MATH 2100 Assignment 12 Solutions

Problem 1. *Show that $|a_i| = |a_j|$ if and only if $(|a|, i) = (|a|, j)$.*

Proof. This comes almost immediately from Theorem 4.2. In fact, a chain of if-and-only-ifs is safe to use here because it's so short:

$$|a_i| = |a_j| \iff \frac{|a|}{(|a|, i)} = \frac{|a|}{(|a|, j)} \iff (|a|, i) = (|a|, j).$$

Note that gcds are never 0, so the division in the reverse direction of the proof is okay. □

Problem 2. *Show that $\langle a\rangle = \langle a^j\rangle$ if and only if $(|a|, j) = 1$.*

Proof. ($\Longrightarrow$) We have $\langle a\rangle = \langle a^j\rangle$, so $a \in \langle a^j\rangle$. Thus there is some $k \in \mathbb{Z}$ such that $a = (a^j)^k = a^{jk}$. But now $1 = aa^{-1} = a^{jk-1}$, so $|a|$ divides $jk - 1$; say $q|a| = jk - 1$ for some $q \in \mathbb{Z}$. Then $1 = jk - q|a|$, so we have a linear combination of j and $|a|$ making 1, and this can only happen if $(|a|, j) = 1$.

(We can also get this quickly from Corollary 2, or by using problem 1: if $\langle a\rangle = \langle a^j\rangle$, then $|a| = |a^j|$, so $(|a|, j) = (|a|, 1) = 1$.)

($\Longleftarrow$) By Theorem 4.2, $\langle a^j\rangle = \langle a^{(|a|,j)}\rangle = \langle a^1\rangle = \langle a\rangle$.

(We *can't* quite get this from problem 1; $|x| = |y|$ does not in general imply $\langle x\rangle = \langle y\rangle$. It does in a cyclic group, but you need to prove it.)

$\therefore$ ($\Longleftrightarrow$). □

Problem 3. *Draw the subgroup lattice of $\mathbb{Z}_{p^2q}$ and the divisor lattice of p^2q, where p and q are distinct primes.*

Proof. We'll do the divisor lattice first. By the Fundamental Theorem of Arithmetic, the factors of p^2q are exactly p^mq^n where $0 \le m \le 2$, $0 \le n \le 1$. There are six of these: $\{1, p, p^2, q, pq, p^2q\}$. Using arrows to mean "is a multiple of", we have

$$\begin{tikzcd}
 & p^2q \arrow[dl] \arrow[dr] \arrow[ddl] \arrow[ddr] \arrow[ddd] & \\
p^2 \arrow[d] \arrow[ddr] & & pq \arrow[dll] \arrow[d] \arrow[ddl] \\
p \arrow[dr] & & q \arrow[dl] \\
 & 1 &
\end{tikzcd}$$

To simplify the diagram, we'll make the arrows transitive; that is, if we have $A \to B \to C$, we'll leave out $A \to C$. This leaves

$$\begin{tikzcd}
 & p^2q \arrow[dl] \arrow[dr] & \\
p^2 \arrow[d] & & pq \arrow[ll, shift left=0, to=3-1] \arrow[d] \\
p \arrow[dr] & & q \arrow[dl] \\
 & 1 &
\end{tikzcd}$$

Now for the subgroup lattice. We know by the Fundamental Theorem of Cyclic Groups that Z_{p^2q} has a unique subgroup for each of its divisors; thus the diagram will look just like the one for p^2q. Moreover, if k is a divisor, the subgroup will be generated by $\frac{p^2q}{(p^2q,k)} = \frac{p^2q}{k}$, giving us our generators.

We get the following lattice, where arrows now mean "is a subgroup of". It matches the divisor lattice if you look at group *sizes*; if you look at generators, it's inverted (why?).

$$\begin{tikzcd}
 & \langle 1 \rangle = \mathbb{Z}_{p^2q} & \\
\langle q \rangle \arrow[ur] & & \langle p \rangle \arrow[ul] \\
\langle pq \rangle \arrow[u] \arrow[urr] & & \langle p^2 \rangle \arrow[u] \\
 & \langle p^2q \rangle = \{0\} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

□

Problem 4. *Find all generators for the unique order-8 subgroup of (a)* $\mathbb{Z}_{24}$ *and (b)* $G = \langle a \rangle$ *where* $|a| = 24$.

Proof. Like problem 3, this is a two-part question where the only real difference is notation. We'll do (b) first and use it to save time with (a).

We know by the Fundamental Theorem of Cyclic Groups that the order-8 subgroup of G is $\langle a^{24/8} \rangle = \langle a^3 \rangle$. Now consider Theorem 4.2, Corollary 2: we have $\langle a^j \rangle = \langle a^3 \rangle$ if and only if $(24, j) = (24, 3) = 3$. What are the numbers (from 0 to 23) whose gcd with 24 is 3? They must be multiples of 3, and they must not be multiples of 6; this leaves 3, 9, 15, and 21. Thus the generators of the order-8 subgroup are exactly

$$\{a^3, a^9, a^{15}, a^{21}\}.$$

What about (a)? Remember that $\mathbb{Z}_{24}$ is just a cyclic group of order 24 written in additive notation. Its generator is 1. Plugging this directly into part (b) and switching notation, we find that the generators are $\{3(1), 9(1), 15(1), 21(1)\}$, or as we usually write them, $\{3, 9, 15, 21\}$. □