第1章　ブール代数の基礎

1.1　序文

このテキストは, ＩＴ大学院の掲示板「寺子屋」で開催された井上茂雄博士によるブール代数の公開セミナーの講義録を編集したものです。セミナー講師の井上茂雄博士と, 演習参加者の鈴木康正氏の承諾を得て, 師玉が電子化し, 当大学院の教材として使用いたします。編集にあたっては，電子掲示板でのセミナーの雰囲気をできるだけ再現するよう，講師からの参加への話しかけその他をそのまま，読者へのそれとして記述しました。

1.2　初等集合論からの準備

このセミナーではブール代数 (Boolean Algebra) の理論について勉強していきたいと思います。
理論に重きを置き, 時に演習を行います。
J. D. Monk 著の Mathematical Logic (GTM37) (Springer-VerlAg) のブール代数の章 (20 ページ) をベースにして, 一緒に勉強して行きましょう (私自身, ブール代数の専門家ではないので).

皆さんは, 意識的にあるいは無意識のうちにブール代数にはすでに何らかの形で出会っていると思います。
論理回路を通じて, 集合の演算を通じて, あるいは命題論理等を通じてです。
しかしながら, ブール代数を数学における代数学としてきちんと習ったことはないのではないでしょうか. 今回のセミナーの目的は, そこにあります。
つまり, ブール代数を数学における代数学としてきちんと理論的に学ぶということです (数理論理学者の目を通じてということですが). 私はブール代数を奥が深い数学の一分野だと思っています。

ブール代数における代数構造は命題論理と親密な関係にあります。
また, それには応用があります (論理回路等). ブール代数は初等集合論から最も簡単に動機付けできるでしょう.

[定義 **1**] (その 1)

集合の体 (field of sets) A とは, 次の性質 (1)-(3) を満たす集合である:

1. $\cup A \in A$
2. 任意の $X \in A$ について, $\cup A \sim X \in A$
3. 任意の $X, Y \in A$ について, $X \cup Y \in A$. またこのとき,A を $\cup A$ の部分集合の体という.

(定義 1 の終わり)

ここで, 若干の記号の説明と約束をします。
まず記号のお約束.A, B を集合とするとき,

$$A \cap B, A \cup B, A \sim B$$

をそれぞれ, 共通部分 (積集合), 合併 (和集合), 差集合とします。
($B \subseteq A$ ならば, $A \sim B$ を A に関する B の補集合といいます。
$A - B$ という記号法も普通に用います。
ある集合 A 内だけで考えているときは, $A \sim B$ を単に B^c と書き, B の補集合といいます。

「$\cup A$」という記号は, 公理的集合論の方からの記号法です。
公理的集合論は, 広い意味での数理論理学 (Logic) の一部分で等号を含む 1 階古典述語論理に基づいて公理的に集合論を展開する学問です。
非常に高度に発達している分野です。
大雑把にいって, その根底の考え方の一つは, 数学的対象の全てを集合として考える, ということです。
$\cup A$ の説明に戻ります。
つまり, A を集合とすると, A の和 (あるいは和集合) $\cup A$ は A の要素の要素全体からなる集合です。

$$\cup\{A, B\}$$

を特に $A \cup B$ と書きます。
だから公理的集合論では, $\cup A$ の $\cup$ 方が $A \cup B$ で使っている $\cup$ より上位概念ですね. 例えば,

$$A = \{\{1, 2\}, \{7, 3\}, \{3, 5, \{4\}\}\}$$

のとき,

$$\cup A = \{1, 2, 3, 5, 7, \{4\}\}$$

です。
このブール代数のセミナーでは, 公理的集合論を表にはあまり出しませんが, 記号法などにその香りが表われています。
とにかく, 基本的な用語も含めてわからなければどんどん質問してくださいね

集合の体 A とは, $\cup A$ に関する補集合と合併をとる演算に関して閉じている集合であるといえます。
すこし表現を変えれば, 集合の体 A とは, A の要素の要素全体からなる集合 $\cup A$ を全体と考えて, その部分集合についての ($\cup A$ に関する) 補集合と合併をとる演算に関して閉じている集合です。

「閉じている」について説明します。
まず, 例で言った方が速いでしょう.
$\mathbf{Z}$ を整数全体の集合とします。 $\mathbf{Z}$ の任意の要素 x, y について, $x+y$ がまた $\mathbf{Z}$ の要素となるとき, $\mathbf{Z}$ は加法+について (に関して) 閉じているといいます。
$\mathbf{Z_p}$ を正の整数全体の集合とします。 $\mathbf{Z_p}$ の任意の要素 x, y について, $x-y$ は必ずしも $\mathbf{Z_p}$ の要素とはなりません.
例えば $3-5=-2$ ですから. Zp は減法ーについて閉じていません. ところが,$\mathbf{Z}$ は当然, 減法ーについて閉じています。
一般の場合は,

[一般の場合]
一般に, 集合 S について,α を直積 $S \times S$ から S への写像とし,

$$(x, y) \in S \times S$$

の α による像

$$\alpha(x, y)$$

($x\alpha y$ とも書く) がまた S の要素のとき, 集合 S は 1 つの算法 α をもつ代数系, あるいは略して α 系といいます。
集合 S はその α 系の台集合といい, このような α を S における二項算法といいます。
S を α 系とします。
T を S の部分集合とするとき,(任意の x, y について (数学の本ではこれがはぶかれて暗黙のうちに仮定されていることも多い),)

$$x, y \in T$$

ならば

$$x\alpha y \in T$$

となるならば, T は α に関して閉じているといいます。
このとき, 写像 α の $T \times T$ への制限 α_t を考えると, T は α_t 系となります。
α と α_t は T の要素に関しては同じ効果を持つので, T もまた α 系と呼ぶのが普通です。
このとき, T は S の部分 α 系といいます。
したがって, 当然 S は α に関して閉じています。

[一般の場合の説明終わり]

[命題 **2**] A を集合の体とする. そのとき, 次が成立する.

1. $0 \in A$;
2. もし $X, Y \in A$ ならば, $X \cap Y \in A$.

(命題 2 の終わり)

命題 2 で 0 は空集合を表します。
つまり, 集合の体 A は空集合を要素に持ち, 演算 $\cap$ について閉じている集合ということです。
それではさっそく演習です。

(演習 1) 命題 2 を証明しなさい.

(演習 1 の終わり)

1.3 参考文献について

このセミナーに参加される方は, ブール代数という言葉およびブール代数それ自体について, すでに程度の差はあれ御存知かと思います。
そうでない方ももちろん参加可能です。
これからブール代数をここで学んでいくわけですから.(また, 今回はお話ですから, 知らない用語等には, あまりこだわらず気にされないようにお願いします。
ここは, 大学院のセミナーですから, 皆さんの知的刺激になるような見慣

れぬ言葉も出てくるでしょう.
あなたが, 過去に一度ブール代数に出合った方だとしましょう. では, どのような所で出合ったのか思い起こしてみましょう.
例えば, 情報・工学・工業関係で論理回路を学んだ際, 論理式を簡単化するときの操作としてブール代数に出会った方がいらっしゃるでしょう. 離散数学, 論理回路, ディジタル回路, スイッチング回路, 情報数学等の科目で出てきたのでは. また, 大学以上で数学を学ばれた方 (別に特に数学科で学ばれたということには限らず) は, 集合の演算がブール代数をなすとかで, 出合われたでしょう. やはり, 情報系・工学系の基礎として, あるいは教養として, あるいはもっと進んだ集合論 (ブール代数値モデルとか) に関わるものとして, あるいはモデル理論や普遍代数 (universal algebra) がらみで (これはいないかな) とか.
またブール代数は束論 (lattice theory) で取り扱うことができるので, こちらから導入された方もいらっしゃるでしょう.
ブール代数はある種の束ですから. 一方, 論理学の方から, 命題論理学がブール代数に対応しているということで学ばれた方もおられるでしょう.
ブール代数は古典命題論理の代数化ですから.

ひょっとして, 命題論理の完全性やコンパクト性定理をブール代数で証明されたのを聴かれたとか.
色々な論理体系の代数モデルで出てきたとか. もっと進んだ形で, 卒業研究とかでかかわった方もおられるかもしれません.
論理回路, 集合, 命題論理を関連付けるものとして総合的に学ばれた方もいるかもしれませんね.

(演習 2) 命題 2 を証明しなさい.

> あなたが, もし意識的に過去ブール代数にかかわったことがあるなら, どのような所で出合ったのか思い起こしてみましょう. もしよければ, ここで紹介してくださるとうれしいのですが.
> セミナー参加者の自己紹介にもなりますし. 意識的にかかわったことが なければ, かかわったことがない, という紹介でもいいですね.

(演習 2 の終わり)

色々な出合いがあったことと思います。
しかし, 大学レベルの教科書や, カリキュラムをみるとブール代数の取り扱いが, おまけぐらいというか, なにかすごく表面的な感じがしてなりません.

そこに私は非常に不満を持っているので, それが, このセミナーを企画した理由です。
つまりこのセミナーで, ブール代数をもっと理論的・数学的 (代数的) にきちんと学ぶ機会を提供したいと思います。
量は多くないですが, 基本となる理論の核となる部分をきっちりと学んでいただけたらと思います。
おそらく, ここで学ぶ内容は他ではなかなか先生について学ぶ機会はないと思います。
短いとはいっても, 半年はかかるでしょう. 皆さんと私のがんばり次第では, もっと早く終わって次のセミナーに移れるかもしれませんが.

このセミナーのテキストといえるものは J. D. Monk 著の Mathematical Logic (GTM37) (Springer-VerlA) のブール代数の章 (20 ページ) です。
私はブール代数の専門家ではありませんが, テキストの著者の Monk さんはブール代数関連の専門家で著名な方です。
この書物は数理論理学の教科書として非常にすぐれた書物です。
皆さんもこの本と将来お友達になれたらいいですね

ブール代数の定義も済んでいないのになんですが, ブール代数の参考文献について少し書いておきます。
ブール代数は, 離散数学, 論理回路, ディジタル回路, 情報数学等の教科書ではたいてい取り扱われているでしょう. 日本語の書物は非常に多いし, 各人の好みの参考書で適宜参考にしていただければと思います。
ブール代数に関して日本語の書物で私の気に入ったものはありません. 私の気に入った入門書はこのセミナーで用いる J.D. Monk 著の Mathematical Logic (GTM37) (Springer-VerlA) のブール代数の章 (20 ページ) ですので, それを使うわけです。
ただ, 今注文していてまだ見ていないのですが, 「現代のブール代数」S. コッペルベルク著, 渕野昌訳, 共立出版はいい本ではないかと期待しています。
ずいぶん前に出ていたのですが, 知りませんでした. ちょうどそのころ私は日本にいなかったし. 渕野さんは数理論理学に関連するブール代数の専門家の一人です。
ただきっと, すごく数学よりで高級な本なのではないかと思います。
早く手に取って見たいものです。
ブール代数の参考文献で, きまって引用される書物は, Monk さんもそれのみを引用されていますが, 次の 2 冊です。

1. P. R. Halmos, Lectures on Boolean Algebra, Princeton, van Nos-

trand, 1963.
2. S. Sikorski, Boolean Algebra, 3rd. ed. New York, Berlin, Springer, 1969.

Halmos さんは, 著名な尊敬されている数学者です。
線形代数の有名な教科書や, 測度論の演習書, 代数的論理学の書, 素朴集合論の教科書 (実は公理的な取り扱いをしている) などの書物を書いておられます。

Sikorski さんは, 論理体系の代数的取り扱いについての定評ある書物 (RASiowa さんと共著) を書いておられます。
また, ポーランド語ですが, 関数論の教科書もあります。

上記 2 冊とも, 入手しずらい (と思う) し, 私も持っていません. 欲しいとは思っていますが.
基本的な数学の概念の解説書として, 現代数学概説 I, 弥永昌吉, 小平邦彦著, 岩波書店 は持っておいて損のない書物です。
読みこなすのは大変だと思いますが, 辞書のように使えばいいのです。
弥永昌吉さんと小平邦彦さんは日本を代表する数学者です。
特に小平さんは, その業績で世界的に著名な尊敬されている数学者です。
弥永昌吉さんは現代の日本の数学の興隆の土台を作るうえで大変大きな功績を残こされた方です。

公理的集合論について, 日本語では, 公理的集合論, 田中尚夫著, 倍風館が, 本格的で非常に良い書物です。
こちらも持っておいて損のない書物です。
素朴集合論についても, 少し書いてあります。
田中尚夫さんは数理論理学の専門家です。

さて, 大学生以上の方に, ブール代数って何ですか？　と尋ねたとき, たぶんこう答えてくれるだろうと思います。
「ブール代数？ああ, 集合の $\cup, \cap, \sim$ についての代数だろ」と答えておしまいになると思います。
でも, それあたっているんですよ. それは次の定理を平たい言葉でいっていることになるのですから.

[ブール表現定理] すべてのブール代数はブール集合代数に同型である.

(ブール表現定理終わり)

本セミナーではこの表現定理を証明します。

[重要] このセミナーでは, 定義, 定理, 命題, 系, 補題を通し番号で番号付けします。
定理 60 の 60 が最終番号で, ブール代数と命題論理の理論が同じものであるという, ブール表現定理とは別の種類の完全性定理を証明して終わります。
演習は別番号で通し番号にします。
演習が何番までいくかはまだ未定です。
そのときどきにおいて自由に出題しますから.
本セミナーのブール代数の取り扱いは公理的, 代数的です。
ブール代数は束論から導入できますが, ここではそれは行いません. 束論的観点からブール代数を見るというのは, このセミナーが終わったあとで, 新しいセミナー, 例えば「論理と位相」(ブール代数と Stone 空間) とか, 「ブール代数 2」(色々なトピックでできる) とか企画できれば, そこで行いたいと思います。

最後に演習で第 2 節を締めくくりましょう. 次の第 3 節で, ブール代数を定義し, いよいよ本格的に入っていきます。

(演習 3) まずは集合の体についての補足です。

(1) 集合の体は定義 1 で定義されたのですが, 集合の体を定義 1 とは異なる 仕方で定義できますか ?

(2) 空でない集合 X が与えられたとします。
この X から集合の体を 作れますか ?
少し, 集合算の復習をしますか ? ちょっと面倒ですが, やって損はないでしょう. 論理学の勉強にも, 具体的なブール代数の演算の勉強にもなりますしね (ブール表現定理 !). 皆さんで手分けしてかまいませんから, 次の集合についての等式, 命題を証明してください.

(3)-I
1. $A \cap (B \sim C) = (A \cap B) \sim C$;
2. $(A \cup B) \sim C = (A \sim C) \cup (B \sim C)$;
3. $A \sim (B \cup C) = (A \sim B) \cap (A \sim C)$;
4. $A \sim (B \cap C) = (A \sim B) \cup (A \sim C)$;

5. $A \sim (A \sim B) = A \cap B$;
6. $A \cup (B \sim A) = A \cup B$;
7. $A \cap B^c = 0 \Leftrightarrow A \subseteq B$;
8. $(A \sim B)^c = A^c \cup B$;
9. $(A \cap B = 0 \; and \; A \cup B = C) \Rightarrow A = C \sim B$.

(3)-II $A \triangle B = (A \sim B) \cup (B \sim A)$ を対称差といいます。
論理回路をやった方は EX-OR(排他的論理和) に対応するものです。
(f) で $A \triangle B$ がどういうものかよくわかりますね. この $\triangle$ の挙動をみて, あれっと思いませんか？.

1. $A \triangle B = B \triangle A$;
2. $(A \triangle B) \triangle C = A \triangle (B \triangle C)$;
3. $A \triangle B = 0 \Leftrightarrow A = B$;
4. $A \triangle 0 = A$;
5. $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$;
6. $A \triangle B = (A \cup B) \sim (A \cap B)$.

(演習 3 終わり)

1.4 ブール代数の公理系

さて, ここで集合の体という具体的な概念から抽象して, 代数構造 $(A, +, \cdot, -, 0, 1)$ を考えましょう. ここで, それぞれ A は集合の体 A_s に, $+$ は $\cup$ に, $\cdot$ は $\cap$ に, $-$ は $\sim$ ($\cup A_s$ に関して) に, 0 は空集合 0 に, 1 は $\cup A_s$ に対応させたいわけです。
まず, $+, \cdot, -, 0, 1$ についての公理を書き出し, 集合の体の具体的な概念を完全に公理化します。
その後, 我々の公理化が実際, 具体的な概念間の全ての真な等式を捉えていることを示します。
全てのブール代数において, $+, \cdot, -, 0, 1$ はブール代数上の演算, 定数であることに注意してください. もちろん, 0 と 1 は, 整数の 0 と 1 とは全く異なる意味で用いられます。

定義 3 ブール代数 (Boolean Algebra)(今後頻繁に BA と略します) は, 次の (1),(2) を満たす体系 $\mathcal{A} = (A, +, \cdot, -, 0, 1)$ である:

1. A は空でない集合である.$0, 1 \in A$. また, $+$ と $\cdot$ は A 上の 2 項演算, $-$ は A 上の 1 項演算であって, A は $+, \cdot, -$ について閉じている;
2. 任意の $x, y, z \in A$ について, 次の条件 (i) $\sim$ (v) を満足する :
   (a) $x + y = y + x$ そして $x \cdot y = y \cdot x$ (交換律, 交換法則);
   (b) $x + (y + z) = (x + y) + z$ そして $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (結合律, 結合法則);
   (c) $x \cdot y + y = y$ そして $(x + y) \cdot y = y$ (吸収律, 吸収法則);
   (d) $x \cdot (y + z) = x \cdot y + x \cdot z$ そして $x + y \cdot z = (x + y) \cdot (x + z)$ (分配律, 分配法則);
   (e) $x \cdot -x = 0$ そして $x + -x = 1$ (補元律, 補元法則, 相補法則)

(任意の $x \in A$ について,$-x$ を x の補元 (complement) といいます。
).
(上で, 結合の強さ (演算の優先順位) は,$-$ が最も強く, その次に $\cdot$, 最後に $+$ です。
この約束によって, 括弧が省略できます。)

特に,$x + y = y$ を $x \leq y$ と書くことにします。
A は $\mathcal{A}$ の, 宇宙 (universe), あるいは基礎集合 (下敷きとなる集合)(underlying set) と呼びます。

(定義 3 の終わり)

定義 3 の (i) $\sim$ (v) はブール代数を定義するための公理です。
今後, ブール代数の公理といったら, この (i) $\sim$ (v) を意味します。
$3(i) \sim 3(v)$ というように引用します。
$+, \cdot, -$ を総称して,Boole 演算 (ブール演算)(Boolean operataion) といいます。
補元は一意的です ((演習 4)(4)). つまり, 任意の $x \in A$ について,

$$(x \cdot y = 0 \quad and \quad x + y = 1) \Rightarrow y = -x$$

です。

(余談ですが, 字体について. 上の A_s は,A のスクリプト体, $\mathcal{A}$ は,A のドイツ語の花文字のつもりです。
フォントがないのでこう書きました. また, 数式の文字は, 実際は全てイタ

リックです。
$< A, +, \cdot, -, 0, 1 >$ の丸括弧も, 本当は不等式の括弧で表したいのですが, そうするとこの掲示板では引用になってしまいますので, やむなく丸括弧にしました (^^;)

[重要] このセミナーにおいて, 特に断らない限り, 任意のブール代数 (BA) は上の $\mathcal{A}$ で, また任意の要素は, A の要素 x, y, z 等として取り扱います。おきまりのチェックによって, 次がいえます。

系 4 もし, A_s が集合の体ならば, $(A_s, \cup, \cap, \sim, 0, \cup A_s)$ はブール代数であり, $\cup A_s$ の部分集合のブール集合代数 (Boolean set algebra of subsets of $\cup A_s$) と呼ばれる.

[証明] (演習 4)(1)　[証明終わり]
定義 3 の公理の形から明らかなように, 次の命題に注意してください.

[命題 **5**] もし, $\mathcal{A} =< A, +, \cdot, -, 0, 1 >$ が BA ならば, $(A, \cdot, +, -, 1, 0)$ もそうである.

[証明] (演習 4)(2)　[証明終わり]
命題 5 から, 双対の原理 (duality principle) がでてきます。
つまり, 初めの $< A, +, \cdot, -, 0, 1 >$ について BA で成立する文 (式) は, そこに現れる全ての $+, \cdot, 0, 1$ をそれぞれ, $\cdot, +, 1, 0$ で置き換えたものは,2 番目の $(A, \cdot, +, -, 1, 0)$ でも成立します。
我々は今後, この双対の原理を自由に用いることにします (演習のときにも自由に使ってください.). ブール代数で成立する基本的な式 (定理) は 第 4 回で提示, 証明, 演習します。
さて, 演習でその準備として基本的なことをチェックしましょう.

