Eric Willard
CS 5602 Intro to Cryptography
Prelim 2

Problem 7

1) List generators of C9: {1, 2, 4, 5, 7, 8} which are all elements coprime to 9. In the other groups of order 9, all non-identity elements must have order 3 because 3 is the only factor of 9.

2) Let G be a group of order 9 that does not equal C_9. Since G is not cyclic $\exists a \in G$ s.t. order(a) = 3 and a generates $\{1,\ a,\ a^2\} \in G$. Picking $b \in G-\{1,\ a,\ a^2\}$ gives $\{b,\ b^2\}$. $\{1,\ a,\ a^2\}$ and $\{b,\ b^2\}$ cannot have any elements in common because b cannot be equivalent to $1, a$ and a^2 because that would imply $b \in \{1,\ a,\ a^2\}$ but $b \in G-\{1,\ a,\ a^2\}$.

3) $\{1,\ a,\ a^2,\ b,\ b^2\}$ are all distinct from above. What remains is to show $\{ab,\ a^2b,\ ab^2,\ a^2b^2\}$ are distinct from every other value.

ab:
$ab \neq 1$ because that implies $b = a^{-1}$
$ab \neq a$ because that implies $b = 1$
$ab \neq b$ because that implies $a = 1$
$ab \neq a^2$ because that implies $b = a$
$ab \neq b^2$ because that implies $a = b$
$ab \neq a^2b$ because that implies $a = a^2$ $or\ b = ab$
$ab \neq ab^2$ because that implies $b = b^2$ $or\ a = ab$
$ab \neq a^2b^2$ because that implies $b = b^2$ $and\ a = a^2$ or $a = a^2b$ or $b = ab^2$

a^2b:
$a^2b \neq 1$ because that implies $b = (a^2)^{-1}$
$a^2b \neq a$ because that implies $b = a^2$
$a^2b \neq b$ because that implies $a^2 = 1$
$a^2b \neq a^2$ because that implies $b = 1$
$a^2b \neq b^2$ because that implies $b = ab^2$
$a^2b \neq ab$ because that implies $a = a^2$
$a^2b \neq ab^2$ because that implies $b = a^2b^2$
$a^2b \neq a^2b^2$ because that implies $b = b^2$

ab^2 :

$ab^2 \neq 1$ because that implies $b^2 = (a)^{-1}$

$ab^2 \neq a$ because that implies $b^2 = 1$

$ab^2 \neq b$ because that implies $a = b^2$

$ab^2 \neq a^2$ because that implies $b^2 = a$

$ab^2 \neq b^2$ because that implies $a = 1$

$ab^2 \neq ab$ because that implies $a = ab^2$

$ab^2 \neq a^2b$ because that implies $a = a^2b^2$

$ab^2 \neq a^2b^2$ because that implies $a = a^2$

a^2b^2 :

$a^2b^2 \neq 1$ because that implies $b^2 = (a^2)^{-1}$

$a^2b^2 \neq a$ because that implies $b^2 = 1$

$a^2b^2 \neq b$ because that implies $a = b$

$a^2b^2 \neq a^2$ because that implies $b^2 = 1$

$a^2b^2 \neq b^2$ because that implies $a^2 = 1$

$a^2b^2 \neq ab$ because that implies $a^2 = a \text{ and } b^2 = b$

$a^2b^2 \neq a^2b$ because that implies $a^2 = a^2b^2$

$a^2b^2 \neq ab^2$ because that implies $b^2 = a^2b^2$

4) What is ba?

$ba \neq 1$ because that implies $a = b^{-1}$

$ba \neq a$ because that implies $b = 1$

$ba \neq b$ because that implies $a = 1$

$ba \neq a^2$ because that implies $b = a$

$ba \neq b^2$ because that implies $a = b$

So $ba \in \{ab,\ a^2b,\ ab^2,\ a^2,\ b^2\}$

5) If G_1 and G_2 are groups, then $G_1 \times G_2 = (g_1, g_2)$ is also a group. $H = (G_1 \times G_2$, *)

(1) H is closed because (a,b)*(c,d) = (ac, bd) and $ac \in G_1 \text{ and } bd \in G_2$

