Homework

Jon Allen

October 22, 2014

Section 3.5: #5, 15, 11 Section 3.6: #7, 20.

3.5 5. Find the cyclic subgroup of $\mathbb{C}^\times$ generated by $(\sqrt{2}+\sqrt{2}i)/2$.

$$\frac{\sqrt{2}+\sqrt{2}i}{2} = \frac{\sqrt{2}}{2}(1+i)$$

$$\left(\frac{\sqrt{2}}{2}(1+i)\right)^2 = \frac{2}{4}2i = i \qquad \left(\frac{\sqrt{2}}{2}(1+i)\right)^3 = \frac{\sqrt{2}}{2}(1+i)\,i = \frac{\sqrt{2}}{2}(i-1)$$

$$\left(\frac{\sqrt{2}}{2}(1+i)\right)^4 = i^2 = -1 \qquad \left(\frac{\sqrt{2}}{2}(1+i)\right)^5 = -\frac{\sqrt{2}}{2}(1+i)$$

$$\left(\frac{\sqrt{2}}{2}(1+i)\right)^6 = i^3 = -i \qquad \left(\frac{\sqrt{2}}{2}(1+i)\right)^7 = -\frac{\sqrt{2}}{2}(i-1) = \frac{\sqrt{2}}{2}(1-i)$$

$$\left(\frac{\sqrt{2}}{2}(1+i)\right)^8 = (-1)^2 = 1 \qquad \left(\frac{\sqrt{2}}{2}(1+i)\right)^9 = \frac{\sqrt{2}}{2}(1+i)$$

And to double check

$$\left(\frac{\sqrt{2}}{2}(1+i)\right)^{-1} = \sqrt{2}\frac{1}{1+i} \qquad \sqrt{2}\frac{1}{1+i} = \sqrt{2}\frac{1-i}{(1+i)(1-i)} = \frac{\sqrt{2}}{2}(1-i)$$

$$\left(\frac{\sqrt{2}}{2}(1+i)\right)^8 = \left(\frac{\sqrt{2}}{2}(1+i)\right)^0 \qquad \left(\frac{\sqrt{2}}{2}(1+i)\right)^7 = \left(\frac{\sqrt{2}}{2}(1+i)\right)^{-1}$$

And so the generated group is:

$$\langle(\sqrt{2}+\sqrt{2}i)/2\rangle = \{1, i, -1, -i, \frac{\sqrt{2}}{2}(1+i), i\frac{\sqrt{2}}{2}(1+i), -\frac{\sqrt{2}}{2}(1+i), -i\frac{\sqrt{2}}{2}(1+i)\}$$

11. Which of the multiplicative groups $\mathbb{Z}_7^\times, \mathbb{Z}_{10}^\times, \mathbb{Z}_{12}^\times, \mathbb{Z}_{14}^\times$ are isomorphic?
The multiplicative groups consist of powers of the elements of the original group that are relatively prime to n. The elements that aren't relatively prime can be represented as multiples of powers of relatively prime numbers and so are redundant.

$$\mathbb{Z}_7^\times = \{[2^{\alpha_1}3^{\alpha_2}4^{\alpha_3}5^{\alpha_5}6^{\alpha_5}]_7 : \alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5 \in \mathbb{Z}\}$$
$$5^6 = 25\cdot 5^4 = 4\cdot 5^4 = 20\cdot 5^3 = 6\cdot 5^3 = 30\cdot 5^2 = 2\cdot 5^2 = 10\cdot 5 = 3\cdot 5 = 15 = 1$$
$$\mathbb{Z}_7^\times = \{[\left(5^4\right)^{\alpha_1}\left(5^5\right)^{\alpha_2}\left(5^2\right)^{\alpha_3}5^{\alpha_4}\left(5^3\right)^{\alpha_5}]_7 : \alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5 \in \mathbb{Z}\} = \langle 5\rangle \cong \mathbb{Z}_6$$