(演習 4)
1. 系 4 を証明しなさい.
2. 命題 5 を証明しなさい.
3. BA で, $x + x = x, x \cdot x = x$ (べき等律),
   $x \cdot 0 = 0, x \cdot 1 = x,$
   $x + 0 = x, x + 1 = 1$
   が成立することを, 証明しなさい.(ブール代数の公理を用いて証明するのですよ.)
4. ブール代数において, 補元が一意的であることを証明しなさい.
5. ブール代数において, 0 と 1 の働きをする要素はそれぞれ 1 つし

かないことを証明しなさい.

6. BA で, 次が成り立つことを証明しなさい.

(a) $x \leq y \Leftrightarrow x \cdot y = x$;

(b) $x \leq y \Leftrightarrow x \cdot -y = 0$.

(注) 上の (4) $\sim$ (6) は全てブール代数の公理を用いて証明します。)

1.5 補足：命題論理・ブール代数・集合論の対応について

命題論理・ブール代数・集合論の対応関係は, 例えば,

[命題論理の世界] 論理記号を $\vee(or), \wedge(\ and\ ), \sim(not), \Leftrightarrow$ (equivalent, 同値記号) とします。
また, T を truth(真), F を falsum(偽)(真理値) とします。

(1)-P $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \vee C)$;
(2)-P $\sim (A \vee B) \Leftrightarrow \sim A \wedge \sim B$;
(3)-P $A \vee \sim A \Leftrightarrow T$;
(4)-P $A \wedge \sim A \Leftrightarrow F$.

[ブール代数の世界]

(1)-B $A \cdot (B + C) = (A \cdot B) + (A \cdot C)$;
(2)-B $-(A + B) = (-A) \cdot (-B)$;
(3)-B $A + (-A) = 1$;
(4)-B $A \cdot (-A) = 0$.

[集合論の世界] ある集合の体 X について, 任意の集合 $A, B, C \in X$ について (当然, $A, B, C \subseteq \cup X$ です),

(1)-S $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
(2)-S $(A \cup B)^c = A^c \cap B^c$;
(3)-S $A \cup A^c = \cup X$;
(4)-S $A \cap A^c = 0$.

上の記号法では,3 つの世界の記号は下のように対応しています,

[命題論理の世界]	[ブール代数の世界]	[集合論の世界]
A, B, C(命題変数)	A, B, C(ブール代数の変数)	A, B, C(集合変数)
$\vee(or)$	$+$	$\cup$
$\wedge(and)$	$\cdot$	$\cap$
$\sim(not)$	$-$	^{c}($\cup X$ について)
$\Leftrightarrow(equivalent)$	$=$ (等号)	$=$ (等号)
$T(truth)$	1	$\cup X$
$F(falsum)$	0	0(空集合)

特に, すべての有限ブール代数はある空でない集合 X のべき集合 $P(X)$ のブール集合代数 (特にこの場合べき集合代数という) と同型です。
前に証明すると予告した, ブール表現定理「すべてのブール代数はブール集合代数と同型である」は, より一般の場合です。
有限ブール代数の場合の同型定理も証明すると思います。
上の定理より, すぐに有限ブール代数の要素の個数は 2 の n 乗 (ある n について) であることがわかります。

1.6 双対原理

前節では, 定義 3 で, ブール代数 (BA と略) $\mathcal{A} =< A, +, \cdot, -, 0, 1 >$ を定義しました. ブール代数を定義する仕方には, 定義 3 以外の方法もあります。
代表的なものとして束論とのからみで定義することができます。
(演習 4) で BA についての若干の命題を証明していただきました. 第節回でブール代数の異なる定義を示す前に, その準備もかねて少し演習の続きを行いましょう. その前に少し双対の原理を復習しましょう.

前節でも書きましたが, 命題 5 から, 双対の原理 (duality principle) が成立します。
つまり, $\mathcal{A} =< A, +, \cdot, -, 0, 1 >$ について BA で成立する文 (式) は, そこに現れる全ての $+, \cdot, 0, 1$ をそれぞれ, $\cdot, +, 1, 0$ で置き換えて作った文 (式) もまたその BA で成立します。
従って, その文 (式) は, もとの $< A, +, \cdot, -, 0, 1 >$ で成立します。
この双対の原理をどんどん使ってみてください. いや使うべきです。
すばらしい原理なのですから. 演習のときにも自由に使ってください. 双対の原理は, 単に式だけでなく, 当然その証明 (文) にも当てはまります。
例えば, $x + x = x$ が証明できたとしましょう. すると, それから双対の原

理を用いてすぐに $x \cdot x = x$ がいえます。
ですが, それのみならず, $x + x = x$ の証明が,

$$\begin{aligned} x &= x \cdot x + x \\ &= x + x \cdot x \\ &= (x + x) \cdot (x + x) \\ &= x \cdot (x + x) + x \cdot (x + x) \\ &= (x + x) \cdot x + (x + x) \cdot x \\ &= x + x \end{aligned}$$

であったとすると, $x \cdot x = x$ の証明として, 上の証明から双対の原理を用いてすぐに,

$$\begin{aligned} x &= x + x \cdot x \\ &= x \cdot x + x \\ &= (x \cdot x) + (x \cdot x) \\ &= (x + (x \cdot x)) \cdot (x + (x \cdot x)) \\ &= ((x \cdot x) + x) \cdot ((x \cdot x) + x) \\ &= x \cdot x \end{aligned}$$

が得られます (括弧は少し補充しました).
　ですから, お互いに双対の関係になっている式 (文) は, 片方の式 (文) が証明できれば, 双対の原理により, もう片方は自動的に成立します。

(演習 5) (注:下の (1) ∼ (4) で, 演習 4 の結果は使ってよいことにします。使わなくてもいいですが. もちろん, 全てブール代数の公理を用いて証明します。)

1. BA で,$--x = x$　(二重否定の法則);
   $-(x + y) = -x \cdot -y$　(ド・モルガンの法則);
   $-(x \cdot y) = -x + -y$　(ド・モルガンの法則)
   が成立することを, 証明しなさい.

2. BA で, 次が成り立つことを証明しなさい.
   (a) $x \leq x$　(反射律);
   (b) $(x \leq y \ and \ y \leq x) \Rightarrow x = y$　(反対称律);

(c) $(x \leq y \ and \ y \leq z) \Rightarrow x \leq z$　(推移律);

3. BA で, 次が成り立つことを証明しなさい.
(a) $x = -y \Leftrightarrow x + y = 1 \ and \ x \cdot y = 0$;
(b) $0 \leq x \leq 1$;
(c) $(x \leq z \ and \ y \leq z) \Rightarrow x + y \leq z$;
(d) $(x \leq z \ and \ y \leq z) \Rightarrow x \cdot y \leq z$;
$(x \leq y \ and \ x \leq z) \Rightarrow x \leq y \cdot z$
(e) $a \cdot x \leq y \Leftrightarrow x \leq -a + y$. (結合の強さは, $-, \cdot, +$ の順！)

4. BA で, $-(-x + -y + z) + -(-x + y) + -x + z = 1$
が成り立つことを証明しなさい.

5. $\mathbf{N}$ を自然数全体の集合とします. N を 0 でない自然数とし, どんな素数 P についても,N は P の 2 乗で割り切れないものとします (ここでは, 0 は自然数の内に含めるものとします). このとき, $An = \{x \in \mathbf{N} : 1 \leq x \leq N, x$ は N を割り切る (つまり, N は x の倍数) $\}$ とおきます。
任意の $x, y \in An$ について, $x + y$ を x と y の最小公倍数と定義し, $x \cdot y$ を x と y の最大公約数と定義します。
また, 任意の $x \in An$ について, $-x$ を N/x (N を x で割った商) と定義します。
このとき, 次の問いに答えなさい.
(a) 任意の $x, y \in An$ について, $x + y = y \Leftrightarrow (y$ は x の倍数) を証明しなさい.
(b) $1, N \in An$ であることを確認しなさい.
(c) $x + y = y$ を, $x \leq y$ と書くことにする. 任意の $x, y, z \in An$ について,
i. $x \leq x$　(反射律);
ii. $(x \leq y \ and \ y \leq x) \Rightarrow x = y$　(反対称律);
iii. $(x \leq y \ and \ y \leq z) \Rightarrow x \leq z$　(推移律)
がいえることを証明しなさい.
(d) 任意の $x, y, z \in An$ について,
$x \cdot (y + z) = x \cdot y + x \cdot z$
$x + y \cdot z = (x + y) \cdot (x + z)$　(分配律, 分配法則)
が成り立つことを証明しなさい.
(e) $\mathcal{A}N = (An, +, \cdot, -, 1, N)$ はブール代数であることを証明しなさい.

(演習 5 の終わり)

さて, これ以後しばらく, ブール代数に関するいくつかの代数的概念を導入し, 調べて行きましょう.

[定義 **7**] $\mathcal{A} =< A, +, \cdot, -, 0, 1 >$ と $\mathcal{B} =< B, +', \cdot', -', 0', 1' >$ を 2 つのブール代数とする.$\mathcal{A}$ と $\mathcal{B}$ が次の条件 (1),(2) を満足するとき, $\mathcal{A}$ は $\mathcal{B}$ の部分代数 (subalgebra) であるという:

1. $A \subseteq B, 0 = 0', 1 = 1'$;
2. 任意の $x, y \in A$ について,$x + y = x +' y, x \cdot y = x \cdot' y, -x = -'x$. また, 任意の $X \subseteq B$ について, $0', 1' \in X$ であって, X が $+', \cdot', -'$ について閉じているならば,X は $\mathcal{B}$ の部分宇宙 (subuniverse) という.
(定義 7 の終わり)

従って, もし $\mathcal{A}$ が $\mathcal{B}$ の部分代数ならば, A は $\mathcal{B}$ の部分宇宙です。
$\mathcal{B}$ の全ての部分宇宙は,$\mathcal{B}$ のある部分代数の基礎集合 (台集合) です。
ですから部分宇宙は, 単に部分代数からその基礎集合以外を無視したものと考えられます。
いうまでもないことですが, B は $\mathcal{B}$ の部分宇宙です。
次の命題は部分宇宙に関する同値な定義を与えます。

[命題 **8**] $\mathcal{A} =< A, +, \cdot, -, 0, 1 >$ をブール代数とし, $X \subseteq A$ とする. そのとき, 次の (1) $\sim$ (3) は同値となる:

1. X は $\mathcal{A}$ の部分宇宙である;
2. $X \neq 0$ であって, X は $+, -$ について閉じている;
3. $X \neq 0$ であって,X は $\cdot, -$ について閉じている.
(命題 8 の終わり)

[証明] (演習 6)　[証明終わり]
次はほとんど明らかです。

[命題 **9**] $\mathcal{A} =< A, +, \cdot, -, 0, 1 >$ をブール代数とする. A_s を $\mathcal{A}$ の部分宇宙を要素とする空でない集合とすると,$\cap A_s$ は, $\mathcal{A}$ の部分宇宙である.
(命題 9 の終わり)

[証明] (演習 8)　[証明終わり]

ここで, 命題 9 に出てきた集合論の記号 $\cap$ を説明します。
$\cap$ は, 集合 $X \neq 0$ について,$\cap X = \{Z : \text{任意の } Y \in X \text{ について, } Z \in Y\}$ と定義される集合で, X の積 (積集合) といいます。
それでは演習で締めくくりましょう. この節は演習が多いですが, じっくりと考えてみてください.

(演習 6) 命題 8 を証明しなさい.(演習 6 の終わり)

(演習 7) $\cap\{X\}, \cap\{X, Y\}$ はそれぞれ, 今までの集合論の記号法では何になるでしょうか. もし, 全体集合を V として, そのなかで X を考えているものとします。
このとき.$X = 0$ として, 無理やり上の $\cap$ についての定義を適用すると, $\cap X$ は何になるでしょうか.(演習 7 の終わり)

(演習 8) 命題 9 を証明しなさい.(演習 8 の終わり)

(演習 9) A の空でない部分集合 X で, $0, 1 \in X$ であり, $+, \cdot$ について閉じているが, X は A の部分宇宙でないというブール代数 $\mathcal{A}$ が存在することを証明しなさい.(演習 9 の終わり)

1.7 双対原理についての補足

任意のブール代数の関係式 ψ について :「公理系 T で ψ が証明可能」$\Rightarrow$「 ψ に現われる全ての $+, \cdot, 0, 1$ を逆転した関係式 ψ_d もまたその公理系 T で 証明可能」が (式に関して限定した形での) 正しい形です。

我々のブール代数 $\mathcal{A} = (A, +, \cdot, -, 0, 1)$ の公理系を T とし, そこから, $+, \cdot, 0, 1$ をそれぞれ $\cdot, +, 1, 0$ に入れ替えて作った $(A, \cdot, +, -, 1, 0)((\mathcal{A})_d$ とする) 用の公理系を $(T)_d$ とします。
このとき,

「公理系 T で ψ が証明可能」$\Rightarrow$「公理系 $(T)_d$ で ψ_d が証明可能」(*)

であることがわかります (これは厳密にやろうとすると, 数理論理学の枠組みで, 証明の長さによる帰納法で証明すべきしろものです。
でも, これはそれほど厳密にやらなくてもわかりますから, 普通, 証明は省略しているのです。
これはだいたい命題 5 から推測できます。
) ((*) の仮定は $\mathcal{A}$ で, 結論は $(\mathcal{A})_d$ で考えていることに注意.) また, $(T)_d$ は $\mathcal{A}$ からみれば T と同じ公理系であり, ψ_d を $\mathcal{A}$ の関係式とみて, (また厳密にいえば, 証明の長さによる帰納法によって)

「公理系 $(T)_d$ で ψ_d が証明可能」⇒「公理系 T で ψ_d が証明可能」(**)

がいえる. ((**) の仮定は $(\mathcal{A})_d$ で, 結論は $\mathcal{A}$ で考えていることに注意.)
従って,(*) と (**) から

「公理系 T で ψ が証明可能」⇒「公理系 T で ψ_d が証明可能」

が成立する.

もっと一般に, 式に限らず, 文 (命題) についても双対の原理は成り立ちます。
上の式に関することも文 (命題) として取り扱うことができるので (例えば,「 $x \cdot x = x$ が成立する.」等), もう一度, 一般的な形で述べておきます。

(ブール代数における双対の原理) ψ が全てのブール代数で成立する命題ならば, その双対命題 ψ_d も全てのブール代数で成立する.

[証明]　例によって, 証明のスケッチです。
ブール代数 $\mathcal{A} = (A, +, \cdot, -, 0, 1)$ について, そこから, $+, \cdot, 0, 1$ をそれぞれ $\cdot, +, 1, 0$ に入れ替えて作ったブール代数を $(\mathcal{A})_d = (A, \cdot, +, -, 1, 0)$ とする (命題 5 より). 同じやり方で $(\mathcal{A})_d$ から, ブール代数 $((\mathcal{A})_d)_d =< A, +, \cdot, -, 0, 1 >$ を作ると, $((\mathcal{A})_d)_d$ は $\mathcal{A}$ と等しくなる. さらに (何らかの帰納法により),「 ψ が $\mathcal{A}$ で成立する」と,「 ψ_d が $(\mathcal{A})_d$ で成立する」は同値であることがわかる. ここで, ψ が全てのブール代数で成立する命題と仮定する.
任意のブール代数 $\mathcal{A}$ について, 仮定から ψ が $(\mathcal{A})_d$ で成立する. 従って, ψ_d が $((\mathcal{A})_d)_d$ で成立する. これは, ψ_d が $\mathcal{A}$ で成立することを意味する.
[証明のスケッチ終わり]
上の双対命題 ψ_d というのは, ψ からその中に含まれる全ての $+, \cdot, 0, 1$ をそれぞれ $\cdot, +, 1, 0$ で置き換えて作った命題です。

ブール代数における双対の原理を言い換えれば,(ブール代数における双対の原理)「命題 ψ がブール代数についての定理ならば, その双対命題 ψ_d もブール代数についての定理である.」ということもできます。

双対の原理を適用するにあたって, 少し注意することを述べます。
例えば, $x \cdot y \leq x + y$ は全てのブール代数について成立します (記号は適当に変えて.
ところが, これに双対の原理を直接適用して, $x + y \leq x \cdot y$ は間違いです。
$x + y \leq x \cdot y$ は一般には成立しません. というのは, $\leq$ は略号なので, $x \cdot y \leq x + y$ というのは $x \cdot y + (x + y) = x + y$ の略記です。

従って, 双対の原理を正しく適用した結果は, $(x+y)\cdot(x\cdot y)=x\cdot y$ です。
これは, 一般的に成立するブール代数の式 (定理) です。
ですから, 双対の原理は適用する前に略記等がその命題か式に含まれていれば, それをもとの形に直してから適用しなければなりません. ちょっと注意が必要ですね.

1.8 基本的な命題

前節までに, ブール代数の初等算術とも言うべき色々な定理を証明していただきました (ここで, 定理とはブール代数において証明された式のこと.).
まずそれを数字が前後しますが, 命題 6 (その 1) として証明付きでまとめておきましょう. (演習等で証明された方も, もう一度復習をかねて目を通しておいてください. やり方等, 参考になるでしょう.) 命題 6(その 1) の内容は, 今後, 特にことわらず自由に用いることにします。

[命題 **6**] (その 1)

1. $x+x=x$; (べき等律)
2. $x\cdot x=x$; (べき等律)
3. $x\leq x$; (反射律)
4. $(x\leq y\ and\ y\leq x)\Rightarrow x=y$; (反対称律)
5. $(x\leq y\ and\ y\leq z)\Rightarrow x\leq z$; (推移律)
6. $x\leq y\Leftrightarrow x\cdot y=x$;
7. $x\cdot 0=0$;
8. $x\cdot 1=x$;
9. $x+0=x$;
10. $x+1=1$;
11. $x\leq y\Leftrightarrow x\cdot -y=0$;
12. $x=-y\Leftrightarrow(x+y=1\ and\ x\cdot y=0)$; (補元の一意性)
13. $--x=x$; (二重否定の法則)
14. $-(x+y)=-x\cdot -y$; (ド・モルガンの法則)
15. $-(x\cdot y)=-x+-y$; (ド・モルガンの法則)
16. $0\leq x\leq 1$;
17. $(x\leq z\ and\ y\leq z)\Rightarrow x+y\leq z$;
18. $(x\leq y\ and\ y\leq z)\Rightarrow x\leq y\cdot z$.

(命題 6(その 1) 終わり)

[命題 **6**] (その 1) の証明

1.

$$\begin{aligned} x &= x \cdot x + x \quad \text{定義 } 3(2)() \\ &= x + x \cdot x \quad \text{定義 } 3(2)() \\ &= (x + x) \cdot (x + x) \quad \text{定義 } 3(2)() \\ &= x \cdot (x + x) + x \cdot (x + x) \quad \text{定義 } 3(2)() \\ &= (x + x) \cdot x + (x + x) \cdot x \quad \text{定義 } 3(2)() \\ &= x + x \quad \text{定義 } 3(2)() \end{aligned}$$

2. 双対の原理を (1) に適用して, $x \cdot x = x$.
3. (1) から, 定義により $x \leq x$.
4. $x \leq y$ と $y \leq x$ を仮定する. $\leq$ の定義から, 定義 3(2)(i) によって, $y = x + y = y + x = x$.
5. $x \leq y$ と $y \leq z$ を仮定する. $\leq$ の定義から, $x + y = y, y + z = z$. 従って, 結合律 (定義 3(2)(ii)) を用いて,

$$x + z = x + (y + z) = (x + y) + z = y + z = z$$

がいえる. すなわち, $x \leq z$ を得る.