(2) * is associative on G_1 and G_2 so it associative on H

(3) $\exists g_1^{-1} \in G_1 \text{ and } \exists g_2^{-1} \in G_2$ s.t. $\exists (g_1^{-1}, g_2^{-1})$ s.t. $(g_1, g_2) * (g_1^{-1}, g_2^{-1}) = (1, 1)$

(4) $(1_{G_1}, 1_{G_2}) = (1, 1)$ is the identity

6) $G_1 = \{1, a, a^2\}$ and $G_2 = \{1, b, b^2\}$

$G_1 \times G_2$	**1**	b	b^2
1	(1,1)	(1, b)	(1, b^2)
a	(a,1)	(a, b)	(a, b^2)
a^2	(a^2,1)	(a^2, b)	(a^2, b^2)

The elements of the table are the elements of G. This shows that G can be formed by the cross product of two smaller groups. Since G is the cross product of two arbitrary groups G_1 and G_2 then no matter which order the cross product is applied, you will still get G. That shows that $ba = ab$, so G is abelian.

7)
Cayley Table assuming $ba = a^2b$
Initial Table:

	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
1	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
a	a	a^2	1	ab	ab^2	a^2b	b	a^2b^2	b^2
a^2	a^2	1	a	a^2b	a^2b^2	b	ab	b^2	ab^2
b	b			b^2	1				
b^2	b^2			1	b				
ab	ab			ab^2	a				
a^2b	a^2b			a^2b^2	a^2				
ab^2	ab^2			a	ab				
a^2b^2	a^2b^2			a^2	a^2b				

Calcuations:

ba=aab
baa =aaba=aaaab
bab=aabb
baab=aabab=aaaabb
babb=aabbb
baabb=aababb=aaaabbb

bba=baab=aabab=aaaabb=abb
bbaa=baaba=aabaaab=aaaabaab=abaab=aaabab=aaaaabb=aabb
bbab=baabb=aababb=aaaabbb=abbb
bbaab=baabab=aabaaabb=aaaabaabb=abaabb=aaababb=aaaaabbb=aabbb
bbabb=baabbb=aababbb=aaaabbbb=abbbb
bbaabb=baababb=aabaaabbb=aaaabaabbb=abaabbb=aaababbb=aaaaabbbb=aabbbb

aba=aaab
abaa =aaaba=aaaaab
abab=aaabb
abaab=aaabab=aaaaabb
ababb=aaabbb
abaabb=aaababb=aaaaabbb

aaba=aaaab
aabaa =aaaaba=aaaaaab
aabab=aaaabb
aabaab=aaaabab=aaaaaabb
aababb=aaaabbb
aabaabb=aaaababb=aaaaaabbb

abba=abaab=aaabab=aaaaabb=aabb
abbaa=abaaba=aaabaaab=aaaaabaab=aabaab=aaaabab=aaaaaabb=aaabb
abbab=abaabb=aaababb=aaaaabbb=aabbb
abbaab=abaabab=aaabaaabb=aaaaabaabb=aabaabb=aaaababb=aaaaaabbb=aaabbb
abbabb=abaabbb=aaababbb=aaaaabbbb=aabbbb
abbaabb=abaababb=aaabaaabbb=aaaaabaabbb=aabaabbb=aaaababbb=aaaaaabbbb=aaabbb
b

Final Table:

	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
1	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
a	a	a^2	1	ab	ab^2	a^2b	b	a^2b^2	b^2
a^2	a^2	1	a	a^2b	a^2b^2	b	ab	b^2	ab^2
b	b	a^2b	ab	b^2	1	a^2b^2	ab^2	a^2	a
b^2	b^2	ab^2	a^2b^2	1	b	a	a^2	ab	a^2b
ab	ab	b	a^2b	ab^2	a	b^2	a^2b^2	1	a^2
a^2b	a^2b	ab	b	a^2b^2	a^2	ab^2	b^2	a	1
ab^2	ab^2	a^2b^2	b^2	a	ab	a^2	1	a^2b	b
a^2b^2	a^2b^2	b^2	ab^2	a^2	a^2b	1	a	b	ab

Counterexample to being associative:

$(b^2 * ab^2) * ab = ab * ab = b^2$

$b^2 * (ab^2 * ab) = b^2a^2 = a^2b^2$

The above two results are different so the Cayley Table is not associative.

