HOMEWORK SOLUTIONS 12/05/03

6.8

Make a multiplication table for $U(9)$. Is this a cyclic group? If so, find all generators.

First of all, the set of $U(9)$ is only those $1 \leq a < 9$ such that $(a, 9) = 1$. This set is $\{1, 2, 4, 5, 7, 8\}$. Here is the table:

	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	6	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

It is certainly cyclic, and 2 and 5 are generators.

6.16

Suppose g is in a group G and that g has order n. Prove that the order of g^{-1} is n as well.

First of all, g has order n means that $g^n = e$, and that $g^m \neq e$ for any $m < n$. Next, suppose $(g^{-1})^n = x$; then multiply in front by g to get $g(g^{-1})^n = gx$, or $(gg^{-1})(g^{-1})^{n-1} = gx$, which is $e(g^{-1})^{n-1} = (g^{-1})^{n-1} = gx$. Do this $n - 1$ more times, and you will have $e = g^n x$. However, $g^n = e$, so $x = e$, and g^{-1} has order no greater than n. Finally, suppose that g^{-1} has some order $m < n$; in that case, let $g^m = y$, and premultiply by g^{-1} (m times) as we just did above with g; then we will get $e = y = g^m$, which is a contradiction, because $m < n$, where n is the order of g. So the order of g and g^{-1} is n.

6.19(a,b,f)

Find the order of the element 2 in each of the following groups. Verify that the order of 2 is a divisor of the order of the group, where appropriate.

Consult the book for each group. For the first one, the multiples of 2 are $2, 4, 1, 3, 0$, so the order is 5 (which is the order of the group). For the units of that same group, on the other hand, the powers of 2 are $2, 4, 3, 1$, so it has order 4, again the order of the group. Finally we look the multiples $2, 4, 6, 8, 10, 0$, which means it has order 6, which does indeed divide the order of the group (12).

6.37

Are $\mathbb{Q}$, $3\mathbb{Z}$, and $3\mathbb{Z} + 1$ rings or not?

Certainly $\mathbb{Q}$ is a ring. It has multiplication and addition, they are closed and associative, and we even have multiplicative inverses. Actually $3\mathbb{Z}$ is also a ring, but it has no multiplicative identity (which is ok); otherwise there is multiplication and a closed addition and so on. However, $3\mathbb{Z} + 1$ is not a ring, as it is clearly not closed under addition ($7 - 4 = 3 \notin 3\mathbb{Z} + 1$).

6.21

Find the order of all elements of $\mathbb{Z}_{12}$ under addition, all its generators, the common property they possess, and the elements of $U(12)$.

Clearly 0 has order zero. Also obviously, 1 has order 12 (you just add it 12 times). $6(2) = 12$, though, so 2 has order 6, and in fact 3 just has order 4. 4 has order 3 (as $3(4) = 12$) and 6 has order just 2. Note that 5 actually has order 12 (the set is $5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0$). Using the theorem from above, we see that 11 has order 12, 10 has order 6, 9 has order 4, 8 has order 3, and 7 has order 12. The generators are $\{1, 5, 7, 11\}$, and their common property is that they are exactly the elements of $U(12)$!

7.1(b,c)

Use the tests in the chapter to decide upon the highest power of 2 and 5 dividing 111650 and 1268904, and whether they are divisible by 3 or 9.

First off, we check the last n digits to see if a number is divisible by 2^n or 5^n. This way we see that $25|111650$ but 125 does not, and even 5 doesn't divide 1268904. On the other hand, 111650 is just even (not divisible by 4) but $8|1268904$ is the highest power. Finally, add the digits together (and reiterate, if needed) to get 111650 to become 14 to become 5 (which is divisible by neither 3 nor 9) and 1268904 to become 30 to become 3 which is not divisible by 9 but is divisible by 3.