6. $(\Rightarrow) x \leq y$ を仮定する. $\leq$ の定義から, $x + y = y$. 定義 3(2)(iii) から, $x \cdot y = x \cdot (x + y) = x$.
($\Rightarrow$ の逆) 今上で, $x + y = y \Rightarrow x \cdot y = x$ を証明した. これに双対の原理を適用すると, $x \cdot y = y \Rightarrow x + y = x$ を得る. ここで, x, y を置き換えると, $y \cdot x = x \Rightarrow y + x = y$. これはすなわち, $x \cdot y = x \Rightarrow x \leq y$ である.
7.

$$\begin{aligned} x \cdot 0 &= x \cdot (x \cdot -x) \quad \text{定義 } 3(2)(v) \\ &= (x \cdot x) \cdot -x \quad \text{定義 } 3(2)(ii) \\ &= x \cdot -x = 0 \quad (2) \text{ と定義 } 3(2)(v) \end{aligned}$$

8.

$$x \cdot 1 = x \cdot (x + -x) \quad \text{定義 } 3(2)(v)$$

$$
\begin{aligned}
&= (-x+x)\cdot x \quad \text{定義 } 3(2)(i)\\
&= x \quad \text{定義 } 3(2)(iii)
\end{aligned}
$$

9. 双対の原理を (8) に適用して $x+0=x$.
10. 双対の原理を (7) に適用して $x+1=1$.
11. $(\Rightarrow) x \le y$ を仮定する.(6) から, $x\cdot y = x$. これを用いて,

$$
\begin{aligned}
x\cdot(-y) &= (x\cdot y)\cdot(-y)\\
&= x\cdot(y\cdot -y) \quad \text{定義 } 3(2)(ii)\\
&= x\cdot 0 = 0 \quad (7) \text{ と定義 } 3(2)(v)
\end{aligned}
$$

$(\Rightarrow$ の逆$) x\cdot -y = 0$ を仮定する. すると,

$$
\begin{aligned}
x\cdot y &= x\cdot y + 0 \quad (9)\\
&= x\cdot y + x\cdot -y \text{ 仮定}\\
&= x\cdot(y+-y) \quad \text{定義 } 3(2)(iv)\\
&= x\cdot 1 = x \quad (8) \text{ と定義 } 3(2)(v)
\end{aligned}
$$

がいえる.(4) から, $x \le y$ が成立する.

12. $(\Rightarrow) x = -y$ を仮定する. これと定義 3(2)(i) と (v) から, $x+y = -y+y = y+-y = 0$ がいえる. また同様に, 定義 3(2)(i) と (v) から, $x\cdot y = -y\cdot y = y\cdot -y = 1$ がいえる.
$(\Rightarrow$ の逆$) x+y=1$ と $x\cdot y = 0$ を仮定する. そのとき,

$$
\begin{aligned}
x &= x\cdot 1 \quad (8)\\
&= x\cdot(y+-y) \quad \text{定義 } 3(2)(v)\\
&= x\cdot y + x\cdot -y \quad \text{定義 } 3(2)(iv)\\
&= 0 + x\cdot -y \quad \text{仮定}\\
&= x\cdot -y + 0 \quad \text{定義 } 3(2)(i)\\
&= x\cdot -y + y\cdot -y \quad \text{定義 } 3(2)(v)\\
&= (x+y)\cdot -y \quad \text{定義 } 3(2)(i) \text{ と } (v)\\
&= 1\cdot -y \quad \text{仮定}\\
&= -y \quad (8) \text{ と定義 } 3(2)(i)
\end{aligned}
$$

13. 定義 3(2)(v) と (12) から, $--x=x$ を得る.
14. まず,

$$\begin{aligned} x+y+-x\cdot -y &= x+(x+-x)\cdot y+-x\cdot -y \quad \text{定義 } 3(2)(iii) \\ &= x+x\cdot y+-x\cdot y+-x\cdot -y \quad \text{定義 } 3(2)(i) \text{ と } (iv) \\ &= x+-x\cdot (y+-y) \quad \text{定義 } 3(2)(iii) \text{ と } (iv) \\ &= x+-x \quad (8) \text{ と定義 } 3(2)(v) \\ &= 1 \quad \text{定義 } 3(2)(v) \end{aligned}$$

$$\begin{aligned} (x+y)\cdot -x\cdot -y &= x\cdot -x\cdot -y+y\cdot -x\cdot -y \quad \text{定義 } 3(2)(i) \text{ と } (iv) \\ &= 0\cdot -y+0\cdot -x \quad \text{定義 } 3(2)(ii) \text{ と } (iv) \\ &= 0+0 \quad (7) \text{ と定義 } 3(2)(i) \\ &= 0 \quad (9) \end{aligned}$$

がいえる. 上の 2 式に (12) を適用して, ド・モルガンの法則 $-(x+y)=-x\cdot -y$ が成立する.
15. 双対の原理を (14) のド・モルガンの法則に適用して, もう一つのド・モルガンの法則 $-(x\cdot y)=-x+-y$ を得る.
16. (9) と定義 3(2)(i) から, $0\leq x$ がいえる.(10) から, $x\leq 1$. 従って, $0\leq x\leq 1$.
17. $x\leq z$ と $y\leq z$ を仮定する. $\leq$ の定義から, $x+z=z, y+z=z$. 従って, 結合律 (定義 3(2)(ii)) を用いて,

$$(x+y)+z=x+(y+z)=x+z=z$$

がいえる. これが証明すべきことであった.
18. $x\leq y$ と $x\leq z$ を仮定する.(6) から, $x\cdot y=x, x\cdot z=x$. 従って, これを用いて結合律 (定義 3(2)(ii)) から,

$$x\cdot (y\cdot z)=(x\cdot y)\cdot z=x\cdot z=z$$

がいえる. これが証明すべきことであった.(注:(18) は (17) に双対の原理を適用して導くこともできる)

[命題 6(その 1) の証明終わり]

もう少し, ブール代数の初等的な性質を見てみましょう.

[命題 **6**] (その 2)

1. $x \leq x + y, y \leq x + y$;
2. $x \cdot y \leq x, x \cdot y \leq y$;
3. $x \leq y \Rightarrow x \cdot a \leq y \cdot a$;
4. $x \leq y \Rightarrow x + a \leq y + a$;
5. $-x \leq y \Leftrightarrow x + y = 1$;
6. $x \leq -y \Leftrightarrow x \cdot y = 0$;
7. $-0 = 1, -1 = 0$;
8. $x \leq y \Rightarrow -y \leq -x$.

(命題 6(その 2) 終わり)

[命題 **6**] (その 2) の証明
(演習 10) を参照.

[命題 6(その 2) の証明終わり]

少し, ウォーミングアップをしましょう.

(演習 10) 命題 6(その 2) を証明しなさい.

(演習 10 の終わり)

さて, ブール代数は束論 (lattice theory) の方から特徴付けできます。
つまり, ブール代数は相補的な分配束として定義することができます。
それについて少し触れておきましょう. 少し長い準備が必要です。
この節はその準備で終わってしまいます。
次節で, ブール代数を相補的な分配束として定義しましょう. まず, 束を定義したいのですが, そのために半順序の概念が必要です。
(順序に関して, 定義が分散すると嫌なので, 下でかなりまとまって書いてしまいます。
そのため, 順序について慣れていない方はつらいと思います。
しかし, これ以後 (できれば次回も), 逐次演習など入れていきますのでだんだんに慣れていってください.)

半順序集合 ((partially ordered set, 略してよく poset (ポーセットと読む) といわれる) とは, 集合 P と次の (1) $\sim$ (3) を満足する P 上の 2 項関係 $\leq$ の組 $(P, \leq)$ のことです: 任意の $x, y, z \in P$ について,

1. $x \leq x$; (反射律)

2. $(x \leq y \ and \ y \leq x) \Rightarrow x = y$; (反対称律)
3. $(x \leq y \ and \ y \leq z) \Rightarrow x \leq z$. (推移律)

このとき, $\leq$ は順序関係 (order relation), 特に (P 上の)(半) 順序 ((partial) order) といいます。

P が空集合のときも定義できるものとします。
また, 明らかに混乱が起きない場合,($P, \leq$) を単に P と書きます。
P を集合を要素とする集合とすると, 集合間の包含関係 $\subseteq$ は明らかに順序関係となり, $(P, \subseteq)$ は半順序集合です。
また, $x \leq y$ を $y \geq x$ とも書くことにします。

この定義から, 命題 6(その 1) によって, ブール代数 A で定義された $\leq$ に関して, $(A, \leq)$ は半順序集合になります。
任意の集合 X について, $(P(X), \subseteq)$ も半順序集合です。

$(P, \leq)$ を半順序集合とします。
Q を P の部分集合とします。
このとき, $\leq'$ を $\leq$ を Q 上で考えたものとすれば, $(P, \leq')$ は半順序集合になります。
この $(P, \leq')$ を単に, $(Q, \leq)$ で表すことにします。
$(Q, \leq)$ は $(P, \leq)$ の部分半順序集合といいます。

B をブール代数 $\mathcal{A}$ の部分宇宙とします。
A で定義された $\leq$ に関して, $(B, \leq)$ は $(A, \leq)$ の部分半順序集合になります。

$(P, \leq)$ を半順序集合とします。
P の要素 a は全ての $x \in P$ について, $x \leq a$ となるとき, 最大元といいます。
同様に, P の要素 a は全ての $x \in P$ について, $a \leq x$ となるとき, 最小元といいます。
P は常に最大元または最小元を持つとは限りません.
P の最大元が存在するときはそれを 1 で, 最小元が存在するときはそれを 0 で表します。

(演習 11)　1. 半順序集合とみたブール代数では最大元, 最小元は存在します

か? もし存在するならば, それは何ですか?

2. 最小元を持つが, 最大元を持たない半順序集合の例を挙げなさい.
3. 最大元を持つが, 最小元を持たない半順序集合の例を挙げなさい.
4. 最大元も, 最小元も持たない半順序集合の例を挙げなさい.
5. 最大元 (最小元) が存在するとき, その一意性を証明しなさい.

(演習 11 の終わり)

半順序集合 $(P, \leq)$ の, 元 x, y は, $(x \leq y \ or \ y \leq x)$ がいえるとき, 比較可能であるといいます。
P の部分集合 C は, C の全ての 2 つの元が比較可能なとき, 連鎖 (または, 鎖)(chain) といいます。
P 自身が連鎖のとき, $(P, \leq)$ を全順序集合 (totally ordered set), あるいは, 線形順序集合 (linearly ordered set) といいます。
そのとき, $\leq$ は (P 上の) 全順序 (total order), あるいは線形順序 (linear order) といいます。

任意の要素 $x, y \in P$ について, $x \leq y$ または $y \leq x$ のいずれかが成り立つとき, $(P, \leq)$ を全順序集合であるというわけです。
「任意の要素 $x, y \in P$ について, $x \leq y$ または $y \leq x$ のいずれかが成り立つ」というところは, 「任意の要素 $x, y \in P$ について, $(x < y \ or \ x = y \ or \ y < x)$」といってもかまいません.
ここで, $x < y$ は $(x \leq y \ and \ x \neq y)$ によって定義されます。
上と同様, $x < y$ を $y > x$ とも書くことにします。

実数全体の集合, 有理数全体の集合, 整数全体の集合などは, 普通の順序で考えて全順序集合です。

(演習 12) 全順序集合でない半順序集合の例を挙げなさい.

(演習 12 の終わり)

M を半順序集合 P の部分集合とします。
P の要素 s は, 全ての $m \in M$ について, $m \leq s (s \leq m)$ を満足するとき, M の上界 (下界) と呼ばれ, $M \leq s (s \leq M)$ と書きます。
M に上界 (下界) が存在するとき, M は上に (下に) 有界であるといいます。
M は上界を持たないこともあるし, 無限個の上界を持つこともあります。

これは下界についても同様です。
特に, s が最小の上界 (最大の下界) であるとき, M の上限 (下限) といいます。
それらの英語は, 上界 (upper bound), 下界 (lower bound), 上限 (supremum), 下限 (infinimum) です。

M の上限 (下限) であるとき, $s = \Sigma M (s = \Pi M)$ (Π は π の大文字) で表します。
$s = \Sigma M (s = \Pi M)$ を, $s = \sup M$ や $s = \cup M (s = \inf M$ や $s = \cap M)$ で表すことも多いです。

(演習 13) 上限 (下限) は存在すれば, 一意的に決まることを証明しなさい.

(演習 13 の終わり)

(演習 14) Nat を自然数全体の集合とします。
Fin を Nat の有限部分集合の全体とします。
$Cofin+$ を Nat の部分集合 E で, E または $Nat \sim E$ が有限になるもの全体の集合とします。
さらに, $FinEven$ を Nat の有限部分集合で偶数のみからなる集合全体の集合とします。
このとき, 半順序集合 $(P(Nat), \subseteq)$ とその部分半順序集合 $(Fin, \subseteq)$, $(Cofin+, \subseteq)$, $(FinEven, \subseteq)$ を考えます。
$FinEven \subseteq Fin \subseteq Cofin+ \subseteq P(Nat)$ は明らかです。
このとき,

1. $FinEven$ は $(Fin, \subseteq)$ では上界を持たないが, $(Cofin+, \subseteq)$ では無限個の上界を持つことを確かめなさい.
2. また, $(P(Nat), \subseteq)$ では, 偶数全体の集合が $FinEven$ の上限になっていることを確かめなさい.

(演習 14 の終わり)

半順序集合 P の要素 (元) m が, $m < x$ となる $x \in P$ が存在しないとき,P の極大元といいます。
同様に, P の要素 (元) m が $m > x$ となる $\mathrm{x} \in P$ が存在しないとき, P の極小元といいます。
極大元 (極小元) はないこともありますし,1 つあるいは複数個あることも

あります。
P が最大元 (最小元) を持つとき, それはただ一つの極大元 (極小元) となります。

ちょっと寄り道ですが, 半順序集合 P が帰納的順序集合 (inductively ordered set) であるとは, $P \neq 0$ であって, P の任意の空でない全順序部分集合 (=連鎖) が上に有界である (上界が存在する) であることをいいます。

ここで, 数学の証明に良く用いる有名な $Zorn$ (ツォルン) の補題を紹介しましょう. それは, 「半順序集合 P が帰納的順序集合ならば, P は極大元を持つ.」です。
これは集合論の選択公理と同値になります。
選択公理とは, 集合論の悩ましい (?) 公理で,「2 つずつ互いに素な空でない集合からなる集合 A が与えられているとき, 次の条件を満たす集合 S が存在する:任意の $X \in A$ について, $S \cap X = \{Y\}$ となる集合 Y が存在する.」というものです。
選択公理には色々なバージョンがあります。
選択公理は証明するときの良い道具になるのですが, 悩ましいというのは, これから, 常識外のことが導き出せるからです。
たとえば, 球を適当に分割してまた寄せ集めると, 元の球と全く同じ球を 2 つ作れるという, バナッハ・タルスキーのパラドックスが選択公理から証明できます。
これについては,
砂田利一著「バナッハ・タルスキーのパラドックス」岩波書店　1997 年という本があります。
砂田さんは数学者として著名な方です。
たしか, 志賀浩二著「無限からの光芒ポーランド学派の数学者達」日本評論社　1988 年
にも, その記述があったように記憶しています。
はっきり記憶していませんが. 志賀さんも数学者として著名な方です。
上の 2 冊とも昔, 書店でパラパラと見ただけなので本当に推薦すべき書物かどうかはわかりません.
著名な方が書いておられるので大丈夫だとは思います。
洋書でも, バナッハ・タルスキーのパラドックスのみについて書かれたものを見たことがあります。
Banach-Tarski Pradox というタイトルだったかな. 忘れました.

選択公理については,(真打登場!) 田中尚夫さんの, 田中尚夫著「選択公理と数学 (増補版)」遊星社　1999 年
に詳しい記述があります。
また, 選択公理のみを扱った数理論理学の専門書 (洋書) (The Axiom of Choice) が North-Holland 社から 2 冊出ています。
田中さんの本はまたしてもお薦めです。
我々のブール代数とも関係があります。
機会があれば見てみてください.(田中さんの本にもバナッハ・タルスキーのパラドックスが, 今述べたものとはすこし異なるかたちで載っています。
)

このセミナーでも, 近い将来, ツォルンの補題を用いて重要な定理を証明します。
さて, 寄り道から本道に戻りましょう.
半順序集合 $(L, \leq)$ において, 任意の 2 元 $x, y \in L$ について, 集合 $\{x, y\}$ の上限および下限が (L の中で) 存在するとき, L を束 (lattice) といいます。
空集合 0, あるいはただ一つの要素からなる半順序集合もそれぞれ束をなします。
特に後者を単位束といいます。
$\{x, y\}$ の上限, 下限をそれぞれ, $x + y, x \cdot y$ と表します。
$+$と $\cdot$ の替わりに, それぞれ, $\cup$ と $\cap$ とか, $\vee$ と $\wedge$ を使うことも多いです。
束に関しても, 双対の原理が成り立ちます。
(注: $x \leq y$ の双対命題は, $y \leq x$ です。)

任意の集合 X について, $(P(X), \subseteq)$ は束になります。

$$x + y = x \cup y, x \cdot y = x \cap y$$

が成立します。
また, 任意の $M \subseteq P(X)$ について,

$$\Sigma M = \cup M, \Pi M = \cap M$$

が成立します。

(演習 15) K を体とし, V を K 上の線形空間とする. L を V の部分空間全体の集合とする.

(線形空間, 線形空間の部分空間の説明は省略します。)
このとき,

1. $(L, \subseteq)$ は束になることを証明しなさい.
2. 任意の $M \subseteq L$ について, $\Pi M = \cap M$ となることを証明しなさい.
3. 任意の $M \subseteq L$ について, ΣM は $\cup M$ によって生成された部分空間となることを証明しなさい.

(演習 15 の終わり)
次節では, ブール代数が相補的な分配束と定義されること, および, ブール代数における大切な定理や, 準同型写像, 同型写像を中心に進めていきます。

1.9 演習 3

(1) 集合の体は定義 1 で定義されたのですが, 集合の体を定義 1 とは異なる仕方で定義できますか？

$\cup$ と $\cap$ の双対性を使って例えば

「集合の体 (field of sets) A とは, 次の性質 (1)-(3) を満たす集合である: (1) $\cup A \in A$ (2) 任意の $X \in A$ について, $\cup A \sim X \in A$ (3) 任意の $X, Y \in A$ について, $X \cap Y \in A$ 」

(2) 空でない集合 X が与えられたとします. この X から集合の体を作れますか？

$A = \{0, X\}$ はその例の一つです。

$\cup A = 0 \cup X = X$ なので, $\cup A \in A$ で定義の条件 (1) が充たされ　$\cup A \sim X = X \sim X = 0 \in A$ と $\cup A \sim 0 = X \sim 0 = X \in A$ により条件 (2) が $0 \cup 0 = 0 \in A, 0 \cup X = X \in A, X \cup 0 = X \in A, X \cup X = X \in A$ から条件 (3) が充たされています.

(3)-I (a) $A \cap (B \sim C) = (A \cap B) \sim C$;

[方法 1] 記号論理の規則は既知なものとします。

x を任意にとると：

$$\begin{aligned} x \in A \cap (B \sim C) &\Leftrightarrow x \in A \; and \; x \in (B \sim C) \\ &\Leftrightarrow x \in A \; and \; (x \in B \; and \; not(x \in C)) \\ &\Leftrightarrow (x \in A \; and \; x \in B) \; and \; not(x \in C) \\ &\Leftrightarrow x \in A \cap B \; and \; not(x \in C) \end{aligned}$$

$$\Leftrightarrow \quad x \in (A \cap B) \sim C$$

x は任意にとったから

$$(\forall x)(x \in A \cap (B \sim C) \Leftrightarrow x \in (A \cap B) \sim C)$$

よって

$$A \cap (B \sim C) = (A \cap B) \sim C$$

[方法 2] $\cap$ と $\cup$ と補集合 c の集合演算は既知としてよいならただし, 補集合は A, B, C を部分集合としてふくむ含適当な集合上での補集合をとるものとして

$$\begin{aligned} A \cap (B \sim C) &= A \cap (B \cap C_c) \\ &= (A \cap B) \cap C^c \\ &= (A \cap B) \sim C \end{aligned}$$

以下、取り合えず [方法 1] のようにします.

