EIDMA

Lecture 7

- *mod n* operations cont.
- Groups
- *inf* and *sup* of a poset
- Order preserving functions

From last week:

Prove

(1) $(\forall p)\ ((p\ mod\ n)\ mod\ n = p\ mod\ n\ )$ and

(2) $(\forall p, q)\ (\ (p+q) mod\ n\ =\ (p\ mod\ n\ +\ q\ mod\ n) mod\ n\ )$.

Part (1) is obvious.

Part (2). Suppose $p\ (mod\ n) = r_p$ and $q\ (mod\ n) = r_q$ that is, for some k_p, k_q we have $p = k_p n + r_p$ and $q = k_q n + r_q$ with $0 \le r_p, r_q < n$. Now, $(p+q) mod\ n = \left(k_p n + r_p + k_q n + r_q\right) mod\ n = \left(n\left(k_p + q_p\right) + r_p + r_q\right) mod\ n = \left(r_p + r_q\right) mod\ n = (p\ mod\ n\ +\ q\ mod\ n) mod\ n\ )$.

Definition.

An algebra $(G,*)$ is a *group* iff

1. $*$ is associative,
2. has an identity element *e:* $(\forall x \in G)(x * e = e * x = x)$
3. every element of G is invertible: $(\forall \text{x} \in G)(\exists y \in G)(x * y = y * x = e)$

If $*$ is commutative, the group is called *Abelian* (or *commutative*).

Fact.

Denote $\mathbb{Z}_n = \{0,1, \dots , n\text{-}1\}$. $(\mathbb{Z}_n, \oplus)$ is an Abelian group.

Comprehension.

Is $(\mathbb{Z}_n,\otimes)$ an Abelian group? For every n? For some? Never?

Find 10 more examples of Abelian groups.

Comprehension – answer.

Is $(\mathbb{Z}_n, \otimes)$ an Abelian group?

The answer is obviously NO because 0 is not invertible, in *mod* n arithmetic, just as it is not in usual arithmetic. (To verify this notice that $0 \otimes k = 0$ for every k, hence it is never equal to 1).

Comprehension – answer.

Is $(\mathbb{Z}_n \setminus \{0\}, \otimes)$ an Abelian group?

Solution. $(\mathbb{Z}_n \setminus \{0\}, \otimes)$ is a group iff n is a prime.

($\Rightarrow$) By contradiction. If $n=pq$, $p,q>1$ then $p \otimes q = 0$, hence it is not an algebra, so it is not a group.

($\Leftarrow$) We know that $\otimes$ is commutative, associative and has the identity element 1. We must show that $(\mathbb{Z}_n \setminus \{0\}, \otimes)$ is an algebra and that every element in $\{1,2, .. ,n\text{-}1\}$ is invertible w. resp. to $\otimes$.

Recall a property of primes:

n is a prime $\Leftrightarrow (\forall p, q)(n|pq \Rightarrow n|p \vee n|q)$.

Take $k \in \{1,2, .. ,n\text{-}1\}$.

Consider all products of the form $k \otimes 1$, $k \otimes 2$, .. , $k \otimes (n\text{-}1)$.

The above property implies that none of k, $2k$, $3k$, ... ,$(n\text{-}1)k$ is divisible by n (because none of 1,2, … , n-1 is).

Hence, $k \otimes 1$, $k \otimes 2$, .. , $k \otimes (n\text{-}1)$ are all from $\{1,2, .. ,n\text{-}1\}$.

This means that $(\mathbb{Z}_n \backslash \{0\}, \otimes)$ is an algebra.

n is a prime $\Leftrightarrow (\forall p, q)(n|pq \Rightarrow n|p \vee n|q)$.

The numbers $k\otimes 1$, $k\otimes 2$, .. , $k\otimes(n\text{-}1)$ are also *pairwise different*: Suppose $k\otimes p = k\otimes q$. Then $n|kp–kq$, i.e., $n|k(p–q)$ which means $n|k$ – not a chance, or $n|p-q$. But $2–n \leq p-q \leq n-2$ and the only number within that bracket divisible by n is 0, so $p-q=0$.

This means $\{k\otimes 1, k\otimes 2, .., k\otimes(n-1)\}$ is an n-1 element subset of the $n-1$ element set $\{1,2,..,n-1\}$ so the two sets are equal hence, one of $k\otimes 1$, $k\otimes 2$, .. , $k\otimes(n\text{-}1)$ must be equal to 1 – even though we don't know which one.

Back to POSETS

Comprehension. Prove or disprove:

If every proper subset of X is a chain, then X is a chain.

Solution attempt. Pick any $x, y \in X$. Since every proper subset of X is a chain, $\{x, y\}$ is a chain. Consequently, every two elements of *X* are *comparable* i.e., *X* is a chain. Clearly, in each case x is comparable to y, hence X is totally ordered by $\preccurlyeq$.
Is this OK? Not quite. We said "every proper subset of *X* is a chain" so the argument doesn't work for two-element sets *X*.

LEAST UPPER BOUND

Definition.

