Math 235 (Fall 2009): Assignment 10 Solutions

1.1: $28 = 4 \cdot 7$. Since $gcd(4,7) = 1$, using the Euclidean Algorithm (or simply by guessing), we find that $1 = 4 \cdot 2 + 7 \cdot (-1)$. We define $e_1 := 1 - 4 \cdot 2 = -7$ and $e_2 := 1 - 7 \cdot (-1) = 8$.

It is easy to check (one by one) that the solutions mod 4 are $0, 1$ and 3. Similarly we check that the only solution mod 7 is 2.

Hence, by the Chinese Remainder Theorem section (in the notes), the solutions mod 28 are: $16 = 0 \cdot e_1 + 2 \cdot e_2$, $9 = 1 \cdot e_1 + 2 \cdot e_2$ and $-5 = 3 \cdot e_1 + 2 \cdot e_2$. Reducing these numbers, we get that the solutions are $16, 9$ and 23.

1.2: $36 = 4 \cdot 9$ and $1 = 4 \cdot (-2) + 9 \cdot 1$. We define $e_1 := 1 - 4 \cdot (-2) = 9$ and $e_2 := 1 - 9 \cdot 1 = -8$.

Solutions mod 4: 1 and 3.

Solutions mod 9: 0, 3 and 6.

Hence, the solutions are $1 \cdot e_1 + 0 \cdot e_2 = 9$, $3 \cdot e_1 + 0 \cdot e_2 = 27$, $1 \cdot e_1 + 3 \cdot e_2 = -15$, $3 \cdot e_1 + 3 \cdot e_2 = 3$, $1 \cdot e_1 + 6 \cdot e_2 = -39$ and $3 \cdot e_1 + 6 \cdot e_2 = -21$. Reducing these numbers, we get $9, 27, 21, 3, 33$ and 15.

1.3: $165 = 3 \cdot 5 \cdot 11$.

$1 = 3 \cdot (-18) + 55 \cdot 1$. We define $\varepsilon_1 := 1 - 3 \cdot (-18) = 55$ and $\varepsilon_2 := 1 - 55 \cdot 1 = -54$.

$1 = 5 \cdot (-2) + 11 \cdot 1$. We define $\lambda_1 := 1 - 5 \cdot (-2) = 11$ and $\lambda_2 := 1 - 11 \cdot 1 = -10$.

And then $e_1 := \varepsilon_1 = 55$, $e_2 := \varepsilon_2 \cdot \lambda_1 = -594$ and $e_3 = \varepsilon_2 \cdot \lambda_2 = 540$. In fact, these numbers can be reduced mod 165 (why?) to obtain: $e_1 := 55$, $e_2 := 66$ and $e_3 := 45$.

Solutions mod 3: 1 and 2.

Solutions mod 5: 2 and 3.

Solutions mod 11: 5 and 6.

Hence, the solutions are $a \cdot e_1 + b \cdot e_2 + c \cdot e_3$ for every $a \in \{1, 2\}$, $b \in \{2, 3\}$ and $c \in \{5, 6\}$. After reducing them, we get: $17, 28, 38, 82, 83, 127, 137$ and 148.

Exercises from the notes:

1.a: One can check that $\tau^2 = (13829)$.

$\tau^2\sigma = (19)(286)(34)$.

$\sigma\tau^2\sigma = (19263)$ and, hence, its order is 5.

1.b: $\sigma\tau = (172345)$.

$\sigma\tau\sigma\tau = (\sigma\tau)^2 = (124)(735)$ and, hence, its order is $lcm(3,3) = 3$.

1.c: Call $\mu = \sigma^{-1} = (987654321)$.

Then $\sigma^{-1}\tau\sigma = \mu(12)(345)(6789)\mu^{-1} = \mu(12)\mu^{-1}\mu(345)\mu^{-1}\mu(6789)\mu^{-1}$.

But $\mu(12)\mu^{-1} = (\mu(1)\ \mu(2))$ (why?). Hence, $\mu(12)\mu^{-1} = (91)$.

Similarly, $\mu(345)\mu^{-1} = (\mu(3)\ \mu(4)\ \mu(5)) = (234)$ and $\mu(6789)\mu^{-1} = (5678)$.

Thus, $\sigma^{-1}\tau\sigma = (91)(234)(5678)$ and its order is $lcm(2,3,4) = 12$.

1.d: Again, let $\mu = \sigma^{-1} = (987654321)$.

$\sigma^{-1}\tau\sigma = \mu\tau\mu^{-1}$.
$\mu(12345)\mu^{-1} = (91234)$ and $\mu(6789)\mu^{-1} = (5678)$.
Therefore, $\sigma^{-1}\tau\sigma = (91234)(5678)$ and its order is $lcm(5,4) = 20$.

2: (b) is not a group because $(1243)^{-1}$ is not in the set.
(d) is not a group because it has 5 elements and $5 \nmid 4! = |S_4|$ (see Lagrange's theorem).
(a) and (c) are subgroups.

3.a: Simple verification.