(b) $(A \cup B) \sim C = (A \sim C) \cup (B \sim C)$;
x を任意にとると：

$$\begin{aligned} x \in (A \cup B) \sim C \quad &\Leftrightarrow \quad x \in (A \cup B) \ and \ notx \in C \\ &\Leftrightarrow \quad (x \in A \ or \ x \in B) \ and \ not \ x \in C \\ &\Leftrightarrow \quad (x \in A \ and \ not \ x \in C) \\ &\qquad \ or \ (x \in B \ and \ not \ x \in C) \\ &\Leftrightarrow \quad x \in (A \sim C) \ or \ x \in (B \sim C) \\ &\Leftrightarrow \quad x \in (A \sim C) \cup (B \sim C) \end{aligned}$$

x は任意にとったから

$$(\forall x)(x \in (A \cup B) \sim C \Leftrightarrow x \in (A \sim C) \cup (B \sim C))$$

よって

$$(A \cup B) \sim C = (A \sim C) \cup (B \sim C)$$

(c) $A \sim (B \cup C) = (A \sim B) \cap (A \sim C)$;

x を任意にとると：

$$
\begin{aligned}
& x \in A \sim (B \cup C) \\
& \quad \Leftrightarrow x \in A \ and \ not \ (x \in B \cup C) \\
& \quad \Leftrightarrow x \in A \ and \ not \ (x \in B \ or \ x \in C) \\
& \quad \Leftrightarrow x \in A \ and \ (not \ x \in B \ and \ not \ x \in C) \\
& \quad \Leftrightarrow x \in A \ and \ not \ x \in B \ and \ x \in A \ and \ not \ x \in C \\
& \quad \Leftrightarrow x \in (A \sim B) \ and \ x \in (A \sim C) \\
& \quad \Leftrightarrow x \in (A \sim B) \cap (A \sim C)
\end{aligned}
$$

x は任意にとったから

$$(\forall x)(x \in A \sim (B \cup C) \Leftrightarrow x \in (A \sim B) \cap (A \sim C))$$

よって

$$A \sim (B \cup C) = (A \sim B) \cap (A \sim C)$$

(d) $A \sim (B \cap C) = (A \sim B) \cup (A \sim C)$;
x を任意にとると:

$$
\begin{aligned}
& x \in A \sim (B \cap C) \\
& \quad \Leftrightarrow x \in A \ and \ not \ (x \in B \cap C) \\
& \quad \Leftrightarrow x \in A \ and \ not \ (x \in B \ and \ x \in C) \\
& \quad \Leftrightarrow x \in A \ and \ (\ not \ x \in Bor \ not \ x \in C) \\
& \quad \Leftrightarrow (x \in A \ and \ not \ x \in B) \ or \ (x \in A \ and \ not \ x \in C) \\
& \quad \Leftrightarrow x \in (A \sim B) \ or \ x \in (A \sim C) \\
& \quad \Leftrightarrow x \in (A \sim B) \cup (A \sim C)
\end{aligned}
$$

x は任意にとったから

$$(\forall x)(x \in A \sim (B \cap C) \Leftrightarrow x \in (A \sim B) \cup (A \sim C))$$

よって

$$A \sim (B \cap C) = (A \sim C) \cup (B \sim C)$$

(e) $A \sim (A \sim B) = A \cap B$;
x を任意にとると:

$$
\begin{aligned}
& x \in A \sim (A \sim B) \\
& \quad \Leftrightarrow x \in A \ and \ not \ (x \in A \sim B) \\
& \quad \Leftrightarrow x \in A \ and \ not \ (x \in A \ and \ not \ x \in B) \\
& \quad \Leftrightarrow x \in A \ and \ (not \ x \in A \ or \ x \in B) \\
& \quad \Leftrightarrow x \in A \ and \ not \ x \in A \ or \ x \in A \ and \ x \in B \\
& \quad \Leftrightarrow x \in A \ and \ x \in B \\
& \quad \Leftrightarrow x \in A \cap B
\end{aligned}
$$

x は任意にとったから

$$(\forall x)(x \in A \sim (A \sim B) \Leftrightarrow x \in A \cap B)$$

よって

$$A \sim (A \sim B) = A \cap B$$

(f) $A \cup (B \sim A) = A \cup B$;
x を任意にとると:

$$
\begin{aligned}
& x \in A \cup (B \sim A) \\
& \quad \Leftrightarrow x \in A \ or \ (x \in B \sim A) \\
& \quad \Leftrightarrow x \in A \ or \ (x \in B \ and \ not \ x \in A) \\
& \quad \Leftrightarrow (x \in A \ or \ x \in B) \ and \ (x \in A \ or \ not \ x \in A) \\
& \quad \Leftrightarrow x \in A \ or \ x \in B \\
& \quad \Leftrightarrow x \in A \cup B
\end{aligned}
$$

x は任意にとったから

$$(\forall x)(x \in A \cup (B \sim A) \Leftrightarrow x \in A \cup B)$$

よって

$$A \cup (B \sim A) = A \cup B;$$

(g) $A \cap B^c = 0 \Leftrightarrow A \subseteq B$;

[証明] 以下で, 補集合は A, B を含むある集合 X について考えることにします.

$A \cap B^c = 0$

$\Leftrightarrow$ 任意の $x \in X$ について, $not\ (x \in A\ and\ notx \in B)$

$\Leftrightarrow$ 任意の $x \in X$ について, $(x \in A \Rightarrow x \in B)$

$\Leftrightarrow A \subseteq B$

または以下による.

右辺を仮定すれば $B^c \subseteq A_c$ により

$$A \cap B^c \subseteq A \cap A_c = 0$$

また $0 \subseteq A \cap B_c$ は常に成り立っているから

$$A \cap B^c = 0$$

左辺を仮定すれば
$A^c \supseteq B_c$ より $A^c \subseteq B_c$
すなわち $A \subseteq B$

(h) $(A \sim B)^c = A^c \cup B$;

x を任意にとると：

$$\begin{aligned} x \in (A \sim B)^c &\Leftrightarrow not\ (x \in A \sim B) \\ &\Leftrightarrow not\ (x \in A\ and\ not\ x \in B) \\ &\Leftrightarrow not\ x \in A\ or\ x \in B) \\ &\Leftrightarrow x \in A^c\ or\ x \in B \\ &\Leftrightarrow x \in A^c \cup B \end{aligned}$$

x は任意にとったから

$$(\forall x)(x \in (A \sim B)^c \Leftrightarrow x \in A^c \cup B)$$

よって

$$(A \sim B)^c = Ac \cup B;$$

(i) $(A \cap B = 0\ and\ A \cup B = C) \Rightarrow A = C \sim B.$
$(A \cap B = 0\ and\ A \cup B = C)$ を仮定し x を任意にとると：

$$\begin{aligned} x \in A &\Rightarrow x \in A \cup B (A \subseteq A \cup B) \\ &\Rightarrow x \in C (A \cup B = C) \end{aligned}$$

また

$$x \in A \Rightarrow\ not\ x \in B (A \cap B = 0)$$

よって

$$\begin{aligned} x \in A &\Rightarrow x \in C\ and\ not\ x \in B \\ &\Rightarrow x \in C \sim B \end{aligned}$$

逆に,

$$\begin{aligned} & x \in C \sim B \\ & \Rightarrow x \in C\ and\ not\ x \in B \\ & \Rightarrow x \in A \cup B\ and\ not\ x \in B \\ & \Rightarrow (x \in A\ or\ x \in B)\ and\ not\ x \in B \\ & \Rightarrow (x \in A\ and\ not\ x \in B)\ or\ (x \in B\ and\ not\ x \in B) \\ & \Rightarrow x \in A \end{aligned}$$

x は任意にとったから

$$(\forall x)(x \in C \sim B \Leftrightarrow x \in A)$$

よって

$$C \sim B = A$$

これは $(A \cap B = 0\ and\ A \cup B = C)$ を仮定して得られたから

$$(A \cap B = 0\ and\ A \cup B = C) \Rightarrow A = C \sim B.$$

(3)-II $A\mathbf{\Delta}B = (A \sim B) \cup (B \sim A)$ を対称差といいます. 論理回路をやった方は EX-OR(排他的論理和) に対応するものです. (f) で $A\mathbf{\Delta}B$ がどういうものかよくわかりますね. この $\mathbf{\Delta}$ の挙動をみて, あれっと思いませんか？

(a) $A\mathbf{\Delta}B = B\mathbf{\Delta}A$;

$A\mathbf{\Delta}B = (A \sim B) \cup (B \sim A) = (B \sim A) \cup (A \sim B) = B\mathbf{\Delta}A$ #∪は交換可能

(b) $(A\mathbf{\Delta}B)\mathbf{\Delta}C = A\mathbf{\Delta}(B\mathbf{\Delta}C)$;

$$\begin{aligned}
&(A\mathbf{\Delta}B)\mathbf{\Delta}C \\
&\quad = ((A \sim B) \cup (B \sim A))\mathbf{\Delta}C \\
&\quad = ((A \sim B) \cup (B \sim A)) \sim C \\
&\quad \cup C \sim ((A \sim B) \cup (B \sim A))
\end{aligned}$$

以後根気良く計算をすれば

$= (A \cap B \cap C) \cup (A \cap B^c \cap C_c) \cup (A^c \cap B \cap C_c) \cup (A^c \cap B^c \cap C)$

また

$$\begin{aligned}
&A\mathbf{\Delta}(B\mathbf{\Delta}C) \\
&\quad = (A \cap B \cap C) \cup (A \cap B^c \cap C_c) \cup (A^c \cap B \cap C_c) \cup (A^c \cap B^c \cap C)
\end{aligned}$$

よって

$$(A\mathbf{\Delta}B)\mathbf{\Delta}C = A\mathbf{\Delta}(B\mathbf{\Delta}C)$$

[別解]： 下の (f) $A\mathbf{\Delta}B = (A \cup B) \sim (A \cap B)$. を用いて

$$\begin{aligned}
&(A\mathbf{\Delta}B)\mathbf{\Delta}C \\
&\quad = (A\mathbf{\Delta}B) \cup C \sim \{(A\mathbf{\Delta}B) \cap C\} \\
&\quad = \{(A \cup B) \sim (A \cap B)\} \cup C \sim \{(A\mathbf{\Delta}B) \cap C\} \\
&\quad = \{(A \cup B) \cap (A^c \cup B_c)\} \cup C \sim \{(A\mathbf{\Delta}B) \cap C\} \\
&\quad = \{(A \cup B \cup C) \cap (A^c \cup B^c \cup C) \sim \{(A\mathbf{\Delta}B) \cap C\} \quad (*1)
\end{aligned}$$

$$
\begin{aligned}
&\{(A\mathbf{\Delta}B)\cap C\}\\
&\quad=\{A\cap C\mathbf{\Delta}B\cap C\}\\
&\quad=\{A\cap C\mathbf{\Delta}B\cap C\}\\
&\quad=\{A\cap C\sim B\cap C\}\cup\{B\cap C\sim A\cap C\}\\
&\quad=\{A\cap C\cap B^c\cup C^c\}\cup\{B\cap C\cap A^c\cup C^c\}\\
&\quad=\{A\cap C\cap B^c\}\cup\{B\cap C\cap A^c\}\qquad(*2)
\end{aligned}
$$

(*1)(*2) から

$$
\begin{aligned}
&(A\mathbf{\Delta}B)\mathbf{\Delta}C\\
&\quad=(A\cup B\cup C)\cap(A\cup B^c\cup C_c)\\
&\qquad\cap(A^c\cup B\cup C_0)\cap(A^c\cup B^c\cup C)
\end{aligned}
$$

同様に

$$
\begin{aligned}
&(A\mathbf{\Delta}B)\mathbf{\Delta}C\\
&\quad=(A\cup B\cup C)\cap(A\cup B^c\cup C_c)\\
&\qquad\cap(A^c\cup B\cup C_c)\cap(A^c\cup B^c\cup C)
\end{aligned}
$$

(c) $A\mathbf{\Delta}B=0\Leftrightarrow A=B$;
まず $A=B$ なら

$$A\mathbf{\Delta}B=(A\sim B)\cup(B\sim A)=0\cup 0=0$$

逆に　$(A\sim B)\cup(B\sim A)=A\mathbf{\Delta}B=0$ なら

$$(A\sim B)=0,(B\sim A)=0$$

となるから　$A\cup B=(A\sim B)\cup B=0\cup B=B$ より

$$A\subseteq A\cup B=B$$

となり, 同様に　$A\cup B=(B\sim A)\cup A=0\cup A=A$ より

$$
\begin{aligned}
&B\subseteq A\cup B=A\\
&A=B
\end{aligned}
$$

(d) $A\mathbf{\Delta}0 = A$;

$$A\mathbf{\Delta}0 = (A \sim 0) \cup (0 \sim A) = A \cup 0 = A$$

(e) $A \cap (B\mathbf{\Delta}C) = (A \cap B)\mathbf{\Delta}(A \cap C)$;

$$\begin{aligned} & A \cap (B\mathbf{\Delta}C) \\ & \quad = A \cap \{(B \sim C) \cup (C \sim B)\} \qquad (\mathbf{\Delta}\text{の定義}) \\ & \quad = \{A \cap (B \sim C)\} \cup \{A \cap (C \sim B)\} \qquad (\text{分配則}) \\ & \quad = \{(A \cap B) \sim C\} \cup \{(A \cap C) \sim B\} \qquad ((3) - I(a)) \end{aligned}$$

ここで (3)-I (d) より

$$\begin{aligned} (A \cap B) \sim (A \cap C) &= \{(A \cap B) \sim A\} \cup \{(A \cap B) \sim C\} \\ &= 0 \cup \{(A \cap B) \sim C\} \\ &= \{(A \cap B) \sim C\} \end{aligned}$$

$$\begin{aligned} (A \cap C) \sim (A \cap B) &= \{(A \cap C) \sim A\} \cup \{(A \cap C) \sim B\} \\ &= 0 \cup \{(A \cap C) \sim B\} \\ &= \{(A \cap C) \sim B\} \end{aligned}$$

となるので, 結局

$$\begin{aligned} & A \cap (B\mathbf{\Delta}C) \\ & \quad = \{(A \cap B) \sim (A \cap C)\} \cup \{(A \cap C) \sim (A \cap B)\} \\ & \quad = (A \cap B)\mathbf{\Delta}(A \cap C) \end{aligned}$$

(f) $A\mathbf{\Delta}B = (A \cup B) \sim (A \cap B)$.
(3-I-(d)) $A \sim (B \cap C) = (A \sim B) \cup (A \sim C)$ により

$$\begin{aligned} (A \cup B) \sim (A \cap B) &= \{(A \cup B) \sim A\} \cup \{(A \cup B) \sim B\} \\ &= (B \sim A) \cup (A \sim B) \qquad (3 - I - (f)) \\ &= A\mathbf{\Delta}B \end{aligned}$$

1.10 演習4

(1) 系 4 を証明しなさい.

『系 4 もし, A_s が集合の体ならば, $(A_s, \cup, \cap, \sim, 0, \cup A_s)$ は BA 』

[証明] 集合の体の定義と集合演算の規則によります。集合演算の規則は前節の演習でやったので全て既知とします.

(1) $A_s \neq 0. \cup A_s \in A$. また, $X, Y \in A$ なら

$$X \cup Y \in A, X \cap Y \in A, \cup A_s \sim X \in A$$

すなわち $\cup, \cap, \sim$ について閉じている.

(2) $X, Y, Z \in A$ を任意にとると,

(i) $X \cup Y = Y \cup X, X \cap Y = Y \cap X$ (交換律, 交換法則)

(ii) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$,
$X \cap (Y \cap Z) = (X \cap Y) \cap Z$ (結合律, 結合法則)

(iii) $X \cap Y \cup Y = Y, (X \cup Y) \cap Y = Y$ (吸収律, 吸収法則)

(iv) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ (分配律, 分配法則)

(v) $X \cap (UA \sim X) = 0$,
$X \cup (UA \sim X) = UA$ (補元律, 補元法則, 相補法則)

[証明終]

(2) 命題 5 を証明しなさい.

もし, $\mathcal{A} =< A, +, \cdot, -, 0, 1 >$ が BA ならば, $< A, \cdot, +, -, 1, 0 >$ もそうである.

[証明] BA の定義から自明. ただし、(2)(i) $\sim$ (v) の各式については, 第 1 式と第 2 式の順序を逆にする.

[証明終]

(3) BA で, $x + x = x, x \cdot x = x$ (べき等律),
$x \cdot 0 = 0, x \cdot 1 = x$,
$x + 0 = x, x + 1 = 1$

[証明]

$$\begin{aligned} x + x &= x + x \cdot (x + y) \quad \text{吸収律第 2 式} \\ &= x \quad \text{吸収律第 1 式} \end{aligned}$$

$$\begin{aligned} x \cdot x &= x \cdot (x + x \cdot (x \cdot y)) \quad \text{吸収律第 1 式} \\ &= x \quad \text{吸収律第 2 式} \end{aligned}$$

$$
\begin{aligned}
x \cdot 0 &= x \cdot (x \cdot -x) \quad \text{補元律第 1 式} \\
&= (x \cdot x) \cdot -x \quad \text{結合律第 2 式} \\
&= x \cdot -x \qquad \text{べき等律} \quad x \cdot x = x \\
&= 0 \quad \text{補元律第 1 式}
\end{aligned}
$$

$$
\begin{aligned}
x \cdot 1 &= x \cdot (x + -x) \quad \text{補元律第 2 式} \\
&= x \cdot x + x \cdot -x \quad \text{分配律第 2 式} \\
&= x + x \cdot -x \qquad \text{べき等律} \quad x \cdot x = x \\
&= x \quad \text{吸収律第 2 式}
\end{aligned}
$$

$$
\begin{aligned}
x + 0 &= x + x \cdot -x \quad \text{補元律第 1 式} \\
&= x \quad \text{吸収律第 2 式}
\end{aligned}
$$

$$
\begin{aligned}
x + 1 &= x + (x + -x) \quad \text{補元律第 1 式} \\
&= (x + x) + -x \quad \text{結合律第 1 式} \\
&= x + -x \qquad \text{べき等律} \quad x + x = x \\
&= 1 \quad \text{補元律第 1 式}
\end{aligned}
$$

[証明終]

(4) ブール代数において, 補元が一意的であることを証明しなさい.

$$(x \cdot y = 0 \; and \; x + y = 1) \Rightarrow y = -x$$

[証明] $x \cdot y = 0 \; and \; x + y = 1$ を仮定すると

$$
\begin{aligned}
-x &= -x \cdot 1 \qquad \text{問題 (3)} \\
&= -x \cdot (x + y) \qquad \text{仮定から} \\
&= -x \cdot x + -x \cdot y \qquad \text{分配律} \\
&= x \cdot -x + y \cdot -x \qquad \text{交換律} \\
&= 0 + y \cdot -x \qquad \text{補元律}
\end{aligned}
$$

$$
\begin{aligned}
y &= y \cdot 1 \qquad \text{問題 (3)} \\
&= y \cdot (x + -x) \qquad \text{補元律} \\
&= y \cdot x + y \cdot -x \qquad \text{分配律} \\
&= x \cdot y + y \cdot -x \qquad \text{交換律} \\
&= 0 + y \cdot -x \qquad \text{仮定から}
\end{aligned}
$$

よって $y = -x$
(証明終)

(5) ブール代数において, 0 と 1 の働きをする要素はそれぞれ 1 つしかないことを証明しなさい.

[証明] まず. A は空でないので $x \in A$ が少なくとも一つ存在する. ここで 0 と 1 の働きをする要素 0' と 1' が在ったとしても補元律より

$$0' = x \cdot -x = 0$$

$$1' = x + -x = 1$$

[証明終]

(6) BA で, 次が成り立つことを証明しなさい.

(a) $x \leq y \Leftrightarrow x \cdot y = x$;

(b) $x \leq y \Leftrightarrow x \cdot -y = 0$.

