21-373: Algebraic Structures
Assignment 2

Peter Battaglino
3. February, 2005

Problem 3.26: Suppose n is an even positive integer and H is a subgroup of $\mathbb{Z}_n$. Prove that either every member of H is even or exactly half of the members of H are even.

<u>Solution:</u> Since $\mathbb{Z}_n$ is a cyclic group, we know that all of its subgroups have to be cyclic. Since H is therefore cyclic, we can write $H = \langle a \rangle$ for some $a \in \mathbb{Z}_n$. Suppose a is even. Then $\sum_{i=1}^{k} a$ must be even for any positive integer k, and all of the elements of $\langle a \rangle = H$ must be even. Now suppose a is odd. Then the elements of $\{a, a+a, a+a+a, \cdots, 0\}$ alternate between being even and odd as we traverse them in order. If this set has an even number of elements (which are necessarily distinct by definition of the group generated by a), then we see that half of them are even and half of them are odd, which was to be shown. To show that the order of $\langle a \rangle$ must be even, given that n is even, we observe that $|a|a \mod n = 0$. Since a is odd by assumption, we conclude that $|a|$ must be even if $|a|a$ is to be divisible by an even number (no odd number is divisible by an even number). Thus we have that the order of the group generated by an odd a must be even, so half the elements are even and half the elements are odd.

Problem 3.52: Let G be a finite group with more than one element. Show that G has an element of prime order.

Solution: Let's pick some element $g \in G$ that has order $|g| = m$. Suppose m is not a prime number, and is not equal to 1. m has the prime decomposition

$$m = p_1^{q_1} p_2^{q_2} \cdots p_n^{q_n}, \tag{1}$$

where each of the q_i are positive integers and each of the p_i are prime. Since g has order m, we know that

$$g^{p_1^{q_1} \cdots p_n^{q_n}} = 1. \tag{2}$$

We can use the properties of exponents to write

$$\left(g^{p_1^{q_1} \cdots p_n^{q_n - 1}} \right)^{p_n} = 1, \tag{3}$$

which says that the order of the element $g' = g^{p_1^{q_1} \cdots p_n^{q_n - 1}}$ divides p_n. Since p_n is a prime number, we know that either $|g'| = 1$ or $|g'| = p_n$. The case $|g'| = 1$ contradicts the assumption that $|g| = m$, so we take $|g'| = p_n$. Thus we have found an element $|g'| \in G$ with prime order, given any element g with non-prime (and non-unity) order.

Problem 4.32: Determine the subgroup lattice for $\mathbb{Z}_{12}$.

<u>Solution:</u> We can list the subgroups of $\mathbb{Z}_{12}$ as

$$\begin{aligned}
\langle 0\rangle &= \{0\} \\
\langle 1\rangle &= \mathbb{Z}_{12} \\
\langle 2\rangle &= \{0,2,4,6,8,10\} \\
\langle 3\rangle &= \{0,3,6,9\} \\
\langle 4\rangle &= \{0,4,8\} \\
\langle 5\rangle &= \mathbb{Z}_{12} \\
\langle 6\rangle &= \{0,6\} \\
\langle 7\rangle &= \mathbb{Z}_{12} \\
\langle 8\rangle &= \{0,4,8\} = \langle 4\rangle \\
\langle 9\rangle &= \{0,3,6,9\} = \langle 3\rangle \\
\langle 10\rangle &= \{0,2,4,6,8,10\} = \langle 2\rangle \\
\langle 11\rangle &= \mathbb{Z}_{12}
\end{aligned}$$

The subgroup lattice is illustrated in Fig. 1.

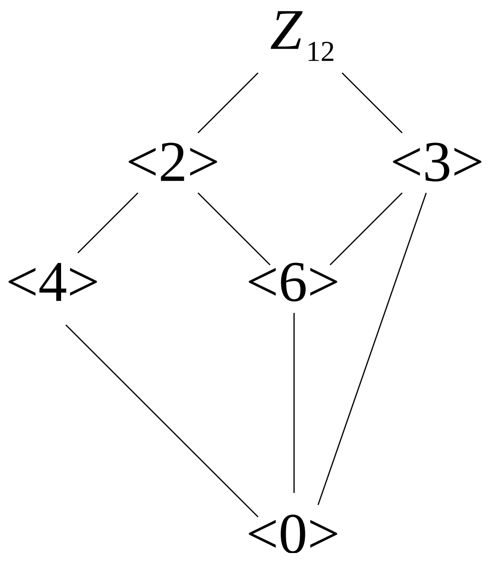

Figure 1: The subgroup lattice for $\mathbb{Z}_{12}$

Problem 4.47: Determine the orders of the elements of D_{33} and how many there are of each.

<u>Solution:</u> Let $R = R_{2\pi/33}$. The group D_{33} contains 33 reflections and 33 rotations (the identity being included in the rotations). Each of the 33 reflections has order 2. The identity rotation is of order 1. Since the only divisors of 33 are itself, 1, 11, and 3, we know that all the subgroups of the group generated by R must have order of 1, 3, 11, or 33. All the groups with order 11 satisfy $11 = 33/\gcd(33,k)$, where R^k is the generator of the group. The values of k which satisfy this equation are 3, 6, 9, 12, 15, 18, 21, 24, 27, and 30. Thus there are 10 groups with order 11. The groups of order 3 satisfy $\gcd(33,k) = 11$, which has the solutions 11 and 22. The rest of the elements in the subgroup $\langle R\rangle \leqslant D_{33}$ must all have order 33, so there are 20 elements with order 33.

To summarize, there is one element with order 1, there are 33 elements with order 2, 2 of order 3, 10 of order 11, and 20 of order 33.

Problem "Additional Problem": Let H, H' be subgroups of a group G. Prove that $H \cup H'$ is a subgroup of G if and only if one of the subgroups H, H' is a subset of the other.

<u>Solution:</u>
$\Rightarrow$:
Let $a \in H, b \in H'$, and $a \notin H'$. Since $a, b \in H \cup H'$ and $H \cup H'$ is a group, we know that $ab \in H \cup H'$, which implies that $ab \in H$ or $ab \in H'$. Suppose $ab \in H$. Then, since $a \in H$ and H is a group, we know that $a^{-1} \in H$ and thus that $a^{-1}ab \in H$, which means that $b \in H$. Now suppose that $ab \in H'$ instead. Then $abb^{-1} \in H'$, so $a \in H'$, which contradicts the assumption $a \notin H'$. Thus we see that if we take one element of H and one element of H', and restrict one of the elements to lie in one of H, H' but not the other, then the other element must be a member of the same subgroup as the first, which means that either $H \subset H'$ or $H \supset H'$ since our argument is valid for arbitrary a and b.
$\Leftarrow$:
Let $H \supset H'$. Then $H \cup H' = H$, and since H is a group, $H \cup H'$ is also a group. Let $H \subset H'$. Then $H \cup H' = H'$, and since H' is a group, $H \cup H'$ is also a group.