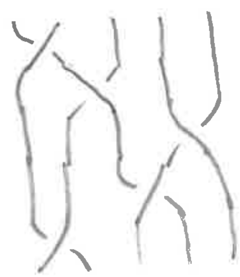
so $bab = abb$ (by cancellation)

$ba = ab$ (cancellation again)

Since this is true for all a, b in G, G is abelian.

2. In class we showed that $a_1 a_2 \neq a_2 a_1$ in B_3. For a braid group with more than 3 strands, the same argument works — you can copy the proof!

3. 

4. $a_1^{-1} a_2 a_4 a_3^{-1} a_1^{-1}$ 

DF 1.3

\# 8. Let σ_i be the permutation of Ω defined by for $i = 1, 2, 3, \ldots$

$$\begin{cases} \sigma_i(i) = i+1 \\ \sigma_i(i+1) = i \\ \sigma_i(j) = j & \text{for any } j \neq i \end{cases}$$

If $i \neq i'$ then $\sigma_i \neq \sigma_{i'}$, so this gives an infinite collection of elements of S_Ω.

DF 1.3 # 16

To form an m-cycle $(k_1 k_2 \dots k_m)$ we have n choices of elemts for k_1. Once k_1 is chosen, there remain $(n-1)$ other choices for k_2.
Similarly, after choosing $k_1, \dots k_j$ there are $n-j$ choices for k_{j+1}. This gives $n(n-1)\cdots(n-m+1)$ total choices of ordered sequences $(k_1 k_2 \dots k_m)$.

However, $(k_1 k_2 \dots k_m) = (k_2 k_3 \dots k_m k_1) = (k_3 k_4 \dots k_2)$ etc.
so we overcounted by a factor of m.

6 a) Let $S = \{ \frac{1}{p} \mid p \text{ is prime} \}$.
let $q \in \mathbb{Q}^{>0}$. Then q can be written as $\frac{a}{b}$, where a, and b are positive integers.
Let $a = p_1 p_2 \cdots p_k$ be the prime factorization of a and $b = q_1 q_2 \cdots q_m$ the prime factorization of b.
Then $\frac{a}{b} = p_1 \cdots p_k \cdot \frac{1}{q_1} \cdot \cdots \frac{1}{q_m}$

Since $p_i = (\frac{1}{p_i})^{-1}$ and $\frac{1}{p_i} \in S$
and $\frac{1}{q_i} \in S$,
we have written $\frac{a}{b}$ as a product of elements of S and their inverses.

b) Suppose $(\mathbb{Q}^{>0}, \times)$ was generated by a finite set S.
Write each element of S as $\frac{a}{b}$ in lowest terms, and let p be the largest prime number appearing in any numerator or denominator.
Let q be a prime larger than p. Then q ~~is~~ $\longrightarrow$

(continued) cannot be written as a product of elements of S and inverses, otherwise we would have a factorization of q into smaller primes.

7. (hint)

to show $|b| = 4$, just multiply

$$b^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$b^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$b^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \text{identity.}$$

Similar for $|a| = 6$.

Consider the set $\{ab, (ab)^2, (ab)^4, \ldots\}$

$$ab = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$(ab)^2 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$$

$(ab)^4 = \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}$ and you can prove (by induction!) that $(ab)^{2k} = \begin{pmatrix} 1 & 0 \\ -2k & 1 \end{pmatrix}$

so this set contains infintely many distinct elements