Let $(X, \preccurlyeq)$ be a poset and let $A \subseteq X$. An element $p \in X$ is called an *upper bound* for A iff for every $a \in A$, $a \preccurlyeq p$. If the set of all upper bounds of A has the smallest element t then t is called the *least upper bound* of A. If it exists, t is denoted by *sup*(A) or LUB(A)

Exercise. Write this definition in the formal, symbolic form, i.e., complete the statement

$t = \sup(A) \ \equiv \ldots$

using only quantifiers, logical and mathematical symbols and, of course, variables

GREATEST LOWER BOUND

Definition. (Twin to LUB)
Let $(X, \preccurlyeq)$ be a poset and let $B \subseteq X$. An element $q \in X$ is called a *lower bound* for B iff for every $b \in B$, $q \preccurlyeq b$. If the set of all lower bounds of B has the largest element *s* then *s* is called the *greatest lower bound* of *B*. If it exists, s is denoted by *inf*(*B*) or GLB(*B*).

Exercise. Write this definition using only …blah, blah, blah…

Remark.

In the ETMAG course we mentioned that for every nonempty, bounded from above subset A of $\mathbb{R}$ there exists the *least upper bound* (in $\mathbb{R}$). It may not be true in other posets. For example consider $(\{1,2,3\}, |)$. Clearly, both 2 and 3 are upper bounds for $\{1\}$ but there is no least upper bound.

Examples.

1. ($\mathbb{N}$, |) For every finite subset A of $\mathbb{N}$ *sup*(A) = LCM(A) (*Least Common Multiple*) and *inf*(A) = GCD(A) (*Greatest Common Divisor*).
2. ($\mathbb{R}$,≤). What is *sup*((0;1)), *sup*([0;1]), *inf*((0;1)), *inf*([0;1])?
3. ($\mathbb{Q}$,≤). What is *sup*($\{x \in \mathbb{Q} \mid x^2 < 2\}$)?
4. ($\mathbb{R}$,≤). What is *sup*($\{x \in \mathbb{R} \mid x^2 < 2\}$)?
5. ($\mathbb{Z}$,≤). What is *sup*($\{x \in \mathbb{Z} \mid x^2 < 2\}$)?

Comprehention.

1. $(\mathbb{N}, |)$. What can you say about *sup* and *inf* of infinite subsets of $\mathbb{N}$?
2. $(2^X, \subseteq)$. What is *sup*$(\{A_i\}_{i\epsilon I})$ and what is *inf*$(\{A_i\}_{i\epsilon I})$ for a family of subsets of X (meaning $A_i \subseteq X$ for each $i \in I$).

ORDER-PRESERVING FUNCTIONS

Definition.

Let $(X,\preccurlyeq)$ and $(Y,\Subset)$ be two posets and let f be a function mapping X into Y, i.e. $f : X \to Y$. We say that f is an *order-preserving function* iff $(\forall a, b \in X)(\text{ a} \preccurlyeq \text{b} \Rightarrow f(a) \Subset f(b)\ )$.

We may think of order-preserving functions as *nondecreasing* functions.

Examples. Is the function f order-preserving?

1. $f:(\mathbb{N},|) \to (\mathbb{N},\leq)$ $f(x) = x$
2. $f:(\mathbb{N},\leq) \to (\mathbb{N},|)$ $f(x) = x$
3. $f:(\mathbb{N},|) \to (\mathbb{N},|)$ $f(x)$ = the number of prime factors of x
4. $f:(\mathbb{N},\leq) \to (\mathbb{N},|)$ $f(x)$ = the number of prime factors of x
5. $f:(\mathbb{N},\leq) \to (\mathbb{N},\leq)$ $f(x)$ = the number of prime factors of x
6. $f:(\mathbb{N},|) \to (\mathbb{N},|)$ $f(x)$ = the number of prime factors of x
7. $f:(2^{\mathbb{N}},\subseteq) \to (\mathbb{N}\cup\{\infty\},\leq)$ $f(A) = |A|$

Comprehension 1

Let $(X, \preccurlyeq)$ and $(Y, \Subset)$ be two posets and let f be an order preserving function

1. A is a chain in $X \Rightarrow f(A)$ is a chain in Y?
2. A is an antichain in $X \Rightarrow f(A)$ is an antichain in Y?

a) What if f is an injection?
b) What if f is a surjection?
c) What if f is a bijection?

Comprehension 1

Let $(X, \preccurlyeq)$ and $(Y, \Subset)$ be two posets and let f be an order preserving function

3. B is a chain in $Y \Rightarrow f^{-1}(B)$ is a chain in X?
4. B is an antichain in $Y \Rightarrow f^{-1}(B)$ is an antichain in X?

a) What if f is an injection?
b) What if f is a surjection?
c) What if f is a bijection?

Comprehension 1 (cont.)

Let $(X, \preccurlyeq)$ and $(Y, \Subset)$ be two posets and let f be an order preserving function

5. p is maximal in $X \Rightarrow f(p)$ is maximal in Y? minimal?
6. $f(p)$ is maximal in $Y \Rightarrow p$ is maximal in X? minimal?

a) What if f is an injection?
b) What if f is a surjection?
c) What if f is a bijection?

Comprehension meta test.

Construct the Hasse diagram for the poset whose elements are problems from Comprehension 1 (including sub-questions a,b,c) and the ordering relation is $q \preccurlyeq p$ iff you consider question p not easier than q.

This is of course a very individual thing and it makes sense assuming that you have nothing better to do than solving all these problems, but have you? Seriously?