[証明] i. $x \leq y$ のとき $x + y = y$ で,

$$\begin{aligned} x \cdot y &= x \cdot (x + y) \\ &= x \cdot x + x \cdot y \quad \text{分配律} \\ &= x + x \cdot y \quad \text{冪等律} \\ &= x \quad \text{吸収律} \end{aligned}$$

逆に、 $x \cdot y = x$ のとき

$$\begin{aligned} x + y &= x \cdot y + y \quad \text{仮定} \\ &= y \quad \text{吸収律} \end{aligned}$$

よって定義から

$$x \leq y$$

ii. $x \leq y$ のとき $x + y = y$ で,

$$\begin{aligned} x \cdot -y &= x \cdot -(x + y) \\ &= x \cdot (-x \cdot -y) \quad \text{ドモルガン則} \end{aligned}$$

$$
\begin{aligned}
&= 0 \cdot -y \qquad \text{結合律、補元律} \\
&= 0 \qquad \text{問題 (3)}
\end{aligned}
$$

逆に, $x \cdot -y = 0$ のとき, ドモルガン則と $-0 = 1$ から

$$
\begin{aligned}
-x + y &= 1 \\
x + y &= x \cdot 1 + y \qquad \text{問題 (3)} \\
&= x \cdot (-x + y) + y \\
&= x \cdot -x + x \cdot y + y \qquad \text{分配律} \\
&= 0 + x \cdot y + y \qquad \text{補元律} \\
&= x \cdot y + y \qquad \text{問題 (3)} \\
&= y \qquad \text{吸収律}
\end{aligned}
$$

よって定義から $x \leq y$

[証明終]

*(6) で使ったドモルガン則

$$-(x + y) = -x \cdot -y$$

$$-(x \cdot y) = -x + -y$$

の証明は

$$
\begin{aligned}
(x + y) + (-x \cdot -y) &= (x + y + -x) \cdot (x + y + -y) \qquad \text{分配律} \\
&= (y + 1) \cdot (x + 1) \qquad \text{交換律、補元律} \\
&= 1 \cdot 1 \qquad \text{問題 (3)} \\
&= 1 \qquad \text{問題 (3)}
\end{aligned}
$$

$$
\begin{aligned}
(x + y) \cdot (-x \cdot -y) &= x \cdot (-x \cdot -y) + y \cdot (-x \cdot -y) \qquad \text{分配律} \\
&= 0 \cdot -y + -x \cdot 0 \qquad \text{結合律、交換律、補元律、} \\
&= 0 + 0 \qquad \text{問題 (3)} \\
&= 0 \qquad \text{問題 (3)}
\end{aligned}
$$

よって, 既に証明した補元の一意性から

$$-(x + y) = -x \cdot -y$$

第 2 式も同様にできる.

[証明終]

* -0=1 については

$$0+1=1$$
$$0\cdot 1=0$$

と補元の一意性による.
全く同様に　　-1=0

1.11　演習５

(1) BA で, $--x=x$ (二重否定の法則);
$-(x+y)=-x\cdot -y$ (ド・モルガンの法則);
$-(x\cdot y)=-x+-y$ (ド・モルガンの法則)
が成立することを，証明しなさい.

[証明] $-x$ は x の補元だから定義により

$$x\cdot -x=0$$
$$x+-x=1 \quad *1$$

$--x$ は $-x$ の補元だから定義により

$$-x\cdot --x=0$$
$$-x+--x=1$$

交換律により

$$--x\cdot -x=0$$
$$--x+-x=1 \quad *2$$

2 組の式*1,*2 により補元の一意性から $--x=x$

$$\begin{aligned}(x+y)+(-x\cdot -y) &= (x+y+-x)\cdot(x+y+-y) \quad \text{分配律}\\ &= (y+1)\cdot(x+1) \quad \text{交換律, 補元律}\\ &= 1\cdot 1 \quad \text{演習 4 問題 (3)}\\ &= 1\end{aligned}$$

$$
\begin{aligned}
&(x+y)\cdot(-x\cdot -y)\\
&= \quad x\cdot(-x\cdot -y)+y\cdot(-x\cdot -y) \quad \text{分配律}\\
&= \quad 0\cdot -y+-x\cdot 0 \quad \text{結合律, 交換律, 補元律,}\\
&= \quad 0+0 \quad \text{演習 4 問題 (3)}\\
&= \quad 0 \quad \text{演習 4 問題 (3)}
\end{aligned}
$$

よって, 既に証明した補元の一意性から

$$-(x+y) = -x\cdot -y$$

以後, 公理, 演習 4 の結果, は断り無く使います. 双対の原理によれば

$$
\begin{aligned}
(x\cdot y)\cdot(-x+-y) &= (x\cdot y\cdot -x)+(x\cdot y\cdot -y)\\
&= (y\cdot 0)+(x\cdot 0)\\
&= 0\cdot 0\\
&= 0
\end{aligned}
$$

$$
\begin{aligned}
(x\cdot y)+(-x+-y) &= (x+(-x+-y))\cdot(y+(-x+-y))\\
&= 1+-y+-x+1\\
&= 1+1\\
&= 1
\end{aligned}
$$

よって, 補元の一意性から

$$-(x\cdot y) = -x+-y$$

[証明終]

(2) BA で, 次が成り立つことを証明しなさい.

(a) $x \le x$ (反射律);
(b) $(x \le y \ and \ y \le x) \Rightarrow x = y$ (反対称律);
(c) $(x \le y \ and \ y \le z) \Rightarrow x \le z$ (推移律);

[証明]

(a) $x + x = x$ から定義により $x \leq x$
(b) $(x \leq y \ and \ y \leq x)$

$$\begin{aligned} &\Rightarrow \quad (x + y = y \ and \ y + x = x) \quad \text{定義} \\ &\Rightarrow \quad x = y + x = x + y = y \\ &\Rightarrow \quad x \leq x \quad \text{定義} \end{aligned}$$

(c) $(x \leq y \ and \ y \leq z)$

$$\begin{aligned} &\Rightarrow \quad (x + y = y \ and \ y + z = z) \quad \text{定義} \\ &\Rightarrow \quad x + z = x + (y + z) = (x + y) + z = y + z = z \\ &\Rightarrow \quad x \leq z \quad \text{定義} \end{aligned}$$

[証明終]

(3) BA で, 次が成り立つことを証明しなさい.

(a) $x = -y \Leftrightarrow x + y = 1 \ and \ x \cdot y = 0$;
(b) $0 \leq x \leq 1$;
(c) $(x \leq z \ and \ y \leq z) \Rightarrow x + y \leq z$;
(d) $(x \leq z \ and \ y \leq z) \Rightarrow x \cdot y \leq z$;
(e) $a \cdot x \leq y \Leftrightarrow x \leq -a + y$.(結合の強さは, $-, \cdot, +$の順 !)

[証明]

(a) $x = -y \Leftrightarrow x + y = 1 \ and \ x \cdot y = 0$ ならば, 補元の一意存在のことですから

$$x = -y \Rightarrow x + y = -y + y = 1 \ and \ x \cdot y = -y \cdot y = 0$$

逆に $x + y = 1 \ and \ x \cdot y = 0$ は以下のように演習 3 で証明済みです. 例えば

$$\begin{aligned} -x &= -x \cdot 1 \\ &= -x \cdot (x + y) \\ &= -x \cdot x + -x \cdot y \\ &= x \cdot -x + y \cdot -x \\ &= 0 + y \cdot -x \end{aligned}$$

$$\begin{aligned} y &= y \cdot 1 \\ &= y \cdot (x + -x) \end{aligned}$$

$$
\begin{aligned}
&= y \cdot x + y \cdot -x \\
&= x \cdot y + y \cdot -x \\
&= 0 + y \cdot -x
\end{aligned}
$$

よって

$$y = -x$$

(b) $0 + x = x$ から定義により $0 \leq x$
$x + 1 = 1$ から 定義により $x \leq 1$

(c) $(x \leq z \ and \ y \leq z)$

$$
\begin{aligned}
&\Rightarrow \quad x + z = z \ and \ y + z = z \quad \text{定義} \\
&\Rightarrow \quad (x + y) + z = (x + z) + y = z + y = y + z = z \\
&\Rightarrow \quad x + y \leq z \quad \text{定義}
\end{aligned}
$$

(d)(d-1) $(x \leq z \ and \ y \leq z) \Rightarrow x \cdot y \leq z$

$$
\begin{aligned}
(x \leq z \ and \ y \leq z) \quad &\Rightarrow \quad x \cdot z = x \ and \ y \cdot z = y \text{ 定義} \\
&\Rightarrow \quad (x \cdot y) \cdot z = (x \cdot z) \cdot y = x \cdot y \\
&\Rightarrow \quad x \cdot y \leq z \text{ 定義}
\end{aligned}
$$

(d-2) $(x \leq y \ and \ x \leq z) \Rightarrow x \leq y \cdot z$;

$x \leq y \ and \ x \leq z \Leftrightarrow x \cdot y = x \ and \ x \cdot z = x$: 演習 4(6)

であることから,

$$
\begin{aligned}
x \cdot (y \cdot z) &= (x \cdot y) \cdot z \text{ : 結合律} \\
&= x \cdot z \\
&= x
\end{aligned}
$$

$x \cdot (y \cdot z) = x \Leftrightarrow x \leq y \cdot z$: 演習 4(6)

[証明終わり]

(e) $a \cdot x \leq y \Leftrightarrow x \leq -a + y$
[証明]

$a \cdot x \leq y$ なら定義により $a \cdot x + y = y$ で

$$\begin{aligned} x + -a + y &= x \cdot (-a + a) + -a + y \\ &= x \cdot -a + x \cdot a + -a + y \\ &= (x \cdot -a + -a) + (x \cdot a + y) \\ &= -a + y \end{aligned}$$

よって

$$x \leq -a + y$$

逆に $x \leq -a + y$ なら定義により $x \cdot (-a + y) = x$ で

$$\begin{aligned} a \cdot x + y &= a \cdot x \cdot (-a + y) + y \\ &= a \cdot x \cdot -a + a \cdot x \cdot y + y \\ &= 0 + a \cdot x \cdot y + y \\ &= y \end{aligned}$$

よって

$$a \cdot x \leq y$$

［証明終］

(4)

$$\begin{aligned} & -(-x + -y + z) + -(-x + y) + -x + z \\ &= x \cdot y \cdot -z + x \cdot -y + -x + z \\ &\qquad \text{第 } 1, 2 \text{ 項についてド・モルガン則} \\ &= x \cdot y \cdot -z + x \cdot -y + -x + (z + x \cdot y \cdot z)z \text{ について吸収律} \\ &= (x \cdot y \cdot -z + x \cdot y \cdot z) + x \cdot -y + -x + z \text{ 交換則} \\ &= x \cdot y \cdot (-z + z) + x \cdot -y + -x + z \text{ 分配則} \\ &= x \cdot y + x \cdot -y + -x + z \\ &= x \cdot (y + -y) + -x + z \text{ 分配則} \\ &= x + -x + z \\ &= 1 + z \\ &= 1 \end{aligned}$$

上で用いたド・モルガン則の一般化

$$-(x_1 + x_2 + \cdots + x_n) = -x_1 \cdot -x_2 \cdot \cdots \cdot -x_n$$

$$-(x_1 \cdot x_2 \cdot \cdots \cdot x_n) = -x_1 + -x_2 + \cdots + -x_n$$

につては

[証明] 数学的帰納法を使うと $n = 2$ については成立.(既に証明済み)

$n \leq k$ について成立つと仮定して

$$\begin{aligned}
&(x_1 + x_2 + \cdots + xk + x_{k+1}) \\
&= -((x_1 + x_2 + \cdots + x_k) + x_{k+1}) \text{結合則} \\
&= -(x_1 + x_2 + \cdots + x_k) \cdot -x_{k+1} \\
&\quad n = 2 \text{の場合のド・モルガン則} \\
&= (-x_1 \cdot -x_2 \cdot \cdots \cdot -x_k) \cdot -x_{k+1} \\
&\quad n = k \text{の場合のド・モルガン則} \\
&= -x_1 \cdot -x_2 \cdot \cdots \cdot -x_k \cdot -x_{k+1}
\end{aligned}$$

よって $n = k + 1$ の場合も成立.

また双対原理により

$$-(x_1 \cdot x_2 \cdot \cdots \cdot x_n) = -x_1 + -x_2 + \cdots + -x_n$$

[証明終]

(5) $\mathbf{N}$ を自然数全体の集合とします. N を 0 でない自然数とし, どんな素数 P についても, N は P の 2 乗で割り切れないものとします (ここでは, 0 は自然数の内に含めるものとします). このとき,

$A_n = \{x \in \mathbf{N} : 1 \leq x \leq N, x \text{は} N \text{を割り切る (つまり, } N \text{は} x \text{の倍数)}\}$

とおきます. 任意の $x, y \in A_n$ について, $x + y$ を x と y の最小公倍数と定義し, $x \cdot y$ を x と y の最大公約数と定義します. また, 任意の $x \in A_n$ について, $-x$ を N/x(N を x で割った商) と定義します. このとき, 次の問いに答えなさい.

(a) 任意の $x, y \in A_n$ について, $x + y = y \Leftrightarrow (y \text{は} x \text{の倍数})$ を証明しなさい.

[証明] x, y の最小公倍数を $L(x, y)$ で表すことにすると

$$\begin{aligned}
x + y = y &\Leftrightarrow L(x, y) = y \text{定義から} \\
&\Leftrightarrow (\exists k \in \mathbf{N})(kx = y) \\
&\Leftrightarrow (y \text{は} x \text{の倍数})
\end{aligned}$$

[証明終]

(b) $1, N \in A_n$ であることを確認しなさい.

[証明] $1/1 = 1, 1 \leq 1 \leq N$ ゆえ $1 \in A_n$
$N/N = 1, 1 \leq N \leq N$ ゆえ $N \in A_n$
[証明終]

(c) $x + y = y$ を, $x \leq y$ と書くことにする. 任意の $x, y, z \in A_n$ について
(i) $x \leq x$ (反射律);
(ii) $(x \leq y \ and \ y \leq x) \Rightarrow x = y$ (反対称律);
(iii) $(x \leq y \ and \ y \leq z) \Rightarrow x \leq z$ (推移律)

[証明] x, y の最小公倍数を $L(x, y)$ で表すことにすると
(i) $L(x, x) = x$ ゆえ

$$x + x = x$$

よって

$$x \leq x$$

(ii) $(x \leq y \ and \ y \leq x)$ とすると

$$L(x, y) = y \ and \ L(y, x) = x$$

$$(\exists k \in \mathbf{N})(kx = y) \ and \ (\exists l \in \mathbf{N})(ly = x)$$

ここで

$(\exists k \in \mathbf{N})(kx = y)$ となる k

$(\exists l \in \mathbf{N})(ly = x)$ となる l

を選ぶと, $y = kx = kly$ から $kl = 1$ よって

$$l = k = 1$$

よって

$$y = x$$

(iii) $(x \leq y \ and \ y \leq z)$ とすると

$$L(x,y) = y \ and \ L(y,z) = z$$

$$(\exists k \in \mathbf{N})(kx = y) \ and \ (\exists l \in \mathbf{N})(ly = z)$$

ここで

$$(\exists k \in \mathbf{N})(kx = y) \text{ となる } k$$

$$(\exists l \in \mathbf{N})(ly = z) \text{ となる } l$$

を選ぶと $(lk)x = ly = z$ よって

$$L(x,z) = z$$

ゆえに

$$x \leq z$$

[証明終]

(d) 任意の $x, y, z \in A_n$ について,

$$x \cdot (y + z) = x \cdot y + x \cdot z$$
$$x + y \cdot z = (x + y) \cdot (x + z) \text{(分配律, 分配法則)}$$

[証明] x, y の最小公倍数を $L(x,y)$ で, 最大公約数と $G(x,y)$ で表すことにすると

$$\begin{aligned} x \cdot (y + z) &= G(x, L(y,z)) \text{ 定義} \\ &= L(G(x,y), G(x,z)) \text{ 自然数の性質} \\ &= x \cdot y + x \cdot z \text{ 定義} \end{aligned}$$

$$\begin{aligned} x + y \cdot z &= L(x, G(y,z)) \text{ 定義} \\ &= G(L(x,y), L(x \cdot z)) \text{ 自然数の性質} \\ &= (x + y) \cdot (x + z) \text{ 定義} \end{aligned}$$

[証明終]

(e) $A_g N = (A_n, +, \cdot, -, 1, N)$ はブール代数であることを証明しなさい.

[証明] $A_n = \{x \in \mathbf{N} : 1 \leq x \leq N, x$ は N を割り切る (つまり, N は x の倍数) $\}$
x, y の最小公倍数を $L(x, y)$ で, 最大公約数と $G(x, y)$ で表すことにする.

(1) (b) から $1, N \in A_n$ で A_n は空でない集合である. $x, y \in A_n$ について $x + y = L(x, y), x \cdot y = G(x, y)$ とすると
$x, y \in A_n$ から

$$x, y \geq 1, (\exists k \in \mathbf{N})(N = kx), (\exists l \in \mathbf{N})(N = ly)$$

このような k, l を選べば $kx = N = ly$ すなわち, N は x, y の公倍数. よって最小公倍数 $L(x, y)$ は N を割り切る.
また $x, y \geq 1$ から

$$L(x, y) \geq 1$$

よって

$$x + y = L(x, y) \in A_n$$

$G(x, y)$ は x, y を割り切り, x, y は N を割り切るから $G(x, y)$ は従って N を割り切る. また $x, y \geq 1$ から $G(x, y) \geq 1$ よって

$$x \cdot y \in A_n$$

$x \in A_n$ なら $x \geq 1, (\exists k \in \mathbf{N})(N = kx)$ でそのような k をとれば $-x = k \geq 1$ で,

$$-x = k \in \mathbf{N}$$

よって A_n は $+, \cdot, -$ について閉じている;

(2) 任意の $x, y, z \in A$ について :
()

$$x + y = L(x, y) = L(y, x) = y + x$$

$$x \cdot y = G(x, y) = G(y, x) = y \cdot x$$

()

$$x + (y + z) = L(x, L(y, z)) = L(L(x, y), z) = (x + y) + z$$

$$x \cdot (y \cdot z) = G(x, G(y, z)) = G(G(x, y), z) = (x \cdot y) \cdot z$$

()

$$x \cdot y + y = L(G(x,y),y) = y$$

$$(x+y) \cdot y = G(L(x,y),y) = y$$

() (d) より

$$x \cdot (y+z) = x \cdot y + x \cdot z,$$

$$x + y \cdot z = (x+y) \cdot (x+z)$$

() どんな素数 P についても, N は P の 2 乗で割り切れないから

$$x \cdot -x = G(x, N/x) = 1 \text{ 自然数の性質}$$

また,

$$L(x, N/x) = N$$

[証明終]

[LCM,GCM についての補足] x, y の最大公約数, 最小公倍数を $G(x,y), L(x,y)$ で表します.

しかし, きりが無いので「素因数分解の一意性」は使うことにします.

P_m で素数全体の集合を表すとします.

写像 $\tau : x \in \mathbf{N} - \{0\} \to \tau(x) \in P((P_m \cup \{1\}) \times \mathbf{N})$ を次のように定義します.

$x \in \mathbf{N}, \neq 0, 1$ とするとき「素因数分解の一意性」から

$$(\exists! n \in \mathbf{N})(\exists! (p_1, p_2, \cdots, p_n) \in {P_m}^n)$$

$$(\exists! (l_1, l_2, \cdots, l_n) \in {N_b}^n)$$

$$(x = {p_1}^{l_1} \cdot {p_2}^{l_2} \cdot \cdots \cdot {p_n}^{l_n})$$

$x = 1$ のときは $x = 1^1$ として

$$\tau(x) = \{(1,1)\} \cup (\cup\{\{\{(p_k, i)\} | i = 1, \cdots, l_k\} | k = 1, \cdots, n\}$$

例: $x = 24$ なら $x = 1^1 \cdot 2^3 \cdot 3$ で

$$\tau(x) = \{(1,1), (2,1), (2,2), (2,3), (3,1)\}$$

このとき τ の作り方から $\tau(x) = \tau(y)$ なら $x = y$ (すなわち単射)

また,

$$\tau(G(x,y)) = \tau(x) \cap \tau(y)$$

$$\tau(L(x,y)) = \tau(x) \cup \tau(y)$$

です.

以下, $x, y, z \neq 0$ とします.