3.b.i:

S_3	id	(12)	(13)	(23)	(123)	(132)
id	id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	id	(132)	(123)	(23)	(13)
(13)	(13)	(123)	id	(132)	(12)	(23)
(23)	(23)	(132)	(123)	id	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	id
(132)	(132)	(23)	(12)	(13)	id	(123)

D_4	1	y	y^2	y^3	x	yx	y^2x	y^3x
1	1	y	y^2	y^3	x	yx	y^2x	y^3x
y	y	y^2	y^3	1	yx	y^2x	y^3x	x
y^2	y^2	y^3	1	y	y^2x	y^3x	x	yx
y^3	y^3	1	y	y^2	y^3x	x	yx	y^2x
x	x	y^3x	y^2x	yx	1	y^3	y^2	y
yx	yx	x	y^3x	y^2x	y	1	y^3	y^2
y^2x	y^2x	yx	x	y^3x	y^2	y	1	y^3
y^3x	y^3x	y^2x	yx	x	y^3	y^2	y	1

Q_8	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

3.b.ii:

S_3

id	1
(12)	2
(13)	2
(23)	2
(123)	3
(132)	3

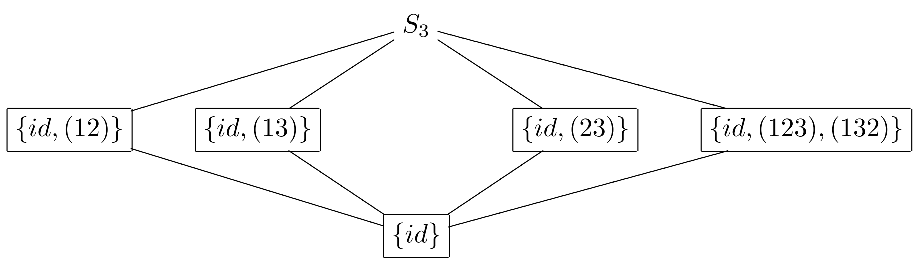
D_4

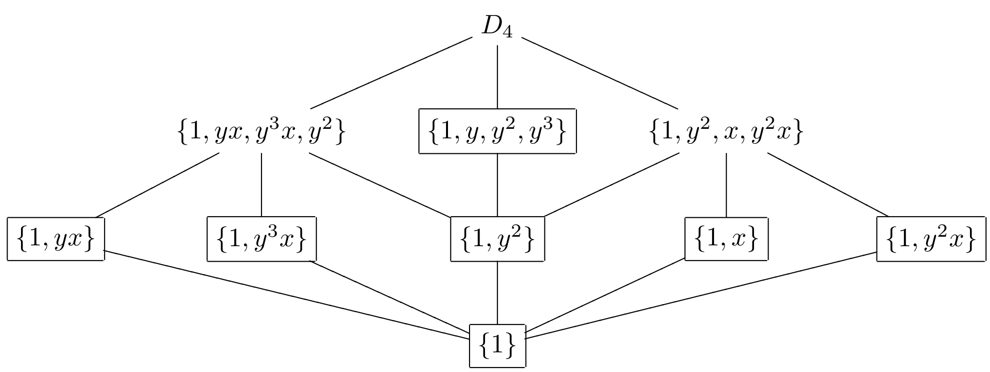
1	1
y	4
y^2	2
y^3	4
x	2
yx	2
y^2x	2
y^3x	2

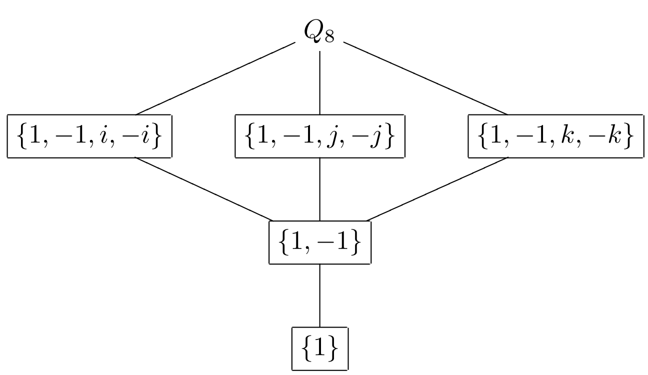
Q_8

1	1
-1	1
i	4
$-i$	4
j	4
$-j$	4
k	4
$-k$	4

3.b.iii: The cyclic groups are the framed ones.







4.a: $\sigma = (1352)(4678)$ and its order is $lcm(4, 4) = 4$.

4.b: The order of (1 2 3)(4 5 6 7)(8 9 10 11 12) is $lcm(3, 4, 5) = 60$.

Let us see that there are no elements of order larger than 60. We know that if $\tau = \alpha_1 ... \alpha_k$ is a product of disjoint cycles of length $r_1, ..., r_k$ then the order of τ is $lcm(r_1, ...r_k)$. Since the cycles are disjoint, $r_1 + ... + r_k \leqslant 12$. Each $2 \leqq r_i \leqslant 12$.

Since we are only interested in the order, we may assume the r_i are all distinct (why?). So, we may also assume $r_1 > ... > r_k$.

Now we can show there is no element of order larger than 60 by checking each case: $r_1 = 12$, $r_1 = 11$, ..., $r_1 = 2$.

We may speed up the process by using the following: we may discard r_i satisfying $r_i | r_j$ for some $j \geqslant i$ (why?).

8: We know every element of S_n is a product of (disjoint) cycles. Hence, it is enough to prove that every cycle is a product of transpositions. One can easily check that $(a_1 a_2 ... a_{n-1} a_n) = (a_1 a_n)(a_1 a_{n-1}) ... (a_1 a_2)$.