BU-CmpE 220 Discrete Mathematics	bingol/Fall 2016
Midterm 1, 1:50 hours	Oct. 25, 2016

Read me. Keep the question sheet. "Textbook" or "Grimaldi5e" means Grimaldi 5th edition. **Numbering.** Number the sheets so that sheet i should marked as Q$(2i-1)$ and Q$(2i)$. Staple your answer sheets and your cheatsheet together such that the cheatsheet should be at the front. Answer to question Qn should go to page Qn. **Answers.** Show your own work. Be clear, precise, short, necessary and sufficient in your answers. Otherwise prepare to lose points. Major mistakes leads to negative points. **No Answer.** Help us in grading, if you do not have the answer, do not attempt to fill the page with junk. Instead, you can get 2 points for the question by clearly indicating that you choose not to answer a question by diagonally writing NO ANSWER across the page. **Cheatsheet.** Open *cheatsheet* of single A4 in your own handwriting, only. Note that you will return it with your answers. **Nos.** No photocopied material. No printouts of any kind. No questions. No exchange of information, books, notes, pencils etc. Neither phones nor any other electronics. **Grading.** Make sure that you check your paper after it is graded. **Objection.** Your are welcomed for well grounded objections. If your object results with no point changes, then you loose 5 point for each question objected. Good luck.

Q1 [20 points]

Prove or disprove the following without use of truthtable.

$a' \wedge (a \vee b) \rightarrow b$

Solution.

$$
\begin{aligned}
a' \wedge (a \vee b) \rightarrow b &\equiv (a' \wedge a) \vee (a' \wedge b) \rightarrow b && //\text{distributivity} \\
&\equiv F \vee (a' \wedge b) \rightarrow b && //a' \wedge a = F \\
&\equiv (a' \wedge b) \rightarrow b && //a \vee F = a \\
&\equiv (a' \wedge b)' \vee b && //p \rightarrow q \equiv p' \vee q \\
&\equiv (a \vee b') \vee b && //\text{Demorgan} \\
&\equiv a \vee (b' \vee b) && //\text{associavity} \\
&\equiv a \vee T && //a \vee a' = T \\
&\equiv T && //a \vee T = T
\end{aligned}
$$

Q2 [20 points]

Definition 0.1. Let A be a set, and let $f\colon A \rightarrow A$ be a bijection. For any integer $k \in \mathbb{Z}$, define the kth power of a bijection as

$$
f^k = \begin{cases} \underbrace{f^{-1} \circ f^{-1} \circ \ldots \circ f^{-1}}_{-k}, & k < 0 \\ 1_A, & k = 0 \\ \underbrace{f \circ f \circ \ldots \circ f}_{k}, & k > 0, \end{cases}
$$

where 1_A is the identity function on A.

Let $O_a^f = \{f^n(a) \mid n \in \mathbb{Z}\}$ for any $a \in A$, Prove that if $a_1, a_2 \in A$, and $O_{a_1}^f \cap O_{a_2}^f \neq \emptyset$, then $O_{a_1}^f = O_{a_2}^f$.

Solution.

Suppose $O_{a_1}^f \cap O_{a_2}^f \neq \emptyset$. Let $a \in O_{a_1}^f \cap O_{a_2}^f$. Since $a \in O_{a_1}^f$ and $a \in O_{a_2}^f$, we have $a = f^{k_1}(a_1) = f^{k_2}(a_2)$ for some k_1 and k_2 in $\mathbb{Z}$. Then

$$
\begin{aligned}
f^{k_1}(a_1) &= f^{k_2}(a_2) \\
f^{-k_2}(f^{k_1}(a_1)) &= f^{-k_2}(f^{k_2}(a_2)) && //f \text{ is a bijection} \\
f^{k_1-k_2}(a_1) &= a_2 && //f^{-k} \circ f^k = 1_A \\
f^k(a_1) &= a_2 && //\text{for } k = k_1 - k_2
\end{aligned}
$$

Hence $a_2 \in O_{a_1}^f$. Therefore, $f^k(a_2) \in O_{a_1}^f$ for all $k \in \mathbb{Z}$. That means $O_{a_2}^f \subseteq O_{a_1}^f$.
Similarly, one can show that $O_{a_1}^f \subseteq O_{a_2}^f$. Hence $O_{a_2}^f = O_{a_1}^f$. □

Q3 [20 points]

Let G be a finite group with identity e, and let a be an arbitrary element of G.

Prove that there exists a positive integer n such that $a^n = e$.

Solution.