< 交換則 : $x + y = y + x$ >

$$\begin{aligned} \tau(G(x,y)) &= \tau(x) \cap \tau(y) \\ &= \tau(y) \cap \tau(x) \\ &= \tau(G(y,x)) \end{aligned}$$

τ は単射だから $G(x,y) = G(y,x)$

< 交換則 : $x \cdot x = y \cdot x$ >

$$\begin{aligned} \tau(L(x,y)) &= \tau(x) \cup \tau(y) \\ &= \tau(y) \cup \tau(x) \\ &= \tau(L(y,x)) \end{aligned}$$

τ は単射だから $L(x,y) = L(y,x)$

< 結合則 : $(x + y) + z = x + (y + z)$ >

$$\begin{aligned} \tau(G(G(x,y),z)) &= \tau(G(x,y)) \cap \tau(z) \\ &= (\tau(x) \cap \tau(y)) \cap \tau(z) \\ &= \tau(x) \cap (\tau(y) \cap \tau(z)) \\ &= \tau(x) \cap \tau(G(y,z)) \\ &= \tau(G(x,G(y,z))) \end{aligned}$$

τ は単射だから $G(G(x,y),z) = G(x,G(y,z))$
全く同様に

< 結合則 : $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ >

$$\begin{aligned} \tau(L(L(x,y),z)) &= \tau(L(x,y)) \cup \tau(z) \\ &= (\tau(x) \cup \tau(y)) \cup \tau(z) \\ &= \tau(x) \cup (\tau(y) \cup \tau(z)) \\ &= \tau(x) \cup \tau(L(y,z)) \\ &= \tau(L(x,L(y,z))) \end{aligned}$$

τ は単射だから $L(L(x,y),z) = L(x,L(y,z))$

$<$ 吸収律 : $x \cdot y + y = y >$

$$\begin{aligned} \tau(G(L(x,y),y)) &= \tau(L(x,y)) \cup \tau(y) \\ &= (\tau(x) \cap \tau(y)) \cup \tau(y) \\ &= \tau(y) \end{aligned}$$

τ は単射だから $G(L(x,y),y) = y$

$<$ 吸収律 : $(x+y) \cdot y = y >$

$$\begin{aligned} \tau(L(G(x,y),y)) &= \tau(G(x,y)) \cap \tau(y) \\ &= (\tau(x) \cup (y)) \cap \tau(y) \\ &= \tau(y) \end{aligned}$$

τ は単射だから $L(G(x,y),y) = y$

$<$ 分配律 : $(x \cdot y) + z = (x+z) \cdot (y+z) >$

$$\begin{aligned} \tau(G(L(x,y),z)) &= \tau(L(x,y)) \cap \tau(z) \\ &= (\tau(x) \cup \tau(y)) \cap \tau(z) \\ &= (\tau(x) \cap \tau(z)) \cup (\tau(y) \cap \tau(z)) \\ &= \tau(G(x,z)) \cup \tau(G(y,z)) \\ &= \tau(L(G(x,z),G(y,z))) \end{aligned}$$

τ は単射だから $G(L(x,y),z) = L(G(x,z),G(y,z))$

$<$ 分配律 : $(x+y) \cdot z = (x \cdot z) + (y \cdot z) >$

$$\begin{aligned} \tau(L(G(x,y),z)) &= \tau(G(x,y)) \cup \tau(z) \\ &= (\tau(x) \cap \tau(y)) \cup \tau(z) \\ &= (\tau(x) \cup \tau(z)) \cap (\tau(y) \cup \tau(z)) \\ &= \tau(L(x,z)) \cap \tau(L(y,z)) \\ &= \tau(G(L(x,z),L(y,z))) \end{aligned}$$

τ は単射だから $L(G(x,y),z) = G(L(x,z),L(y,z))$

N をどんな素数 P についても, P の 2 乗で割り切れない数とすると $N = 1 \cdot p_1 \cdot \cdots \cdot p_n$ の形をしているので, x が N を割りきるとすると x は 1 と, $p_1, \cdots, p_n$ から幾つか選ばれた素数の積で $-x = N/x$ は 1 と x に使われた $p_1, \cdots, p_n$ の残りの素数の積で

$$\tau(G(x, N/x)) = \{(1, 1)\} = \tau(1)$$

τ は単射だから $G(x, N/x) = 1$
また

$$\tau(L(x, N/x)) = \tau(N)$$

τ は単射だから $L(x, N/x) = N$

第2章　演習の解答

2.1　演習1

(1) から $UA \in A$
(2) から $0 = UA \sim UA \in A$
$X, Y \in A$ から (2) により $UA \sim X, UA \sim Y \in A$
(3) により $UA \sim (X \cap Y) = (UA \sim X) \cup (\cup A \sim Y) \in A$
(2) により $X \cap Y = (UA) \cap (X \cap Y) = UA \sim (UA \sim (X \cap Y)) \in A$

2.2　演習7

$\cap\{X\}, \cap\{X, Y\}$ はそれぞれ, 今までの集合論の記号法では何になるでしょうか. もし, 全体集合を V として, そのなかで X を考えているものとします. このとき, $X = 0$ として, 無理やり上の $\cap$ についての定義を適用すると, $\cap X$ は何になるでしょうか.
(演習7の終わり)

$$\begin{aligned}(\forall z \in 0)(y \in z) &\Leftrightarrow (\forall z)(z \in 0 \Rightarrow y \in z) \\ &\Leftrightarrow (\forall z)(not\ (z \in 0)\ or\ y \in z)\end{aligned}$$

で最後の式は恒真式.

よって

$$(\forall y)(y \in \{y | y \in V\ and\ (\forall z \in X)(y \in z)\} \Leftrightarrow y \in V)$$

従って,

$$\cap X = \{y | y \in V\ and\ (\forall z \in X)(y \in z)\} = V$$

2.3　演習8

命題8 $A_g =< A, +, \cdot, -, 0, 1 >$ をブール代数とし, $X \subseteq A$ とする. そのとき, 次の (1)〜(3) は同値となる：

(1) (1) は (1) X は A_g の部分宇宙である；
(2) $X \neq 0$ であって, X は $+, -$ について閉じている；
(3) $X \neq 0$ であって, X は $\cdot, -$ について閉じている.

(命題 8 の終わり)

[証明] 定義から

(1) なら (2),(3) は定義から明らか.
(2) なら $X \neq 0$ で少なくとも $x \in X$ となる元が 1 つ存在.
$-$ について閉じているから $-x \in X$ で ,
$+$ について閉じているから $1 = x + -x \in X$
また $x, y \in X$ について

$$-x, -y \in X$$

よって

$$-x + -y \in X$$

ゆえに

$$x \cdot y = -(-x + -y) \in X$$

従って $\cdot$ について閉じている.
さらに

$$0 = x \cdot -x \in X$$

結局, $(X, +, \cdot, -, 0, 1)$ は部分代数.

全く同様に
(3) なら $X \neq 0$ で少なくとも $x \in X$ となる元が 1 つ存在.
$-$ について閉じているから $-x \in X$ で ,
$\cdot$ について閉じているから $0 = x \cdot -x \in X$
また $x, y \in X$ について

$$-x, -y \in X$$

よって

$$-x \cdot -y \in X$$

ゆえに

$$x + y = -(-x \cdot -y) \in X$$

従って $+$ について閉じている.
さらに

$$1 = x + -x \in X$$

結局, $(X, +, \cdot, -, 0, 1)$ は部分代数.

[証明終]

命題 9 $A_g =< A, +, \cdot, -, 0, 1 >$ をブール代数とする. A_s を A_g の部分宇宙を要素とする空でない集合とすると, $\cap A_s$ は, A_g の部分宇宙である.
(命題 9 の終わり)

[証明] まず, $(\forall X \in A_s)(0 \in X), (\forall X \in A_s)(1 \in X)$ より

$$0 \in \cap A_s, 1 \in \cap A_s$$

$x, y \in \cap A_s$ とすると：

$$(\forall X \in A_s)(x + y \in X)$$

$(\forall X \in A_s)(x \cdot y \in X)$ で $(\forall X \in A_s)(-x \in X)$ で

$$x + y \in \cap A_s, x \cdot y \in \cap A_s, -x \in \cap A_s$$

[証明終]

2.4 演習 9

A の空でない部分集合 X で, $0, 1 \in X$ であり, $+, \cdot$ について閉じているが, X は A の部分宇宙でないというブール代数 A_g が存在することを証明しなさい.

[証明] $A_g = \{A, +, \cdot, -, 0, 1)$ で, $x \in A, \neq 0, 1, -x \neq 0, 1$ のとき $X = \{0, 1, x\}$ なら X は $+, \cdot$ について閉じているが, しかし, $-x$ は X の元でないので 部分宇宙ではない. [証明終]

2.5 演習 10

命題 6 (その 2)

(1) $x \leq x + y, y \leq x + y$;
$x + (x + y) = (x + x) + y = x + y$
よって定義から

$$x \leq x + y$$

$y + (x + y) = y + (y + x) = (y + y) + x = y + x = x + y$
よって定義から

$$y \leq x + y$$

(2) $x \cdot y \leq x, x \cdot y \leq y$;
$x \cdot y + x = x$ よって定義から

$$x \cdot y \leq x$$

$x \cdot y + y = y$ よって定義から

$$x \cdot y \leq y$$

(3) $x \leq y \Rightarrow x \cdot a \leq y \cdot a$;

$$\begin{aligned} x \leq y &\Rightarrow x + y = y \\ &\Rightarrow (x + y) \cdot a = y \cdot a \\ &\Rightarrow x \cdot a + y \cdot a = y \cdot a \\ &\Rightarrow x \cdot a \leq y \cdot a(\text{定義}) \end{aligned}$$

(4) $x \leq y \Rightarrow x + a \leq y + a$;

$$\begin{aligned} x \leq y &\Rightarrow x + y = y \\ &\Rightarrow x + y + a = y + a \\ &\Rightarrow x + y + a + a = y + a \\ &\Rightarrow (x + a) + (y + a) = y + a \\ &\Rightarrow x + a \leq y + a(\text{定義}) \end{aligned}$$

(5) $-x \leq y \Leftrightarrow x + y = 1$;

$$\begin{aligned} -x \leq y &\Rightarrow -x + y = y \\ &\Rightarrow x + y = x + (-x + y) \\ &\quad = (x + -x) + y = 1 + y = 1 \end{aligned}$$

$$x+y=1 \quad \Rightarrow \quad -x+y=(-x+y)\cdot 1=(-x+y)\cdot(x+y)$$
$$=-x\cdot x+-x\cdot y+y\cdot x+y\cdot y$$
$$=0+(-x+x)\cdot y+y=y+y=y$$

(6) $x \leq -y \Leftrightarrow x\cdot y=0$;

$$x \leq -y \Rightarrow x\cdot -y=x \Rightarrow x\cdot y=x\cdot -y\cdot y=0$$

$$x\cdot y=0$$
$$\Rightarrow \quad x\cdot -y=x\cdot -y+0$$
$$=x\cdot -y+x\cdot y=x\cdot(y+-y)=x\cdot 1=x$$

(7) $-0=1, -1=0$;
$0+1=1$ *and* $0\cdot 1=0$ よって $-0=1$
$1+0=1$ *and* $1\cdot 0=0$ よって $-1=0$

(8) $x \leq y \Rightarrow -y \leq -x$.
$x+y=y \Rightarrow -x\cdot -y=-y \Rightarrow -y=-x\cdot -y \Rightarrow -y \leq -x$

(1) $x \leq x$; (反射律)
(2) $(x \leq y$ *and* $y \leq x) \Rightarrow x=y$; (反対称律)
(3) $(x \leq y$ *and* $y \leq z) \Rightarrow x \leq z$. (推移律)

2.6 演習 11

(1) 半順序集合とみたブール代数では最大元, 最小元は存在しますか？もし存在 するならば, それは何ですか？
[解]
命題 6(その 1)(16) により
$(\forall x \in A)(0 \leq x \leq 1)$, また $0, 1 \in A$,
よって最小元は 0 , 最大元は 1

(2) 最小元を持つが, 最大元を持たない半順序集合の例を挙げなさい. 以下 0 は N に入れます.
[解]
例 1　　自然数全体の集合 N. 最小元は 0

例 2　　実数の半開区間 $[0,1) \subseteq R$ 順序は実数 R の順序

$$\begin{aligned} \inf[0,1) &= 0, 0 \in [0,1), \text{最小元 } 0 \\ \sup[0,1) &= 1,\ not\ (1 \in [0,1)) \text{ 最大元なし} \end{aligned}$$

(3) 最大元を持つが, 最小元を持たない半順序集合の例を挙げなさい.

[解]

例 1　　$\{-n | n \in N\}$ 順序は整数の順序です. 最大元は 0

例 2　　実数の半開区間 $(0,1] \subseteq R$ ただし順序は実数 R の順序です.

$$\begin{aligned} \inf(0,1] &= 0,\ not\ (0 \in (0,1]) \text{ 最小元なし} \\ \sup(0,1] &= 1, 1 \in (0,1] \text{ 最大元 } 1 \end{aligned}$$

(4) 最大元も, 最小元も持たない半順序集合の例を挙げなさい.

例 1　　実数全体の集合 R

例 2　　実数の開区間 $(0,1) \subseteq R$ 順序は実数 R の順序です.

$$\begin{aligned} \inf(0,1) &= 0,\ not\ (0 \in (0,1)), \text{最小元なし} \\ \sup(0,1) &= 1,\ not\ (1 \in (0,1)) \text{ 最大元なし} \end{aligned}$$

(5) 最大元 (最小元) が存在するとき, その一意性を証明しなさい.

[証明] 最大元が M_1, M_2 とすると：

$$(\forall x \in P)(x \leq M_1) M_1 \in P$$

$$(\forall x \in P)(x \leq M_2) M_2 \in P$$

第 1 式の x に M_2 を代入し, 第 2 式の x に M_1 を代入すると
$M_2 \leq M_1, M_1 \leq M_2$ よって

$$M_1 = M_2$$

最小元が m_1, m_2 とすると：

$$(\forall x \in P)(m_1 \leq x) m_1 \in P$$

$$(\forall x \in P)(m_2 \leq x) m_2 \in P$$

第 1 式の x に m_2 を代入し, 第 2 式の x に m_1 を代入すると

$$m_1 \leq m_2, m_2 \leq m_1$$

よって

$$m_1 = m_2$$

[証明終]

2.7 演習 12

全順序集合でない半順序集合の例を挙げなさい.(演習 12 の終わり)

[解] 異なる要素を 2 つ以上もつ集合を X として, そのべき集合 $P(X)$ は $\subseteq$ で半順序集合になるが例えば $a, b \in X$ で $a \neq b$ なら $\{a\}, \{b\} \in P(N)$ は $\{a\} \subseteq \{b\}$ でも $\{b\} \subseteq \{a\}$ でもない.

2.8 演習 13

上限 (下限) は存在すれば, 一意的に決まることを証明しなさい.
(演習 13 の終わり)

[証明] (1) 手抜きの解答 :
上限 (下限) はそれぞれ, 上界, 下界の最小元, 最大元で存在すれば, 上の (5) で最大元 (最小元) の一意性は証明済みです.

(2) まじめにやると :
s_1, s_2 が上限なら それぞれ, 上界でもあり
上限 s_1 は上界のうち最小だから, $s_1 \leq s_2$
上限 s_2 は上界のうち最小だから, $s_2 \leq s_1$
よって $s_1 = s_2$

l_1, l_2 が下限ならそれぞれ, 下界でもあり
下限 l_1 は下界のうち最大だから, $l_2 \leq l_1$
下限 l_2 は下界のうち最大だから, $l_1 \leq l_2$
よって $l_1 = l_2$

[証明終]

2.9 演習 14

Nat を自然数全体の集合とします. Fin を Nat の有限部分集合の全体とします. $Cofin+$ を Nat の部分集合 E で, E または $Nat \sim E$ が有限になるもの全体の集合とします. さらに, $FinEven$ を Nat の有限部分集合で偶数のみからなる集合全体の集合とします. このとき, 半順序集合 $(P(Nat), \subseteq)$ とその部分半順序集合 $(Fin, \subseteq), (Cofin+, \subseteq), (FinEven, \subseteq)$ を考えます. $FinEven \subseteq Fin \subseteq Cofin+ \subseteq P(Nat)$ は明らかです.
このとき,

(1) $FinEven$ は $(Fin, \subseteq)$ では上界を持たない.

[証明] 背理法によります.
M を $FinEven$ の $(Fin, \subseteq)$ での上界とすると, 任意の $X \in FinEven$ について,

$$X \subseteq M$$

任意 $n \in N$ について偶数 $\lceil 2n \rceil$ 1 個だけからなる集合 $\{2n\}$ は $\{2n\} \in FinEven$ で, これから

$$\{2n\} \subseteq M$$

$$\{2n | n \in N\} = \cup\{2n\} \subseteq M$$

これは, M が有限集合である (Fin の元である) ことに反します.
[証明終]

$(Cofin+, \subseteq)$ では無限個の上界を持つことを確かめなさい.

[証明] 例えば任意の $k \in N$ について, $X_k = N \sim \{2k+1\}$ とおくと

$$N \sim X_k = \{2k+1\}$$

ゆえ,

$$X_k \in Cofin+$$

で, X_k は奇数 $2k+1$ を 1 個だけ N から取り除いた, N の部分集合ですから, $Even$ を偶数全体の集合とすと, $Even \subseteq X_k$ で

$$(\forall Y \in FinEven)(Y \subseteq Even \subseteq X_k)$$

よって, X_k は $FinEven$ の $Cofin+$ の上界で, $k \in N$ を N 全体で動かせば, このような X_k は無限個.

[証明終]

(2) また, $(P(Nat), \subseteq)$ では, 偶数全体の集合が $FinEven$ の上限になっていることを確かめなさい.

[証明] $Even$ を偶数全体の集合とすると,

$$(\forall A \in FinEven)(A \subseteq Even)$$

ゆえ, $Even$ は $FinEven$ の $(P(Nat), \subseteq)$ での上界
M を $FinEven$ の任意の上界とすると, $x \in Even$ を任意にとれば, x は偶数で, $\{x\} \in FinEven$ で M は $FinEven$ の上界だから $\{x\} \subseteq M$ よって $x \in M$ $x \in Even$ を任意にとったから

$$(\forall x)(x \in Even \Rightarrow x \in M)$$

よって

$$Even \subseteq M$$

M は任意にとったから $Even$ は上界の最小元. すなわち上限.

[証明終]

2.10 演習 15

K を体とし, V を K 上の線形空間とする. L を V の部分空間全体の集合とする.(線形空間, 線形空間の部分空間の説明は省略します.) このとき,

(1) $(L, \subseteq)$ は束になることを証明しなさい.

[**(1)** の証明] $\subseteq$ が L の半順序を定義することは, 今までに何度も出てきたので省略します.

$X, Y \in L$ を任意にとると, X, Y は V の部分線形空間で $X \cap Y$ も部分線形空間.

(実際, $x, y \in X \cap Y, \alpha, \beta \in K$ を任意にとると, $x, y \in X$ ゆえ

$$\alpha x + \beta y \in X$$

全く同様に $x, y \in Y$ ゆえ

$$\alpha x + \beta y \in Y$$

よって

$$\alpha x + \beta y \in X \cap Y$$

すなわち, $X \cap Y$ は V の部分線形空間.)
よって

$$X \cap Y \in L$$

$X \cap Y \subseteq X, Y$ で, $X \cap Y$ は $\{X, Y\}$ の下界の一つ.