8)

Cayley Table assuming $ba = ab^2$

Initial Table:

	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
1	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
a	a	a^2	1	ab	ab^2	a^2b	b	a^2b^2	b^2
a^2	a^2	1	a	a^2b	a^2b^2	b	ab	b^2	ab^2
b	b			b^2	1				
b^2	b^2			1	b				
ab	ab			ab^2	a				
a^2b	a^2b			a^2b^2	a^2				
ab^2	ab^2			a	ab				
a^2b^2	a^2b^2			a^2	a^2b				

Calculations:

baa = abba=ababb=aabbbb=aab
bab=abbb=a
baab=abbab=ababbb=aabbbbb=aabb
babb=abbbb=ab
baabb=abbabb =ababbbb=aabbbbbb=aa

aba=aabb
abaa =aabba=aababb=aaabbbb=aaab
abbb=a
abab=aabbb=aa
abaab=aabbab=aababbb=aaabbbbb=aaabb
ababb=aabbbb=aab
abaabb=aabbabb =aababbbb=aaabbbbbb=aaa

aaba=aaabb
aabaa =aaabba=aaababb=aaaabbbb=aaaab
aabbb=aa
aabab=aabbb=aaa
aabaab=aaabbab=aaababbb=aaaabbbbb=aaaabb

aababb=aaabbbb=aaab
aabaabb=aaabbabb =aaababbbb=aaaabbbbbb=aaaa

bba=babb=abbbb
bbaa=babba=abbbabb=abbabbbb=ababbbbbb=aabbbbbbbb=aabb
bbab=babbb=abbbbb
bbabb=babbbb=abbbbbb
bbaab=babbab=abbbabb=abbabbbbb=ababbbbbbb=aabbbbbbbbb=aabbb

abba=ababb=aabbbb
abbaa=ababba=aabbbabb=aabbabbbb=aababbbbbb=aaabbbbbbbb=aaabb
abbab=ababbb=aabbbbb
abbabb=ababbbb=aabbbbbb
abbaab=ababbab=aabbbabb=aabbabbbbb=aababbbbbbb=aaabbbbbbbbb=aaabbb

Finished table:

	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
1	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
a	a	a^2	1	ab	ab^2	a^2b	b	a^2b^2	b^2
a^2	a^2	1	a	a^2b	a^2b^2	b	ab	b^2	ab^2
b	b	ab^2	a^2b	b^2	1	a	a^2b^2	ab	a^2
b^2	b^2	ab	a^2b^2	1	b	ab^2	a^2	a	a^2b
ab	ab	a^2b^2	b	ab^2	a	a^2	b^2	a^2b	1
a^2b	a^2b	b^2	ab	a^2b^2	a^2	1	ab^2	b	a
ab^2	ab^2	a^2b	b^2	a	ab	a^2b^2	1	a^2	b
a^2b^2	a^2b^2	b	ab^2	a^2	a^2b	b^2	a	1	ab

Counterexample to being associative:
$(b^2 * a^2b) * ab = a^2 * ab = b$
$b^2 * (a^2b * ab) = b^2 * 1 = b^2$
The above two results are different so the Cayley Table is not associative.

9)

Cayley Table assuming $ba = a^2b^2$

Initial Table:

	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
1	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
a	a	a^2	1	ab	ab^2	a^2b	b	a^2b^2	b^2
a^2	a^2	1	a	a^2b	a^2b^2	b	ab	b^2	ab^2
b	b			b^2	1				
b^2	b^2			1	b				
ab	ab			ab^2	a				
a^2b	a^2b			a^2b^2	a^2				
ab^2	ab^2			a	ab				
a^2b^2	a^2b^2			a^2	a^2b				

Calculations:

ba=aabb

baa=aabba=aabaabb=aaaaabbabb=aabbabb=aabaabbbb=aaaabbabbbb=abbab=abaabb=aaabbabb=baabbbb=aabbab=aabaabb=...

Trying to get rid of ba in ba^2 seems to get stuck in a loop.

I think it gets stuck here because if $ba = a^2b^2$ that would mean $b = a^2$ $and\ a = b^2$ which is not possible.

10) From work above it can be seen that there are only two groups of order 9, and that they are abelian. These groups would be C_9 and $C_3 \times C_3$.