Consider the sequence $a^1, a^2, a^3, \ldots$. Since G is finite, not all terms of this sequence can be distinct. It eventually repeats itself. That is, $a^i = a^j$ for some $i < j$.
Then

$$\begin{aligned}
a^i &= a^j && \text{//eventually repeats} \\
&= a^{j-i+i} && \text{//addition in integers} \\
&= a^i a^{j-i} && \text{//definition of } a^n \\
(a^i)^{-1} a^i &= (a^i)^{-1}(a^i a^{j-i}) && \text{//left multiply by the unique inverse of } a^i \\
e &= ((a^i)^{-1} a^i) a^{j-i} && \text{// inverse and associativity} \\
&= e a^{j-i} && \text{//identity} \\
&= a^{j-i} && \text{//identity.}
\end{aligned}$$

So $e = a^n$ for $n = j - i$. □

Q4 [20 points]

Consider the following relations on $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$:

1. $(m, n) \in R_1 \iff m \mid n$.
2. $(m, n) \in R_2 \iff |m - n| \leq 2$.
3. $(m, n) \in R_3 \iff m + n$ is even.
4. $(m, n) \in R_4 \iff 3 \mid (m + n)$.

a) For each relation, determine whether it is reflexive, symmetric, antisymmetric or transitive. Justify your answer.
b) Which relations are partial orders, and which are equivalence relations?

Solution.

a) 1. R_1
   - Reflexivity: (Proof) Let $a \in \mathbb{Z}^+$ be an arbitrary number. Since $a \mid a$, $(a, a) \in R_1$.
   - Symmetry: (Disproof) $(3, 6) \in R_1$, but $(6, 3) \notin R_1$.
   - Anti-Symmetry: (Proof) $\forall a, b \in \mathbb{Z}^+$ if $a \mid b$ then $b = ka$, for some $k \in \mathbb{Z}^+$. Also, since $b \mid a$ then $a = lb$, for some $l \in \mathbb{Z}^+$. Substituting the first into the second, we get $kl = 1$ which yields $k = l = 1$ and therefore $a = b$.
   - Transitivity: (Proof) $\forall a, b, c \in \mathbb{Z}^+$ if $a \mid b$ then $b = ka$, and if $b \mid c$ then $c = lb$, where $k, l \in \mathbb{Z}^+$. Substituting the first into the second, we get $c = lka$. This means $(a, c) \in R_1$.

   2. R_2
   - Reflexivity: (Proof) $\forall a \in \mathbb{Z}^+$, since $|a - a| = 0 \leq 2$, $(a, a) \in R_2$.
   - Symmetry: (Proof) $\forall a, b \in \mathbb{Z}^+$ $|a - b| = |b - a|$. It follows that, $(a, b) \in R_2 \longrightarrow (b, a) \in R_2$.
   - Anti-Symmetry: (Disproof) $(1, 3), (3, 1) \in R_2$, but $1 \neq 3$.
   - Transitivity: (Disproof) $(1, 3), (3, 5) \in R_2$, but $(1, 5) \notin R_2$.

   3. R_3
   - Reflexivity: (Proof) $\forall a \in \mathbb{Z}^+$, since $a + a = 2a$, which is even regardless of a, $(a, a) \in R_3$.
   - Symmetry: (Proof) $\forall a, b \in \mathbb{Z}^+$, $a + b = b + a$ due to the commutativity of addition. It follows that, $(a, b) \in R_3 \longrightarrow (b, a) \in R_3$.
   - Anti-Symmetry: (Disproof) $(1, 3), (3, 1) \in R_3$, but $1 \neq 3$.
   - Transitivity: (Proof) Let $(a, b), (b, c) \in R_3$. Then $a + b = 2k$ and $b + c = 2l$ for some $k, l \in \mathbb{Z}^+$. Adding these up, $a + 2b + c = 2(k + l)$. Subtracting $2b$ from both sides, we get $a + c = 2(k + l - b)$ which is a positive and even number. Hence $(a, c) \in R_3$.

   4. $R_(4)$
   - Reflexivity: (Disproof) $(1, 1) \notin R_4$.
   - Symmetry: (Proof) $\forall a, b \in \mathbb{Z}^+$, $a + b = b + a$ due to the commutativity of addition. It follows that, $(a, b) \in R_4 \longrightarrow (b, a) \in R_4$.
   - Anti-Symmetry: (Disproof) $(3, 6), (6, 3) \in R_4$, but $3 \neq 6$.
   - Transitivity: (Disproof) $(4, 2), (2, 1) \in R_4$, but $(4, 1) \notin R_4$.

b) Partial Order: R_1. Equivalence Relation: R_3.

Quotation of the exam: Niels Abel (1802 — 1829)
https://en.wikipedia.org/wiki/Niels_Henrik_Abel

> The mathematicians have been very much absorbed with finding the general solution of algebraic equations, and several of them have tried to prove the impossibility of it. However, if I am not mistaken, they have not as yet succeeded. I therefore dare hope that the mathematicians will receive this memoir with good will, for its purpose is to fill this gap in the theory of algebraic equations.

Quoted in opening of Memoir on algebraic equations, proving the impossibility of a solution of the general equation of the fifth degree (1824)
source: http://www-history.mcs.st-and.ac.uk/history/Quotations/Abel.html