CISS451: Cryptography and Computer Security
Assignment 4

Objectives

1. Use group axioms
2. Write a complete proof for a fact regarding groups
3. Construct groups when given a size

Make sure you read the comments before Q1 very carefully before hacking proofs.

Basic math writing

If you have a sequence of deductions where the left-hand-side is the same, you can write this:

$$\begin{aligned} & x = 1+2+3+4+5 \\ \therefore\ & x = 3+3+4+5 \\ \therefore\ & x = 6+4+5 \end{aligned}$$

Of course this is a shorthand for saying "x is $1+2+3+4+5$. Therefore x is $3+3+4+5$. Therefore x is $6+4+5$." It's "proper math" (just like "proper English") to write

$$\begin{aligned} x &= 1+2+3+4+5 \\ &= 3+3+4+5 \\ &= 6+4+5 \end{aligned}$$

Because that's the same as saying "x is $1+2+3+4+5$, *which is* $3+3+4+5$, *which is* $6+4+5$." When you need to change the left-hand side, you would write

$$\begin{aligned} x &= 1+2+3+4+5 \\ &= 3+3+4+5 \\ &= 6+4+5 \\ \therefore\ x+1 &= 6+4+5+1 \\ &= 10+5+1 \end{aligned}$$

Or you can use words:

$$\begin{aligned} x &= 1+2+3+4+5 \\ &= 3+3+4+5 \\ &= 6+4+5 \end{aligned}$$

and therefore

$$\begin{aligned} x+1 &= 6+4+5+1 \\ &= 10+5+1 \end{aligned}$$

When a sequence of deductions is not computational like the above, it might be better not to write in the above form in a math paragraph form, but rather in a text paragraph form:

Since x is $6+4+5$, adding 1, we get $x+1$ is $6+4+5+1$.

This form of writing is best when you are not doing computations. This is especially true when you have "for all" and "there exists" quantifiers in your argument. You can of course mix text paragraph form and math paragraph form. For instance:

For all x and y in $\mathbb{R}$ with $x > 0$ and $y > 0$, there is some integer n such that

$$\begin{aligned} & nx > y \\ \therefore \quad & n > y/x \end{aligned}$$

Frequently you need to justify an argument. For instance:

By the neutral axiom,

$$xy = (xy)e$$

Therefore by the associativity axiom

$$xy = x(ye)$$

Or you can do it this way:

$$\begin{aligned} xy &= (xy)e && \text{by the neutrality axiom} \\ &= x(ye) && \text{by the associativty axiom} \end{aligned}$$

(This style is for classroom use. Most books/research papers actually prefer the previous style.) Of course besides quoting axioms, you can also quote assumptions, theorems, etc.

$$\begin{aligned} xy &= (xy)e && \text{by the neutrality axiom} \\ &= x(ye) && \text{by the associativty axiom} \\ &= x(y(wz)) && \text{by Theorem 42} \end{aligned}$$

Do not start your proof abruptly. You for example reference a given assumption:

Since $x > 0$, we have

$$\begin{aligned} & \sqrt{x} > 0 \\ \therefore \quad & \sqrt{x} + 1 > 1 \\ \therefore \quad & \frac{\sqrt{x}+1}{x} > \frac{1}{x} \end{aligned}$$

Compare this to without the "Since ...":

$$\begin{aligned} & \sqrt{x} > 0 \\ \therefore \quad & \sqrt{x} + 1 > 1 \\ \therefore \quad & \frac{\sqrt{x}+1}{x} > \frac{1}{x} \end{aligned}$$

you'll see that the second version is very abrupt.

Writing proof by induction

For proof by induction, state clearly your $P(n)$. When you are proving the base case, say you are proving the base case. When you are proving the inductive case, say you are proving the inductive case. When you are done with the inductive case, say you are done. When you are completely done, say so and make a recap. That's called good writing: lead the reader. Read a proof by induction from any textbook (or on the web). Here's a standard example.

Prove that $1 + 2 + \cdots + n = n(n + 1)/2$.

We will prove the above by mathematical induction. (That's called leading the reader.) Let $P(n)$ be the statement:

$$P(n) : 1 + 2 + \cdots + n = n(n + 1)/2$$

for $n \geq 1$.

We will first prove the base case. When $n = 1$,

$$1 + \cdots + n = 1$$

and

$$n(n + 1)/2 = 1(1 + 1)/2 = 1$$

Hence the base case $P(1)$ holds.

