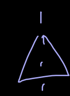
1. The group D_3 of symmetries of the triangle is isomorphic to S_3. But by Cayley's theorem, the group is also isomorphic to a *subgroup* of S_6. Find such a subgroup (using the proof of Cayley's theorem).

μ_1: 

$$D_3 = \{ \overset{1}{r_0}, \overset{2}{r_1}, \overset{3}{r_2}, \overset{4}{\mu_1}, \overset{5}{\mu_2}, \overset{6}{\mu_3} \}$$

$$r_1 \cong \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix} = \lambda_{r_1}$$

what does r_1 "do" to the elements of D_3?

$$r_1 \cdot r_2 = r_1 r_2 = r_0$$

r_1: $r_2 \mapsto r_0$

$r_0 \mapsto r_1$

$r_1 \mapsto r_2$

$\mu_1 \mapsto \mu_2$

$\mu_2 \mapsto \mu_3$

$\mu_3 \mapsto \mu_1$

	r_0	r_1	r_2	μ_1	μ_2	μ_3
r_1	r_1	r_2	r_0	μ_2	μ_3	μ_4

2. The identity can be written as $\varepsilon = (13)(24)(35)(14)(12)(15)(34)(45)$. Mimic the proof that ε must be even and show how to eliminate $x = 5$ from the product of transpositions and write ε as the product of 2 fewer transpositions in the process. Show all intermediate steps.

$(34)(45) = (345)$

$(35)(34) = (345)$

$(15)(35)$

$(35)(13)$

$(12)(35)$

$(14)(35)(12)$

$\cancel{(35)(35)}(14)(12)$

3. Suppose the group G has subnormal series

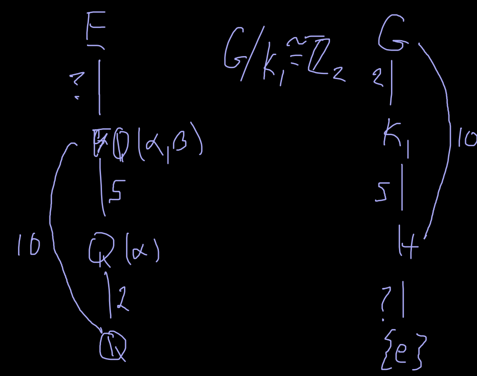
$$G \supset H \supset \{e\}$$

$G \supset K_1 \supset H \supset \{e\}$

$G \supset K_2 \supset H \supset \{e\}$

and that $G/H \cong \mathbb{Z}_{10}$. Assume also that H is simple.

(a) Explain how we know that the above series is not a composition series.



(b) Explain how we could find two different composition series for G.

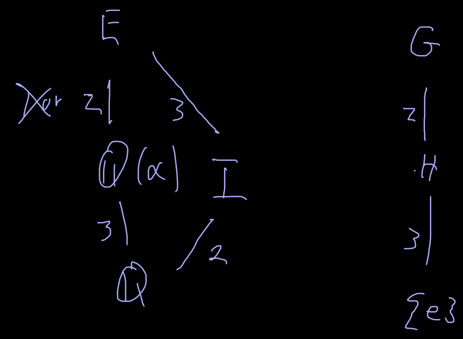
(c) Prove that if H is abelian, then G is solvable.

(d) If G happens to be the Galois group for some field E over $\mathbb{Q}$, what can you say about subfields of E?

4. Consider the polynomial $p(x) = x^3 + 5x^2 - 10x + 15$. Let E be the splitting field for $p(x)$ and G be the Galois group of E over $\mathbb{Q}$.

(a) Prove that G contains an element of order 3.

S_3 $\quad\quad$ $\mathbb{Z}_6$



(b) Prove that G contains an element of order 2.

H is normal in G

(c) Explain how we know that there is a intermediate field I strictly between $\mathbb{Q}$ and E that is the splitting field for a polynomial. What can you say about this field?

(d) Explain how you know that $G \cong S_3$ and not to $\mathbb{Z}_6$.

(e) Does the argument above prove that $p(x)$ is not solvable by radicals? Is $p(x)$ solvable by radicals?

5. Consider the number $n = 1643 = 31 \cdot 53$.

(a) What is 42^{1560} congruent to modulo 1643? Explain, using group theory. What if we replaced 42 with another number?

$42 \in U(1643)$

$\varphi(p^k) = p^k - p^{k-1}$

$\mathbb{Z}_{17}$

$\text{ord}(g) = 6$

$a^{\varphi(n)} \equiv 1 \mod n$ $\quad 42^k = 1$

for $\gcd(a,n) = 1$

$|U(1643)| = \varphi(1643)$

$= \varphi(31 \cdot 53) = \varphi(31) \cdot \varphi(53)$

$42^{1560} \equiv 1 \mod 1643$ $\quad = 30 \cdot 52 = 1560$

(b) Note that $E = 7$ is relatively prime to 1643. Find an integer D such that $(a^7)^D \equiv a \pmod{1643}$ for any a relatively prime to 1643. Explain how you know your D works.

$1 = D \cdot 7 + K \cdot \varphi(1643)$

want $7 \cdot D = K \cdot \varphi(1643) + 1$

$(a^7)^D = a^{K \cdot \varphi(1643) + 1} = (a^{\varphi(1643)})^K \cdot a^1 \equiv 1^K \cdot a^1 \mod 1643$

$D = 223$ $\quad$ since $\quad 7 \cdot 223 \equiv 1 \pmod{1560}$

6. What is the difference between an inner direct product and an external direct product? Illustrate with an example.

7. I'm thinking of an abelian group that contains elements of order 9 but not of order 27, and elements of order 2 and 5 but not of orders 4 or 25. Further, there is not other prime number p (other than 2, 3, or 5) such that there is an element of order p. Which of the following can you deduce about my group? Which must be true, which can't be true, and which might or might not be true.

   (a) There are elements of order 3.

   (b) There are elements of order 10.

   (c) The group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$.

   (d) The group is cyclic.

8. Find all abelian groups of order 480. $= 2^5 \cdot 3 \cdot 5$

$\mathbb{Z}_{2^5} \times \mathbb{Z}_3 \times \mathbb{Z}_5$ ✓ $(1,1,1)$

$\mathbb{Z}_2 \times \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \times \mathbb{Z}_5$ ✓

$\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_5$

9. Let $X = \{1, 2, 3, 4, 5, 6\}$ and $G = \{(1), (12), (345), (354), (12)(345), (12)(354)\}$. Find X_g, G_x and $\mathcal{O}_x$ for each $g \in G$ and $x \in X$. Then verify the orbit-stabilizer theorem and Burnside's theorem.

10. How many different ways could the vertices of an equilateral triangle be colored using three colors?

11. Use Burnside's theorem to explain why $\binom{7}{3} = \frac{1}{3!}P(7,3)$. That is, why are there 6 times as many ways to make three scoop ice-cream cones chosen from 7 flavors as there are to make three scoop milkshakes (cones and shakes not allowing for repeated flavors).