Z が $\{X, Y\}$ の下界とすると；
$x \in Z$ を任意にとると, $Z \subseteq X, Y$ から $x \in X, Y$ で $x \in X \cap Y$
よって,

$$Z \subseteq X \cap Y$$

すなわち, $X \cap Y$ は下界のうち最大元
すなわち下限で,

$$\inf\{X, Y\} = X \cap Y$$

$[X \cup Y] = \{\alpha_0 x_0 + \cdots + \alpha_k x_k | x_0, \cdots, x_k$ は有限個の $X \cup Y$ の元, $\alpha_0, \cdots, \alpha_k$ は有限個の K の元 $\}$
とおくと, $[X \cup Y]$ は V の部分線形空間,
(実際 $x, y \in [X \cup Y], \lambda, \mu \in K$ を任意にとると,

$$x, y \in [X \cup Y]$$

ゆえ有限個の $x_0, \cdots x_k \in X \cup Y, \alpha_0, \cdots \alpha_k \in K$ が存在して

$$x = \alpha_0 x_0 + \cdots + \alpha_k x_k$$

同様に有限個の $y_0, \cdots y_m \in X \cup Y, \beta_0, \cdots \beta_m \in K$ が存在して

$$y = \beta_0 y_0 + \cdots + \beta_m y_m$$

$$\begin{aligned}
&\lambda x + \mu y \\
&\quad = \lambda(\alpha_0 x_0 + \cdots + \alpha_k x_k) + \mu(\beta_0 y_0 + \cdots + \beta_m y_m) \\
&\quad = \lambda\alpha_0 x_0 + \cdots + \lambda\alpha_k x_k + \mu\beta_0 y_0 + \cdots + \mu\beta_m y_m
\end{aligned}$$

$$\in [X \cup Y]$$

よって

$$\lambda x + \mu y \in [X \cup Y]$$

すなわち, $[X \cup Y]$ は V の部分線形空間)
ゆえに,

$$[X \cup Y] \in L$$

また $[X \cup Y]$ の作り方から $(k = 0, \alpha 0 = 1, x_0 \in X \cup Y$ の場合を考えれば)

$$X \cup Y \subseteq [X \cup Y]$$

Z を V の部分線形空間として, $\{X, Y\}$ の上界, すなわち $x \subseteq Z, Y \subseteq Z$ とすると, $w \in [X \cup Y]$ を任意にとると, 有限個の $x_0, \cdots x_k \in X \cup Y, \alpha_0, \cdots \alpha_k \in K$ が存在して

$$w = \alpha_0 x_0 + \cdots + \alpha_k x_k$$

ここで $X \subseteq Z, Y \subseteq Z$ から $X \cup Y \subseteq Z$ で, Z は部分線形空間ゆえ, $x_0, \cdots x_k \in X \cup Y \subseteq Z, \alpha_0, \cdots \alpha_k \in K$ から

$$\alpha_0 x_0 + \cdots + \alpha_k x_k \in Z$$

よって (こ れも有限個の線形結合だから)

$$w \in Z$$

w はを任意にとったので,

$$[X \cup Y] \subseteq Z$$

結局,

$$\inf\{X, Y\} = X \cap Y,$$

$$\sup\{X, Y\} = [X \cup Y]$$

[(1) の証明終]

(2) 任意の $M \subseteq L$ について, $\Pi M = \cap M$ となることを証明しなさい.
$x, y \in \cap M, \alpha, \beta \in K$ を任意にとると, $\cap M$ の定義から $X \in M$ を任意にとると $x, y \in X$ よって

$$\alpha x + \beta y \in X$$

$X \in M$ は任意にとったから $\alpha x + \beta y \in \cap M$ よって $\cap M$ は V の部分線形空間
任意の $X \in M$ について $\cap M \subseteq X$ で, $\cap M$ は M の下界.
Y が M の下界とすると；

$$(\forall X \in M)(Y \subseteq X)$$

$x \in Y$ を任意にとると, 任意の $x \in M$ について $Y \subseteq X$ から

$$x \in X$$

よって

$$x \in \cap M$$

$x \in Y$ を任意にとったので,

$$Y \subseteq \cap M$$

すなわち, $\cap M$ は下界のうち最大元すなわち下限で,

$$\Pi M = \cap M$$

(3) 任意の $M \subseteq L$ について, ΣM は $\cup M$ によって生成された部分空間となることを証明しなさい. と，$[\cup M] = \{\alpha_0 x_0 + \cdots + \alpha_k x_k | x_0, \cdots, x_k$ は, 有限個の $\cup M$ の元, $\alpha_0, \cdots, \alpha_k$ は有限個の K の元 $\}$ とおくと,
$x, y \in [\cup M], \lambda, \mu \in K$ を任意にとると,

$$x, y \in [\cup M]$$

ゆえ

$$x_0, \cdots x_k \in \cup M, \alpha_0, \cdots \alpha_k \in K$$

が存在して

$$x = \alpha_0 x_0 + \cdots + \alpha_k x_k$$

同様に

$$y_0, \cdots y_m \in \cup M, \beta_0, \cdots \beta_m \in K$$

が存在して

$$y = \beta_0 y_0 + \cdots + \beta_m y_m$$

$$\begin{aligned}
&\lambda x + \mu y \\
&\quad = \lambda(\alpha_0 x_0 + \cdots + \alpha_k x_k) + \mu(\beta_0 y_0 + \cdots + \beta_m y_m) \\
&\quad = \lambda\alpha_0 x_0 + \cdots + \lambda\alpha_k x_k + \mu\beta_0 y_0 + \cdots + \mu\beta_m y_m
\end{aligned}$$

$$\in [\cup M]$$

よって (この線形結合も有限個でできているので)

$$\lambda x + \mu y \in [\cup M]$$

すなわち, $[\cup M]$ は部分線形空間

作り方から $(\forall X \in M)(X \subseteq \cup M)$ で $\cup M$ は M の上界. Z を V の部分線形空間として, M の上界, すなわち, $(\forall X \in M)(X \subseteq Z)$ とすると $w \in [\cup M]$ を任意にとると, 有限個の $x_0, \cdots x_k \in \cup M, \alpha_0, \cdots \alpha_k \in K$ が存在して

$$w = \alpha_0 x_0 + \cdots + \alpha_k x_k$$

ここで $(\forall X \in M)(X \subseteq Z)$ から, $\cup M \subseteq Z$ で, Z は部分線形空間ゆえ, $x_0, \cdots x_k \in \cup M \subseteq Z, \alpha_0, \cdots \alpha_k \in K$ から

$$\alpha_0 x_0 + \cdots + \alpha_k x_k \in Z$$

よって

$$w \in Z$$

w はを任意にとったので, $[\cup M] \subseteq Z$ よって $[\cup M]$ は上界のうち最小元すなわち, 下限で $\Sigma M = [\cup M]$

第3章　ストーンの同型定理

3.1　2^X 上のブール代数の構造

(0) 準備
$(0,1,+,\cdot,-,0,1)$ は演算の規則

$$1+1=1, 1+0=1$$

$$0+1=1, 0+0=0$$

$$1\cdot 1=1, 1\cdot 0=0$$

$$0\cdot 1=0, 0\cdot 0=0$$

$$-0=1, -1=0$$

のもとでブール代数になっています.[証明は根気良く公理をチェックするだけなので省略]

(1) 2^X 上のブール代数の構造
0 と 1 は

$$\begin{aligned} 0 : x \in X &\longmapsto 0 \in \{0,1\} \\ 1 : x \in X &\longmapsto 1 \in \{0,1\} \end{aligned}$$

で定義し, $+,\cdot,-$ は $g,h \in 2^X$ について

$$\begin{aligned} -g : x \in X &\longmapsto -g(x) \in \{0,1\} \\ g+h : x \in X &\longmapsto g(x)+h(x) \in \{0,1\} \\ g\cdot h : x \in X &\longmapsto g(x)\cdot h(x) \in \{0,1\} \end{aligned}$$

で定義すれば $(2^X,+,\cdot,-,0,1)$ はブール代数です.

ただし, 上の定義式の右辺の $g(x),h(x) \in \{0,1\}$ についての演算 $g(x)+h(x), g(x)\cdot h(x), -g(x)$ はブール代数 $(\{0,1\},+,\cdot,-,0,1)$ の演算です.

[証明] X が空集合でなければ 2^X が空集合でないことは自明. $+, \cdot, -$ が 2^X 上の演算であることも自明なので省略. 以下 $g, h, k \in 2^X$ を任意とり公理 (i) $\sim$ (v) が成立することを確認します.

これは g, h, k が何れも X 上で定義され,0 か 1 の値しか取らない関数であることと,(0) で述べたように $(\{0,1\}, +, \cdot, -, 0, 1)$ がブール代数であることを用いて根気良くチェックすればできます.

以下, 各 $x \in X$ に対する $g(x), h(x), k(x) \in \{0,1\}$ についての演算 $(+, \cdot, -)$ は (0) のブール代数 $(0, 1, +, \cdot, -, 0, 1)$ の演算で, 交換律, 結合律, 吸収律, 補元律その他は断りなく使います.

(i) 交換律

$x \in X$ を任意とると

$$\begin{aligned}(g+h)(x) &= g(x)+h(x)\\ &= h(x)+g(x)\\ &= (h+g)(x)\end{aligned}$$

x は任意だったから

$$(\forall x \in X)((g+h)(x) = (h+g)(x))$$

よって

$$g + h = h + g$$

全く同様にして ($+$ を $\cdot$ に替えて)

$$g \cdot h = h \cdot g$$

(ii) 結合律

$x \in X$ を任意とると

$$\begin{aligned}((g+h)+k)(x) &= (g+h)(x)+k(x)\\ &= (g(x)+h(x))+k(x)\\ &= g(x)+(h(x)+k(x))\\ &= (g+(h+k))(x)\end{aligned}$$

x は任意だったから

$$(\forall x \in X)(((g+h)+k)(x) = (g+(h+k))(x))$$

よって

$$(g+h)+k = g+(h+k)$$

全く同様にして ($+$ を $\cdot$ に替えて)

$$(g \cdot h) \cdot k = g \cdot (h \cdot k)$$

(iii) 吸収律

$x \in X$ を任意とると

$$\begin{aligned}((g \cdot h)+h)(x) &= (g \cdot h)(x) + h(x) \\ &= (g(x) \cdot h(x)) + h(x) \\ &= h(x)\end{aligned}$$

x は任意だったから

$$(\forall x \in X)(((g \cdot h)+h)(x) = h(x))$$

よって

$$(g \cdot h)+h = h$$

全く同様にして $+$ を $\cdot$ に, $\cdot$ を $+$ に替えて $x \in X$ を任意とると

$$\begin{aligned}((g+h) \cdot h)(x) &= (g+h)(x) \cdot h(x) \\ &= (g(x)+h(x)) \cdot h(x) \\ &= h(x)\end{aligned}$$

x は任意だったから

$$(\forall x \in X)((g+h) \cdot h)(x) = h(x))$$

よって

$$(g+h) \cdot h = h$$

(iv) 分配律

$x \in X$ を任意とると

$$\begin{aligned}(g \cdot (h+k))(x) &= g(x) \cdot (h+k)(x) \\ &= g(x) \cdot (h(x)+k(x)) \\ &= (g(x) \cdot h(x)) + (g(x) \cdot k(x)) \\ &= (g \cdot h)(x) + (g \cdot k)(x) \\ &= (g \cdot h + g \cdot k)(x)\end{aligned}$$

x は任意だったから

$$(\forall x \in X)((g \cdot (h+k))(x) = (g \cdot h + g \cdot k)(x))$$

よって

$$g \cdot (h+k) = g \cdot h + g \cdot k$$

$x \in X$ を任意とると

$$\begin{aligned}(g + (h \cdot k))(x) &= g(x) + (h \cdot k)(x) \\ &= g(x) + (h(x) \cdot k(x)) \\ &= (g(x) + h(x)) \cdot (g(x) + k(x)) \\ &= (g+h)(x) \cdot (g+k)(x) \\ &= ((g+h) \cdot (g+k))(x)\end{aligned}$$

x は任意だったから

$$(\forall x \in X)((g + (h \cdot k))(x) = ((g+h) \cdot (g+k))(x))$$

よって

$$g + (h \cdot k) = (g+h) \cdot (g+k)$$

(v) 補元律

$x \in X$ を任意とると

$$\begin{aligned}(g \cdot (-g))(x) &= g(x) \cdot (-g(x)) \\ &= 0\end{aligned}$$

$$\begin{aligned}(g + (-g))(x) &= g(x) + (-g(x)) \\ &= 1\end{aligned}$$

x は任意だったから

$$(\forall x \in X)((g \cdot (-g))(x) = 0(x))$$

$$(\forall x \in X)((g + (-g))(x) = 1(x))$$

よって

$$g \cdot (-g) = 0, g + (-g) = 1$$

(2) 双射 $f : P(X) \to 2^X$ の構成
これは

$$f : Y \in P(X) \longmapsto f(Y) \in 2^X$$
$$f(Y) : x \in X \longmapsto \chi_Y(x) \in \{0, 1\}$$

で定義します. χ_Y は X 上の Y の特性関数で $x \in Y$ のとき 1 、$x \in X - Y$ のとき 0 をとる関数です. これが双射であることは
(a) $Y, Z \in P(X)$ を任意にとり $f(Y) = f(Z)$ とすると

$$(\forall x \in X)(f(Y)(x) = f(Z)(x))$$

で x を任意にとると

$$\begin{aligned} x \in Y &\Leftrightarrow f(Y)(x) = 1 \\ &\Leftrightarrow f(Z)(x) = 1 \\ &\Leftrightarrow x \in Z \end{aligned}$$

で, x は任意でしたから

$$(\forall x)(x \in Y \Leftrightarrow x \in Z)$$

よって

$$Y = Z$$

Y, Z は任意でしたから

$$(\forall Y \in P(X))(\forall Z \in P(X))(f(Y) = f(Z) \Rightarrow Y = Z)$$

すなわち, f は単射

(b) $g \in 2^X$ を任意にとり, $Y \in P(X)$ を $Y = \{x | x \in X \; and \; g(x) = 1\}$ とすれば：$x \in X$ を任意にとると, $x \in Y$ のとき $\chi_Y(x) = 1 = g(x)$ $x \in X - Y$ のとき $\chi_Y(x) = 0 = g(x)$ x は任意にとったから

$$(\forall x \in X)(\chi_Y(x) = g(x))$$

すなわち,

$$\chi_Y = g$$

よって

$$f(Y) = g$$

$g \in 2^X$ は任意にとったので

$$(\forall g \in 2^X)(\exists Y \in P(X))(f(Y) = g)$$

すなわち f は全射

(3) 双射 $f : P(X) \to 2^X$ がブール代数の構造について同型であること. これも, 特性関数の性質から殆ど自明ですが, $(P(X), \cup, \cap, \sim, 0, X)$ がブール代数であることは演習 (3) で既に示されています. $(2^X, +, \cdot, -, 0, 1)$ もブール代数であることは (1) で示しました.

$Y, Z \in P(X)$ のとき $Y \cup Z, Y \cap Z, X - Y$ の特性関数については

(a) $\chi_{Y \cup Z} = \chi_Y + \chi_Z$

(b) $\chi_{Y \cap Z} = \chi_Y \cdot \chi_Z$

(c) $\chi_{X-Y} = -\chi_Y$

が成立します. これと f の定義から

$$f(Y \cup Z) = \chi_{Y \cup Z} = \chi_Y + \chi_Z = f(Y) + f(Z)$$

$$f(Y \cap Z) = \chi_{Y \cap Z} = \chi_Y \cdot \chi_Z = f(Y) \cdot f(Z)$$

$$f(X - Y) = \chi_{X-Y} = -\chi_Y = -f(Y)$$

(a) $\sim$ (b) の [証明]

$x \in X$ を任意にとると, $x \in Y \cup Z$ のとき

$$\chi_{Y \cup Z}(x) = 1$$

また, $x \in Y \; or \; x \in Z$ から

$$\chi_Y(x) = 1 \; or \; \chi_Z(x) = 1$$

よって

$$\chi_Y(x) + \chi_Z(x) = 1$$

ゆえに

$$\chi_{Y \cup Z}(x) = \chi_Y(x) + \chi_Z(x)$$

$x \in X - (Y \cup Z)$ のとき

$$\chi_{Y \cup Z}(x) = 0$$

また, $X - (Y \cup Z) = (X - Y) \cap (X - Z)$ ゆえ $x \in (X - Y)\ and\ x \in (X - Z)$ から

$$\chi_Y(x) = 0\ and\ \chi_Z(x) = 0$$

よって

$$\chi_Y(x) + \chi_Z(x) = 0$$

ゆえに

$$\chi_{Y \cup Z}(x) = \chi_Y(x) + \chi_Z(x)$$

結局, どちらの場合でも

$$\chi_{Y \cup Z}(x) = \chi_Y(x) + \chi_Z(x) = (\chi_Y + \chi_Z)(x)$$

$x \in X$ を任意にとったので

$$(\forall x \in X)(\chi_{Y \cup Z}(x) = (\chi_Y + \chi_Z)(x))$$

よって

$$\chi_{Y \cup Z} = \chi_Y + \chi_Z$$

$x \in X$ を任意にとると $x \in Y \cap Z$ のとき

$$\chi_{Y \cap Z}(x) = 1$$

また, $x \in Y \ and \ x \in Z$ から

$$\chi_Y(x) = 1 \ and \ \chi_Z(x) = 1$$

よって

$$\chi_Y(x) \cdot \chi_Z(x) = 1$$

ゆえに

$$\chi_{Y \cap Z}(x) = \chi_Y(x) \cdot \chi_Z(x)$$

$x \in X - (Y \cap Z)$ のとき

$$\chi_{Y \cap Z}(x) = 0$$

また, $X - (Y \cap Z) = (X - Y) \cup (X - Z)$ ゆえ $x \in (X - Y) \ or \ x \in (X - Z)$ から

$$\chi_Y(x) = 0 \ or \ \chi_Z(x) = 0$$

よって

$$\chi_Y(x) \cdot \chi_Z(x) = 0$$

ゆえに

$$\chi_{Y \cap Z}(x) = \chi_Y(x) \cdot \chi_Z(x)$$

結局、どちらの場合でも

$$\chi_{Y \cap Z}(x) = \chi_Y(x) \cdot \chi_Z(x) = (\chi_Y \cdot \chi_Z)(x)$$

$x \in X$ を任意にとったので

$$(\forall x \in X)(\chi_{Y \cap Z}(x) = (\chi_Y \cdot \chi_Z)(x))$$

よって

$$\chi_{Y \cap Z} = \chi_Y \cdot \chi_Z$$

$x \in X$ を任意にとると $x \in Y$ のとき

$$\chi_X - Y(x) = 0$$

また $\chi_Y(x) = 1$ ゆえ $-\chi_Y(x) = 0$
よって

$$\chi_{X-Y}(x) = -\chi_Y(x)$$

$x \in X - Y$ のとき

$$\chi_{X-Y}(x) = 1$$

また $\chi_Y(x) = 0$ ゆえ $-\chi_Y(x) = 1$
よって

$$\chi_{X-Y}(x) = -\chi_Y(x)$$

結局, どちらの場合でも

$$\chi_{X-Y}(x) = -\chi_Y(x) = (-\chi_Y)(x)$$

$x \in X$ を任意にとったので

$$(\forall x \in X)(\chi_{X-Y}(x) = (-\chi_Y)(x))$$

よって

$$\chi_X - Y = -\chi_Y$$

[証明終]

(命題) ブール代数の同型写像の逆写像は, またブール代数の同型写像である.
(命題終わり)

[証明] $f : A \to B$ をブール代数の同型写像とします.
任意の $a, b \in A$ について,

$$f(a \cdot b) = f(a) \cdot f(b), f(-a) = -f(a)$$

がいえます.
$f^{(-1)} : B \to A$ を f の逆写像とします.
f が全単射であることから, $f^{(-1)}$ は全単射です.
任意の $x, y \in B$ について,

$$f^{(-1)}(x), f^{(-1)}(y) \in A$$

ですから, f が準同型写像であることから,

$$f(f^{(-1)}(x) \cdot f^{(-1)}(y)) = f(f^{(-1)}(x)) \cdot f(f^{(-1)}(y))$$

がいえます.
任意の $x \in B$ について, $f(f^{(-1)}(x)) = x$ ですから, 上の式は

$$f(f^{(-1)}(x) \cdot f^{(-1)}(y)) = x \cdot y$$

となります. 従って,

$$f^{(-1)}(f(f^{(-1)}(x)\cdot f^{(-1)}(y))) = f^{(-1)}(x\cdot y).$$

任意の $a\in A$ について, $f^{(-1)}(f(a)) = a$ がいえるから, 上の式は

$$f^{(-1)}(x)\cdot f^{(-1)}(y) = f^{(-1)}(x\cdot y)$$

となり,

$$f^{(-1)}(x\cdot y) = f^{(-1)}(x)\cdot f^{(-1)}(y). \quad (*)$$

同様にして, 任意の $x\in B$ について, $f^{(-1)}(x)\in A$ ですから, f が準同型写像であることから,

$$f(-f^{(-1)}(x)) = -f(f^{(-1)}(x)) = -x.$$

上と同様に考えて,

$$f^{(-1)}(f(-f^{(-1)}(x))) = f^{(-1)}(-x).$$

従って,

$$f^{(-1)}(-x) = -f^{(-1)}(x)) \quad (**)$$

がいえる. (*) と (**) から, $f^{(-1)}$ もまた, 準同型写像であり, 全単射であるから, 同型写像である.