Next, we will prove the inductive case. Assume that $P(n)$ holds, i.e.,

$$1 + 2 + \cdots + n = \frac{n(n + 1)}{2}$$

Therefore we have the following:

$$\begin{aligned} 1 + 2 + \cdots + n + (n + 1) &= \frac{n(n + 1)}{2} + (n + 1) \\ &= (n + 1)\left(\frac{n}{2} + 1\right) \\ &= (n + 1)\left(\frac{n + 2}{2}\right) \\ &= \frac{(n + 1)((n + 1) + 1)}{2} \end{aligned}$$

Therefore $P(n + 1)$ holds and hence the inductive case holds.

Therefore by the principle of (weak) mathematical induction, $P(n)$ holds for all $n \geq 1$, i.e.,

$$1 + 2 + \cdots + n = \frac{n(n + 1)}{2}$$

holds for all $n \geq 1$. □

Read the above proof carefully several times. Then write your own version – and compare it with the above.

When an argument is long, note how I state what I'm going to prove and after the argument is complete, I remind the reader the goal.

Note also that in the above, there's one main argument. But there are two sub-arguments: the base case and the inductive case arguments. That structure (just like the structure in a piece of code) has to be clear:

> We will prove the above by mathematical induction. ...
>
> > We will first prove the base case. ...
> > Hence the base case $P(1)$ holds.
> >
> > Next, we will prove the inductive case. ...
> > Therefore $P(n+1)$ holds and hence the inductive case holds.
>
> Therefore by the principle of (weak) mathematical induction, $P(n)$ holds for all $n \geq 1$, i.e.,
>
> $$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$
>
> holds for all $n \geq 1$.

A well written proof has no holes (gaps), no errors, *and reads well*. Think of you standing in front of a judge and jury defending your case: you are the butlet but you did not do it. The point is not whether *you* believe yourself. Of course you do. But rather, can you make the *judge and jury* believe you?

After you are done, read your proof again. Even if there are no errors, can it be improved? Can it be shortened? Can it be written clearer? Or can you reach the same conclusion by a different and better route?

Quoting/referencing axioms etc

Call the group axioms by these names:

- Closure axiom
- Associativity axiom
- Inverse axiom
- Neutrality axiom

We have three tiny propositions in the notes. Call them

- Uniqueness of identity
- Uniqueness of inverse
- Cancellation property

You can reference these in a text paragraph such as:

By the associativity axiom, from $x * (x * y) = z$, we get $(x * x) * y = z$.

Or in a math paragraph:

$$\begin{aligned} & x * (x * y) = z \\ \therefore \quad & (x * x) * y = z && \text{by associativity axiom} \end{aligned}$$

Q1. Let $f : G \to G'$ be an isomophism of group $(G, *, e)$ and $(G', *', e')$. Prove the following

(a) $f(e) = e'$
(b) If $x \in G$, then $f(x^{-1}) = f(x)^{-1}$. (Make sure you read those two $^{-1}$ very carefully!)
(c) If $x \in G$, then $f(x^n) = f(x)^n$ for all integer n. (Hint: First prove this is true for $n \geq 0$ – use induction.)
(d) If G is abelian, then G' is also abelian.

Besides (d), most of the algebraic facts of G would correspond to the same algebraic facts in G' since they are isomorphic. For instance if G has exactly 10 elements of order 5, then G' also has exactly 10 elements of order 5 and if G is a cyclic group of order 12, then G' is also a cyclic group of order 12, etc.

(By the way, it should be clear that $f(f^{-1}(x)) = x$ and $f^{-1}(f(y)) = y$. That has nothing to do with group theory. That's just a fact about inverse functions.)

SOLUTION.

(a) Goal: Show $f(e) = e'$

$$\begin{aligned} f(e) &= f(e * e) && \text{by the identity property of e} \\ &= f(e) *' f(e) && \text{by the definition of group isomorphism} \end{aligned}$$

and

$$\begin{aligned} f(e) &= f(e) *' e' && \text{by neutrality axiom in G'} \\ f(e) *' f(e) &= f(e) *' e' \\ f(e) &= e' && \text{by the cancellation property} \end{aligned}$$

(b) Goal: show $f(x^{-1}) = f(x)^{-1}$

Let $x \in G$

$$\begin{aligned} f(x * x^{-1}) &= f(e) && \text{Since } x * x^{-1} = e \text{ by the inverse axiom} \\ f(x * x^{-1}) &= e' && \text{by part (a)} \\ & \text{then} \\ f(x) * f(x^{-1}) &= e \\ f(x^{-1}) &= f(x)^{-1} * e \end{aligned}$$

Therefore, $f(x^{-1}) = f(x)^{-1}$

(c) Goal: Show an inverse is ... inversible?