$$
\begin{aligned}
\mathbb{Z}_{10}^{\times} &= \{[3^{\alpha_1}7^{\alpha_2}9^{\alpha_3}]_{10} : \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}\} \\
3^4 &= 9 \cdot 3^2 = 27 \cdot 3 = 7 \cdot 3 = 21 = 1 \\
\mathbb{Z}_{10}^{\times} &= \{[3^{\alpha_1}\left(3^3\right)^{\alpha_2}\left(3^2\right)^{\alpha_3}]_7 : \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}\} = \langle 3 \rangle \cong \mathbb{Z}_4 \\
\mathbb{Z}_{12}^{\times} &= \{5^{\alpha_1}7^{\alpha_2}11^{\alpha_3} : \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}\} \\
5^2 &= 25 = 1 \qquad 7^2 = 49 = 1 \qquad 11^2 = 121 = 1 \\
5 \cdot 7 &= 35 = 11 \qquad 7 \cdot 11 = 77 = 5 \qquad 5 \cdot 11 = 55 = 7 \\
Z_{12}^{\times} &= \{1, 5\} \times \{1, 7\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \\
Z_{14}^{\times} &= \{[3^{\alpha_1}5^{\alpha_2}9^{\alpha_3}11^{\alpha_4}13^{\alpha_5}] : \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \in \mathbb{Z}\} \\
3^6 &= 9 \cdot 3^4 = 27 \cdot 3^3 = 13 \cdot 3^3 = 39 \cdot 3^2 = 11 \cdot 3^2 = 33 \cdot 3 = 5 \cdot 3 = 15 = 1 \\
Z_{14}^{\times} &= \{[3^{\alpha_1}\left(3^5\right)^{\alpha_2}\left(3^2\right)^{\alpha_3}\left(3^4\right)^{\alpha_4}\left(3^3\right)^{\alpha_5}] : \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \in \mathbb{Z}\} = \langle 3 \rangle \cong \mathbb{Z}_6
\end{aligned}
$$

So $\mathbb{Z}_7^{\times}$ and $\mathbb{Z}_{14}^{\times}$ are isomorphic.

15. Prove that any finite cyclic group with more than two elements has at least two different generators.

Lets call our group G with generator a. So $G = \langle a \rangle$. Furthermore the order of $\langle a \rangle$ is finite, and more than two, and so $\text{ord}(\langle a \rangle) = \text{ord}(a) = n$ where $2 < n \in \mathbb{N}$. That is to say $G = \{e, a, a^2, \ldots, a^{n-1}\}$.

Now because $n > 2$ we know that $1 \neq n - 1$ and because the order of a is n we know that $a \neq a^{n-1} \neq e$. So lets see what happens if we apply the group operation $n - 1$ times to the element a^{n-1}.

$$\left(a^{n-1}\right)^{n-1} = a^{(n-1)^2} = a^{n^2-2n+1} = (a^n)^n (a^n)^{-2} a^1 = e^n e^{-2} a = a$$

And so a^{n-1} generates a and a generates G. The immediate consequence of this fact is that a^{n-1} generates G.

Note: I had some problems with this because all I have shown is that if a generates a group, then so does it's inverse, which seems kind of too obvious and maybe even the same statement. But then I considered the smallest group which fits the definition: $G = \{e, a, a^2\}$. Now $a^{-1} = a^2$ and obviously e can not generate G, so the only other possible element to generate G is a^{-1}. So that's what I went with in my proof.

3.6 7. Find the order of each element of D_6.

$$
\begin{array}{ccc}
e = e & (a^1)^6 = e & (a^2)^3 = e \\
(a^3)^2 = e & (a^4)^3 = e & (a^5)^6 = e \\
b^2 = e & (ba)^2 = (baa^{-1}b) = e &
\end{array}
$$

by assumption

$$ba^n = a^{-n}b$$

by induction

$$a^{-1}ba^n = a^{-1}a^{-n}b \qquad baa^n = ba^{n+1} = a^{-(n+1)}b$$

and then

$$(ba^n)^2 = ba^na^{-n}b = e$$

And so we have $\text{ord}(e) = 1$ (duh), $\text{ord}(a) = \text{ord}(a^5) = 6, \text{ord}(a^2) = \text{ord}(a^4) = 3$ and $\text{ord}(ba^k) = 2 \quad \forall 0 \leq k \leq 5 \in \mathbb{Z}$

20. Let the dihedral group D_n be given by elements a of order n and b of order 2, where $ba = a^{-1}b$. Find the smallest subgroup of D_n that contains a^2 and b.

    Hint: Consider two cases, depending on whether n is odd or even.

    The group specified is $\langle a^2 \rangle \times \langle b \rangle$. We know that $\text{ord}(a) = n$ and so if $k < n$ then $a^k \neq e$.

    Assume n is even. Then $(a^2)^{\frac{n}{2}} = e$ and $\forall 0 < k < \frac{n}{2}$ we know that $(a^2)^k \neq e$ and so the subgroup we are looking for consists of $\{a^{2j}b^k : 0 \leq j \leq \frac{n}{2}, 0 \leq k \leq 1 \text{ and } j, k \in \mathbb{Z}\}$

    Now lets assume n is odd. Then $n = 2k + 1$ and for all $0 < j \leq k$ we know that $a^{2j} \neq e$. And further $a^{2(k+1)} = a^{2k+1}a = a$. That is to say $\langle a^2 \rangle = \langle a \rangle$. And so it follows that the subgroup we are looking for is $\langle a \rangle \times \langle b \rangle$ which is the original group D_n.