[証明終わり]

3.2 ストーンの同型定理

A がブール代数として、 $x\subseteq A$ が A 上のブール代数の真のフィルターというのは

$(F1)$ $(\forall a\in x)$ $(\forall b\in A)$ $(a\le b\Rightarrow b\in x)$
$(F2)$ $(\forall a\in x)$ $(\forall b\in x)$ $(a\cdot b\in x)$
$(F3)$ $1\in x$
$(F4)$ $\neg(0\in x)$ (0 は x の元でない)

$K = \{x\in P(A) | x$ は A 上の真のフィルター $\}$ は順序「 $\subseteq$ 」ついて帰納的順序集合

[証明] まず, $K \subseteq P(A)$ で, $P(A)$ は $\subseteq$ について順序集合なので, K も順序集合. 次に Y が順序 $\subseteq$ での K の空でない全順序部分集合とすると, $\cup Y$ は A 上の真のフィルター

(証明)**(F1)** $a \in \cup Y, b \in A$ を任意にとって, $a \leq b$ とすると $a \in \cup Y$ から

$$(\exists y \in Y)(a \in y)$$

このような $y_0 \in Y$ を選ぶと, $a \in y_0$ と $a \leq b$ から, y_0 は真のフィルターだから,

$$b \in y_0$$

よって

$$(\exists y \in Y)(b \in y)$$

ゆえに $b \in \bigcup Y$ となり

$$a \leq b \Rightarrow b \in \bigcup Y$$

$a \in \bigcup Y, b \in A$ は任意にとったから

$$(\forall a \in \bigcup Y)(\forall b \in A)(a \leq b \Rightarrow b \in \bigcup Y)$$

(F2) $a \in \bigcup Y, b \in \bigcup Y$ を任意にとると,

$$(\exists y \in Y)(a \in y), (\exists y \in Y)(b \in y)$$

このような $y_0, y_1 \in Y$ を選んで, $a \in y_0, b \in y_1$ とすると Y は $\subseteq$ について全順序だったから $y_0 \subseteq y_1$ または $y_1 \subseteq y_0$ ここで $y_0 \subseteq y_1$ の場合を考えると

$$a \in y_1, b \in y_1$$

よって

$$a \cdot b \in y_1 (y_1 \text{は真のフィルターだから})$$

$y_1 \subseteq \cup Y$ だから $a \cdot b \in \bigcup Y$ $y_1 \subseteq y_0$ の場合も全く同じ. 結局

$$(\forall a \in \bigcup Y)(\forall b \in \bigcup Y)(a \cdot b \in \bigcup Y)$$

(F3) Y は空でないから

$$(\exists y)(y \in Y)$$

このような $y_0 \in Y$ を選べば y_0 は真のフィルターだから

$$1 \in y_0$$

よって

$$(\exists y \in Y)(1 \in y)$$

ゆえに

$$1 \in \bigcup Y$$

(F4) $0 \in \cup Y$ とすると

$$(\exists y \in Y)(0 \in y)$$

このような $y_0 \in Y$ を選ぶと $0 \in y_0$ であり, しかし y_0 は真のフィルターだから $\neg(0 \in y_0)$ で矛盾.

(証明終)

$\cup Y$ が A 上の真のフィルターだから

$$\cup Y \in K$$

z の作り方から明らかに

$$(\forall y \in Y)(y \subseteq \cup Y)$$

よって $\cup Y$ は順序 $\subseteq$ について Y の K での上界 K の任意の空でない全順序部分集合 Y が上界をもつから K は帰納的

[証明終]

K は順序 $\subseteq$ について 帰納的順序集合なので Zorn の補題から極大な元が存在.

(定義 3) $X = \{x \in P(A) | x$ は A 上の真のフィルター $and\ x$ は極大 $\}$

(定義 4) $a \in A$ について $s(a) = \{x \in X | a \in x\}$ とすると

$$a \in A, s(a) = \{x \in X | a \in x\}$$

が定義できる.

よって写像

$$s : a \in A \mapsto s(a) \in P(X)$$

が定義される.
s については以下が成り立つ.

$$\begin{aligned} s \text{ が単射} \quad & (s(a) = s(b) \Rightarrow a = b) \\ & s(a + b) = s(a) \cup s(b) \\ & s(a \cdot b) = s(a) \cap s(b) \\ & s(-a) = X \sim s(a) \end{aligned}$$

(*1) $a \leq b$ は A 上の順序関係である.

(*2) $a, b \in A$ について

$$a \cdot b \leq a, b \leq a + b$$

$$a \leq b \Leftrightarrow (-b) \cdot a = 0$$

(*3) 任意の $a, b, a', b' \in A$ について, $a \leq a', b \leq b'$ のとき

$$a \cdot b \leq a' \cdot b', a + b \leq a' + b'$$

(*4) x を A 上の極大な真のフィルターとするとき

$$((\forall a \in A)(\forall b \in A)(a + b \in x \Leftrightarrow (a \in x \ or \ b \in x))$$

(*4 の証明) $a, b \in A$ を任意にとり; $a \in x \ or \ b \in x$ とすると $a \in x$ のとき, (*2) から $a \leq a + b$ なので x は真のフィルターなので (F1) から

$$a + b \in x$$

同様に $b \in x$ のときも

$$a + b \in x$$

逆に $a + b \in x$ として $\neg(a \in x) \ and \ \neg(b \in x)$ とすると:

$f = \{y \in A | a + y \in x\}$ は A 上の真のフィルター

(証明)**(F1)** $y \in f, k \in A$ を任意にとり, $y \leq k$ とすると f の定義から

$$a + y \in x$$

(*3) から

$$a + y \leq a + k$$

x は真のフィルターだから

$$a + k \in x$$

よって

$$k \in f$$

(F2) $y \in f, k \in f$ を任意にとると f の定義から

$$a + y \in x, a + k \in x$$

$$a + y \cdot k = (a + y) \cdot (a + k)$$

x は真のフィルターだから

$$(a + y) \cdot (a + k) \in x$$

よって f の定義から

$$y \cdot k \in f$$

(F3) $a + 1 = 1$

x は真のフィルターだから

$$1 \in x$$

よって f の定義から

$$1 \in f$$

(F4) $0 \in f$ とすると f の定義から

$$a \in x$$

これは仮定 $\neg(a \in x)$ に矛盾.

よって

$$\neg(0 \in f)$$

(証明終)

f の作り方から

$$x \subseteq f, x \neq f$$

(証明) $y \in x$ を任意にとると (*2) から $y \leq a + y$ で x は真のフィルターだから

$$y \in f$$

y は任意だったから

$$(\forall y)(y \in x \Rightarrow y \in f)$$

よって

$$x \subseteq f$$

一方, f の定義から $b \in f$, 仮定から $\neg(b \in x)$ よって

$$x \neq f$$

(証明終)

しかし, x は極大な真のフィルターだったから $x \subseteq f$ により $x = f$ となり矛盾

(*4 の証明終)

$(\forall a \in F)(\forall b \in F)(a + b \in F \Leftrightarrow (a \in F \ or \ b \in F))$ がいえる真のフィルター F を素フィルターといいます.

(*5) x を A 上の真のフィルターとするとき

$$(\forall a)(a \in x \Rightarrow \neg(-a \in x))$$

特に x が極大な真のフィルターとするとき

$$(\forall a)(a \in x \Leftrightarrow \neg(-a \in x))$$

(*5 の証明) x を A 上の真のフィルターとし $a \in x$ を任意にとると, $-a \in x$ とすると F2 から $0 = a \cdot (-a) \in x$ で (F4) の $\neg(0 \in x)$ に矛盾

特に x が極大な真のフィルターとするとき

$$1 \in x, 1 = a + (-a)$$

から (*4) により

$$a \in x \ or \ -a \in x$$

よって

$$\neg(-a \in x) \Rightarrow a \in x$$

(*5 の証明終)

$(\forall a)(a \in F \Leftrightarrow \neg(-a \in F))$ がいえる真のフィルターを超フィルター (ウルトラフィルター)(ultrafilter) といいます. 超フィルターは常に a か $-a$ のどちらか一方のみが F の要素となるような真のフィルターです.
(*5) は, 次の命題に集約されます.

(命題) A 上の真のフィルター F について, 次の (1) $\sim$ (3) は同値である.

(1) F は極大フィルターである.
(2) F は超フィルターである.
(3) F は素フィルターである.

(命題終わり)

(*6) x を A 上の真のフィルターとするとき

$$(\forall a)(\forall b)((a \in x \ and \ b \in x)) \Leftrightarrow a \cdot b \in x)$$

(*6 の証明) x を A 上の真のフィルターとし, a, b を任意にとる.
$a \in x \ and \ b \in x$ なら (F2) により

$$a \cdot b \in x$$

逆に $a \cdot b \in x$ なら (*2) から

$$a \cdot b \leq a \ and \ a \cdot b \leq b$$

で (F1) により

$$a \in x \ and \ b \in x$$

(*6 の証明終り)

(*7) $a \neq 0$ とすると $F_a = \{z \in A | a \leq z\}$ は真のフィルター

(*7 の証明)

(F1) $p \in F_a, q \in A$ を任意にとり, $p \leq q$ とすると $a \leq p, p \leq q$ から $\leq$ が順序関係なので (*1)
$a \leq q$ で

$$q \in F_a$$

よって

$$(\forall p \in F_a)(\forall q \in A)(p \leq \Rightarrow q \in F_a)$$

(F2) $p \in F_a, q \in F_a$ を任意にとると $a \leq p, a \leq$ から

$$a = a \cdot a \leq p \cdot q \quad (*2)$$

で $p \cdot q \in F_a$ よって

$$(\forall p \in F_a)(\forall q \in F_a)(p \cdot q \in F_a)$$

(F3) $a + 1 = 1$ から

$$a \leq 1$$

よって

$$1 \in F_a$$

(F4) $0 \in F_a$ とすると

$$a \leq 0$$

また $0 + a = a$ から

$$0 \leq a$$

で結局 $a = 0$ となって矛盾.

(*7 の証明終)

(*8) f を A 上の真のフィルターとし, $Z = \{x | x : A$ 上の極大な真のフィルター $and\ f \subseteq x\}$ とおくとき

$$f = \cap Z$$

(**8 の証明)** Z の定義より任意の $x \in Z$ について $f \subseteq x$ だから $f \subseteq \cap Z$. $\cap Z \subseteq f$ を示すため,

$$\sim f \subseteq \sim \cap Z$$

を示す. ($\sim$ は $P(A)$ 上で) $y \in \sim f$ とすると

$$(\forall p \in f)((-y) \cdot p \neq 0)$$

(証明) これを否定した $(\exists p \in f)((-y) \cdot p = 0)$ を仮定すると, これを充たす $p \in f$ を選んで, $(-y) \cdot p = 0$ よって

$$p \leq y \quad (*2)$$

これから, $y \in f$ となり矛盾

(証明終)

g_0 を $f \cup \{-y\}$ の元の有限個の積全体

$$g_0 = \{k \in A | (\exists n \in N)(\exists y_1, \cdots, y_n \in f \cup \{-y\})(k = y_1 \cdots \cdots y_n)\}$$

とおき,

$$f_0 = \{p \in A | (\exists k \in g_0)(k \leq p)\}$$

とすると, f_0 は A 上の真のフィルターで,

$$-y \in f$$

(証明) まず, g_0 の定義式中,

$$y_1 = 1 \in f, y_2 = -y, k = y_1 \cdot y_2$$

とおけば $-y \in g_0$. そこで f_0 の定義式中, $k = p = -y$ と置けば, $-y \in f_0$ 以下, f_0 が A 上の真のフィルタであることを示す.

(F1) $p \in f_0, q \in A$ を任意にとり $p \leq q$ とすると f_0 の定義から

$$(\exists k \in g_0)(k \leq p)$$

このような $k \in g_0$ を選び, $k \leq p$ とすると $p \leq q$ から $k \leq q$ よって f_0 の定義から

$$q \in f_0$$

(F2) $p \in f_0, q \in f_0$ を任意にとると f_0 の定義から

$$(\exists k \in g_0)(k \leq p), (\exists h \in g_0)(h \leq q)$$

このような $k, h \in g_0$ を選び, $k \leq p, h \leq q$ とすると (*2 から)

$$k \cdot h \leq p \cdot q$$

g_0 の定義から

$$(\exists n \in N)(\exists y_1, \cdots, y_n \in f \cup \{-y\})(k = y_1 \cdot \cdots \cdot y_n)$$

$$(\exists m \in N)(\exists z_1, \cdots, z_m \in f \cup \{-y\})(h = z_1 \cdot \cdots \cdot z_m)$$

このような $y_1, \cdots, y_n$ と $z_1, \cdots, z_n$ を選べば

$$k \cdot h = y_1 \cdot \cdots \cdot y_n \cdot z_1 \cdot \cdots \cdot z_m$$

よって

$$k \cdot h \in g_0$$

よって f_0 の定義から

$$p \cdot q \in f_0$$

(F3) まず, g_0 の定義式中, $y_1 = 1 \in f$ とおけば

$$1 \in g_0$$

f_0 の定義式中, $k = p = 1$ と置けば,

$$1 \in f_0$$

(F4) $0 \in f_0$ とすると f_0 の定義から

$$(\exists k \in g_0)(k \leq 0)$$

g_0 の定義から

$$(\exists n \in N)(\exists y_1, \cdots, y_n \in f \cup \{-y\})(k = y1 \cdot \cdots \cdot y_n)$$

このような $y_1, \cdot, y_n \in f \cup \{-y\}$ をとると

$$0 \leq k = y_1 \cdot \cdots \cdot y_n \leq 0$$

よって

$$y_1 \cdot \cdots \cdot y_n = 0$$

ここで

$$(\forall p \in f)((-y) \cdot p \neq 0)$$

であるから $y_1, \cdots, y_n$ の中で $-y$ と等しいものがあると矛盾する. 従って, $y_1, \cdots, y_n$ は全て f の元
しかしこれから

$$0 = y_1 \cdot \cdots \cdot y_n \in f$$

となって矛盾.

(証明終)

よって f_0 は A 上の真のフィルターで, $-y \in f_0$
$K = \{z | z$ は A 上の真のフィルター $and\ f_0 \subseteq z\}$ とおくと K は順序 $\subseteq$ について帰納的順序集合で $f_0 \subseteq x$ となる極大な真のフィルター x が存在.

(証明) 前節の解答「 $K = \{z | z$ は A 上の真のフィルター $\}$ が順序 $\subseteq$ について帰納的順序集合」と殆ど同じなので、違うところだけ書きます.
Y が K の空でない全順序部分集合なら $\bigcup Y$ が A 上の真のフィルターで,

$$(\forall y \in Y)(y \subseteq \bigcup Y)$$

であることは全く同じで, K の定義と $Y \subseteq K$ から

$$(\forall y \in Y)(f_0 \subseteq y)$$

で

$$f_0 \subseteq \bigcup Y$$

よって

$$\bigcup Y \in K$$

で $\bigcup Y$ は Y の K 上での上界
K の空でない任意の全順序部分集合が K 上での上界をもつから K は順序 $\subseteq$ について帰納的

(証明終) $f \subseteq f_0$ であるから $f \subseteq x$ であることに注意して Zorn の補題から K の極大元 x が存在. これは $-y \in f_0 \subseteq x$ を充たしている. x は極大なので、$\neg(y \in x)(*5)$ よって $\neg(y \in \cap Z)$ すなわち $y \in \sim \cap Z$ (*8 の証明終)

(*9) $F_a = \{z \in A | a \leq z\}, s(a) = \{x \in X | a \in x\}$ について：$F_a = \cap s(a)$

(*9 の証明) $a = 0$ のときは $F_0 = \{z \in A | 0 \leq z\} = A$ $s(0) = \{x \in X | 0 \in x\} = \phi$ で、$\cap s(a) = \{z \in A | (\forall x \in S(a))(z \in x)\}$ から $\cap s(0) = A$ よって $F_0 = \cap s(0)$. $a \neq 0$ のとき (*7) から F_a は A 上の真のフィルターで $s(a)$ は $F_a \subseteq x$ となる A 上の極大な真のフィルター x 全体の集合と等しい.

(証明) $x \in s(a)$ のとき $z \in F_a$ を任意にとると $a \leq z, z \in A$ $a \in x$ ゆえ (F1) により $z \in x$ zは任意にとったから $F_a \subseteq x$ 逆に x を $F_a \subseteq x$ となる A 上の極大な真のフィルターとすると a 自身 $a \leq a$ で　$a \in F_a$ よって $a \in x$ すなわち $x \in s(a)$ (証明終) よって、(*8) により $F_a = \cap s(a)$

(*9 の証明終)

以下

$$X = \{x \in P(A) | x \text{ は } A \text{ 上の極大な真のフィルター }\}$$
$$s(a) = \{x \in X | a \in x\}$$
$$s : a \in A \mapsto s(a) \in P(X)$$

について

$$(1) s \text{ が単射 } (s(a) = s(b) \Rightarrow a = b)$$
$$(2) s(a + b) = s(a) \cup s(b)$$
$$(3) s(a \cdot b) = s(a) \cap s(b)$$
$$(4) s(-a) = X \sim s(a)$$

[証明]

(1) $a, b \in A$ を任意にとり、$s(a) = s(b)$ とする. $s(a)$ の定義から $(\forall x \in s(a))(a \in x)$ で $a \in \cap s(a)$ $s(b)$ の定義から $(\forall x \in s(b))(b \in x)$ で $b \in \cap s(b)$ (*9) と仮定から $a \in \cap s(a) = \cap s(b) = F_b = \{z \in A | b \leq z\}$ で $a \leq b$ 全く同様に $b \in \cap s(b) = \cap s(a) = F_a = \{z \in A | a \leq z\}$ で $b \leq a$ よって $a = b$

(2) $a, b \in A$ を任意にとり $x \in s(a + b)$ を任意にとると x は A 上の極大な真のフィルターで $a + b \in x$ よって (*4) から $a \in x or b \in x$ これから $x \in s(a) or x \in s(b)$ よって $x \in s(a) \cup s(b)$ $x \in s(a + b)$ を任意だったから $s(a + b) \subseteq s(a) \cup s(b)$ 逆に、$x \in s(a) \cup s(b)$ を任

意にとると,$x \in s(a) or x \in s(b)$ よって $a \in x or b \in x$
(*2) から $a \leq a+b, b \leq a+b$ なので $a \in x or b \in x$
どちらの場合でも $a+b \in x$ 従って、$x \in s(a+b)$
$x\ in s(a) \cup s(b)$ を任意にとったので $s(a) \cup s(b) \subseteq s(a+b)$
結局、$s(a+b) = s(a) \cup s(b)$

(3) $a, b \in A$ を任意にると

$x \in s(a \cdot b)$
$\Leftrightarrow a \cdot b \in x\ and\ x$ は極大な真のフィルター
$\Leftrightarrow a \in x\ and\ b \in x\ and\ x$ は極大な真のフィルター $(*6)$
$\Leftrightarrow x \in s(a)\ and\ x \in s(b)$ 定義
$\Leftrightarrow x \in s(a) \cap s(b)$

よって $s(a \cdot b) = s(a) \cap s(b)$

(4) $a \in A$ を任意にとると

$x \in s(-a)$
$\Leftrightarrow -a \in x\ and\ x$ は極大な真のフィルター
$\Leftrightarrow \neg(a \in x)\ and\ x$ は極大な真のフィルター $(*5)$
$\Leftrightarrow x \in X\ and \neg(x \in s(a))$
$\Leftrightarrow x \in X \sim s(a)$

よって $s(-a) = X \sim s(a)$ [証明終リ]

$(s(A), \cup, \cap, \sim, 0, X)$ はブール代数です。

[証明] これは $s(A) \subseteq P(X)$ で、今まで何度か出てきましたように $(P(X), \cup, \cap, \sim, 0, X)$ がブール代数ですので、$0, X \in s(A)$ と、$s(A)$ が $\cup, \cap, \sim$ について閉じていることを示せばいいわけです。
$s(A)$ が部分宇宙 (部分ブール代数) であることをいえばいいので,
$\cap, \sim$ についてのみ閉じていることを示せばいいです.
s の定義から $0 = s(0) \in s(A)$, (左辺の 0 は空集合の意味です。) s の定義と (4) から

$$X = X \sim 0 = X \sim s(0) = s(-0) \in s(A)$$

$g, h \in s(A)$ のとき

$$(\exists a \in A)(g = s(a))$$
$$(\exists b \in A)(h = s(b))$$

でこのような $a, b \in A$ をとれば、(2) を用いて

$$g \cup h = s(a) \cup s(b) = s(a + b) \in s(A)$$

同様に (3) を用いて

$$g \cap h = s(a) \cap s(b) = s(a \cdot b) \in s(A)$$

また (4) を用いれば

$$X \sim g = X \sim s(a) = s(-a) \in s(A)$$

よって、$s(A)$ が $\cup, \cap, \sim,$ について閉じています。[証明終]

既に証明した (命題) ブール代数の同型写像の逆写像は，またブール代数の同型写像である.

（命題終わり）により A と $s(A)$ はブール代数の構造について同型。その同型写像は

$$X = \{x \in P(A) | x \text{ は } A \text{ 上の極大な真のフィルター } \}$$
$$s(a) = \{x \in X | a \in x\}$$
$$s : a \in A \mapsto s(a) \in P(X)$$

で定義される。