I will prove this via mathematical induction.
First, I will show that if $x \in G$, then $f(x^n) = f(x)^n$ for all integer n where $n \geq 0$

If $n = 0$, we define $f(x^0) = 1 = f(x)^0$
If $n = 1$, we define $f(x^1) = x = f(x)^1$

Thus, our $P(0)$ case for positive integers is
$P(0) = f(x^2) = f(x * x) = f(x) * f(x) = f(x)^2$
Therefore, $P(0)$ holds for $n = 2$.

Assume $P(k)$ is true. That is, $P(k) = f(x^n) = f(x)^n$ for all $x \geq 0$

Now, I will show $P(k+1)$ to be true

$$\begin{aligned} f(x^{k+1}) &= f(x^k x) \\ &= f(x^k) * f(x) \\ &= f(x)^k * f(x) && \text{by the inductive hypothesis} \\ &= f(x)^{k+1} \end{aligned}$$

Now I must show $f(x^n) = f(x)^n$ when $x < 0$

We can write n as $-m$, and thus "pretend" $m > 0$

$$\begin{aligned} f(x^n) &= f(x^{-m}) \\ &= f((x^{-1})^m) \\ &= f(x)^{-m} && \text{by part (b)} \\ &= f(x)^n && \text{because } n = -m \end{aligned}$$

(d) Goal: Show that if G is abelian, then G' is also abelian

If G is abelian, and because f is an isomorphism, we can say $\forall\ x, y \in G$, $\exists\ a, b \in G'$ such that
$a = f(x)$ and $b = f(y)$. Hence
$a * b = f(x) * f(y) = f(x * y) = f(y * x) = f(y) * f(x) = b * a$
Thus, if G is abelian, G' is too.

Q2. In the following, let $(G, *, e)$, $(G', *', e')$, and $(G'', *'', e'')$ be groups.

(a) Let $\mathrm{id}_G : G \to G$ be the identity function $\mathrm{id}(x) = x$. Prove that id is a group isomorphism.
(b) Let $f : G \to G'$ be a group isomorphism. Since f is a bijection, it has an inverse function $f^{-1} : G' \to G$. Prove that f^{-1} is also a group isomorphism.
(c) Suppose $f : G \to G'$ and $f' : G' \to G''$ are group isomorphisms. Prove that the composition of function $f' \circ f : G \to G''$ is also a group isomorphism.

The above says that the concept of group isomorphism is a an equivalence relation on the collection of all groups: if G, G', G'' are groups, then

- Reflexive: $G \simeq G$
- Symmetric: $G \simeq G' \implies G' \simeq G$
- Transitive: $G \simeq G', G' \simeq G'' \implies G \simeq G''$

SOLUTION.

(a)

(b)

(c)

Q3. If $(G, *, e)$ and $(G', *', e')$ are groups, then you can define $G'' = G \times G'$ (cartesian product) as the set of tuples (x, x') where $x \in G$ and $x' \in G$, and you can also define $*''$ by

$$(x, x') *'' (y, y') = (x * y, x' *' y')$$

Let $e'' = (e, e') \in G \times G'$.

(a) Prove that $(G'', *'', e'')$ is a group. (Make sure you state clearly what is the inverse $(x, y)^{-1}$ of (x, y) in $G \times G' = G''$.)
(b) Prove that if G and G' are abelian, then G'' is also abelian.
(c) Prove that $G \times \{e'\}$ is a subgroup of G'' which is isomorphic to G. Make sure you state the isomorphism function and then prove that it is a group isomorphism. You can and should think of $G \times \{e'\}$ as an isomorphic copy of G inside G''. (Note that the intersection of $G \times \{e'\}$ and $\{e\} \times G'$ is the simplest possible subgroup, i.e., $\{(e, e')\}$.)
(d) Is $\mathbb{Z}/6$ isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/3$? Why?
(e) Is $\mathbb{Z}/4$ isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$? Why?

The above says that

- The cartesian product of groups is a group.
- The product of abelian groups is abelian.
- The product of G, G' contains isomorphic copies of G and G'.

The concept is somewhat similar to the fact that the x– and y–axis (two $\mathbb{R}$'s) appears inside (i.e., $\mathbb{R}^2$) and their intersection is $\{(0, 0)\}$. The group product allows you to create more groups. Furthermore the group product can be easily understood if you know everything about the individual component groups. For instance since $\mathbb{Z}/2$ is a group (under $+$), you immediately have the group $\mathbb{Z}/2 \times \mathbb{Z}/2$, $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$, etc.

SOLUTION.

(a)

(b)

(c)

(d)

(e)

Q4. Recall that S_n is the symmetric group on n symbols, i.e., S_n is the set of bijections $\{1, ..., n\} \to \{1, ..., n\}$. Each element of S_n can be thought of as a permutation of $\{1, ..., n\}$. Recall that the bijection on $\{1, 2, 3, 4, 5, 6\}$

$$\begin{aligned} 1 &\mapsto 3 \\ 2 &\mapsto 1 \\ 3 &\mapsto 2 \\ 4 &\mapsto 6 \\ 5 &\mapsto 5 \\ 6 &\mapsto 4 \end{aligned}$$

can be written using permutation notation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix}$$

or cycle notation

$$\sigma = (1\ 3\ 2)(4\ 6)(5)$$

The above is an element of S_6. Note that it's clear that $|S_6| = 6!$. Of course you can compose bijections os S_n since they are functions. For instance suppose I pick $\sigma = (1)(2\ 3\ 4)$ and $\tau = (1\ 2)(3\ 4)$ in S_4. Then

$$\begin{aligned} (\tau \circ \sigma)(1) &= \tau(\sigma(1)) = \tau(1) = 2 \\ (\tau \circ \sigma)(2) &= \tau(\sigma(2)) = \tau(3) = 4 \end{aligned}$$

etc. and of course $\tau \circ \sigma \in S_4$. Define the identity function id_n of S_n by $\mathrm{id}_n(i) = i$ for all $i \in \{1, ..., n\}$. Then $(S_n, \circ, \mathrm{id}_n)$ is a group (this is easy to prove – I'll just let you think about it.)

(a) Draw the group table of S_3. (Note that $|S_3| = 3! = 6$.)
(b) Is S_3 abelian?
(c) What is the size of the largest cyclic subgroup of S_3? (For $\sigma \in S_3$, compute the order of σ, i.e., the smallest k such that $\sigma^k = (1)(2)(3)$. What is the largest possible k for all $\sigma \in S_3$?).
(d) What is the size of the largest cyclic subgroup of S_5?
(e) Is S_n abelian if $n > 3$? (I hope it's obvious that $S_1 = C_1 = \mathbb{Z}/1$ and $S_2 = C_2 = \mathbb{Z}/2$ and are therefore dead easy.)

SOLUTION.

(a)

$\circ$	(1)(2)(3)	(1 2)(3)	(1 3)(2)	(1)(2 3)	(1 2 3)	(1 3 2)
(1)(2)(3)						
(1 2)(3)						
(1 3)(2)						
(1)(2 3)						
(1 2 3)						
(1 3 2)						

(b)

(c)

(d)

(e)

Q5. Find all non-isomorphic groups of size 6. First do a complete listing of all possible group tables. Narrow it down so that isomorphic ones are identified. For the remaining non-isomorphic groups, make them concrete by recognizing them as the standard groups mentioned in the notes: $\mathbb{Z}/N$, matrix groups, permutation/symmetric groups, etc.

SOLUTION.

(I'll do the first few steps for you.)

Let $G = \{e, A, B, C, D, E\}$ be a group of size 6. (Therefore all the symbols e, A, B, C, D, E are distinct.) where e is the identity element. We have to complete the following group table:

$*$	e	A	B	C	D	E
e						
A						
B						
C						
D						
E						

Since e is the identity element we have

$*$	e	A	B	C	D	E
e	e	A	B	C	D	E
A	A					
B	B					
C	C					
D	D					
E	E					

AA can be e, B, C, D, or E.

Case 1: $AA = e$.

$*$	e	A	B	C	D	E
e	e	A	B	C	D	E
A	A	e				
B	B					
C	C					
D	D					

E	E					

AB can be C, D, E.

Case 1.1: $AA = e, AB = C$.

$*$	e	A	B	C	D	E
e	e	A	B	C	D	E
A	A	e	C			
B	B					
C	C					
D	D					
E	E					

It seems that AC can be B, D, or E (3 choices). But in fact from $AB = C$, we get

$$
\begin{aligned}
& A(AB) = AC && \\
\therefore\ & (AA)B = AC && \text{by associativity axiom} \\
\therefore\ & eB = AC && \text{since } AA = e \\
\therefore\ & B = AC && \text{by neutrality axiom}
\end{aligned}
$$

Therefore there is only one choice for AC, i.e., $AC = B$. Hence

$*$	e	A	B	C	D	E
e	e	A	B	C	D	E
A	A	e	C	B		
B	B					
C	C					
D	D					
E	E					

(Pro tip: Don't just brute force and try all possible options. Use the algebraic relations as much as possible to cut down on the number of cases to examine. Also, keep the cases organized so that you can iterate over all of them without missing any.)