Bochnak - Real Algebraic Geometry

ashiato45 take notes

2016 年 3 月 11 日

1 Ordered Fields, Real Closed Fields

1.1 Ordered Fields, Real Fields

- (Definition 1.1.1, ordering of a field): $\leq$ is an ordering of a field $F \iff$
  1. (total): $\leq$ is a total.
  2. (addition): $x \leq y \implies x + z \leq y + z$
  3. (non-negative and mult.): $0 \leq x$, $0 \leq y \implies 0 \leq xy$.
- (Small prop.): $x \leq y$, $z \geq 0 \implies xz \leq yz$. $\because x \leq y \iff 0 \leq y - x \iff 0 \leq (y-x)z \leq 0 \leq yz - xz \iff xz \leq yz$.
- Let's define a ordering of the field of rational function $\mathbb{R}(X)$. (Think X as "infinite small").
- (Example 1.1.2): There exists the unique ordering of $\mathbb{R}(X)$ satisfying
  - it preserves the ordering of $\mathbb{R}$.
  - X is smaller than any positive real number.
  - X is positive.

  $\because$We prove the ordering is unique if any first. Let FC(f) is the coefficient of the lowest term of f for $f \in \mathbb{R}[X]$. (FC stands for Following Coefficient twinned with Leading Coefficient) Let $\mathbb{R}[X]^+ = \{f \in \mathbb{R}[X]; \mathrm{FC}()\}$
  1. $0 < X$ $\because$Requirement.
  2. ${}^\forall a > 0\colon\ X < a$ $\because$Requirement.
  3. $\leq$ preserves the ordering of $\mathbb{R}$. $\because$Requirement.
  4. ${}^\forall a > 0\colon\ {}^\forall n \geq 0\colon\ X^{n+1} < aX^n$
  5. ${}^\forall a > 0\colon\ {}^\forall m > n \geq 0\colon\ X^m < aX^n$
  6. ${}^\forall a > 0, b \in \mathbb{R}\colon\ {}^\forall m > n \geq 0\colon\ bX^m < aX^n$
  7. ${}^\forall a > 0, b \in \mathbb{R}\colon\ {}^\forall m > n \geq 0\colon\ 0 < bX^m + aX^n$
  8. ${}^\forall P(X) \in \mathbb{R}[X]^+\colon\ 0 < P(X)$
  9. ${}^\forall Q(X) \in \mathbb{R}[X]^+\colon\ 0 < \frac{1}{Q(X)}$
  10. ${}^\forall P(X), Q(X) \in \mathbb{R}[X]^+\colon\ 0 < \frac{P(X)}{Q(X)}$
  11. ${}^\forall P(X) \in \mathbb{R}[X]^-, Q(X) \in \mathbb{R}[X]^+\colon\ \frac{P(X)}{Q(X)} < 0$
  12. $$ {}^\forall P(X), R(X) \in \mathbb{R}[X], Q(X), S(X) \in \mathbb{R}[X]^+\colon\ \begin{cases} \mathrm{FC}(PS - RQ) > 0 & \to \frac{P}{Q} > \frac{R}{S} \\ \mathrm{FC}(PS - RQ) = 0 & \to \frac{P}{Q} = \frac{R}{S} \\ \mathrm{FC}(PS - RQ) < 0 & \to \frac{P}{Q} < \frac{R}{S} \end{cases}. \tag{1} $$

  This requirement defines a binary relation $\leq$ (check the sign of FC of the numerator[*1]). We prove it is

[*1] denominator:分母、numerator:分子

exactly an ordering.

- (Reflexivity): Obvious.
- (Anti-symmetry): Obvious.
- (Total): Obvious.
- (Non-negative and mult.): Assume $\frac{P}{Q} \geq 0$ and $\frac{R}{S} \geq 0$. $\mathrm{FC}(P) \geq 0$ and $\mathrm{FC}(R) \geq 0$ hold. Paying attention to managing lowest terms, $\mathrm{FC}(PR) = \mathrm{FC}(P)\mathrm{FC}(R) \geq 0$. This means $\frac{PR}{QS} \geq 0$.
- (Transitivity): Assume $\frac{P}{Q} \leq \frac{R}{S}, \frac{R}{S} \leq \frac{T}{U}$ and $Q, S, U \in \mathbb{R}[X]^+$. By (Non-negative and mult.), they are equivalent to $PSU \leq RQU$ and $RQU \leq TQS$. We write for a polynomial f f's n-th coeffficient f_n. For a pair of polynomials (f, g), let $\varphi(f, g)$ is an n such that $f_0 = g_0, \ldots, f_{n-1} = g_{n-1}$, $f_n \neq g_n$. (If $f = g$, let $\varphi(f, g) = \infty$.) $\varphi(PSU, TQS) = \min(\varphi(PSU, RQU), \varphi(RQU, TQS))$ holds. Let $N = \varphi(PSU, TQS)$.
  - If $N = \infty$ then $\varphi(PSU, RQU) = \varphi(RQU, TQS) = \infty$. This means $PSU = RQU = TQS$.
  - If $N < \infty$ then $(PSU)_0 = (RQU)_0 = (TQS)_0, \ldots, (PSU)_{N-1} = (RQU)_{N-1} = (TQS)_{N-1}$ holds. Moreover, $(PSU)_N \leq (RQU)_N$ and $(RQU)_N \leq (TQS)_N$ hold. This means $PSU \leq TQS$.
- (Addition): Obvious.

- Define $\leq$ of $\mathbb{R}(X)$ as
  1. $$[a_k X^k + \cdots + a_n X^n \geq 0,\, a_k \neq 0,\, k \leq n] \iff [a_k > 0] \tag{2}$$
  2. $$[P(X)/Q(X) > 0] \iff [P(X)Q(X) > 0] \tag{3}$$
- This implies immediately
$$\cdots < X^2 < X < 1 < X^{-1} < X^{-2} < \ldots. \tag{4}$$
- (Small prop.): These two rules generates an ordering of a field (Def. 1.1.1). ☹TODO.
- (Small prop.): $\mathbb{R}(X)$ is not archimedean [*2] i.e.
$$^{\exists}P(X) \in \mathbb{R}(X):\ ^{\forall}n \in \mathbb{N}:\ n < P(X). \tag{5}$$
☹Take $P(X) = 1/X$. Fix $n \in \mathbb{N}$. $X < 1/n$ holds.
$$\begin{align} X < \frac{1}{n} &\iff \frac{1}{n} - X > 0 \tag{6}\\ &\iff \frac{1 - nX}{n} > 0 \tag{7}\\ &\iff 1 - nX > 0 \tag{8}\\ &\iff \frac{1}{X} - n > 0 \tag{9}\\ &\iff \frac{1}{X} > n. \tag{10}\end{align}$$
- This implies $1/X$ is "infinitely large", and X is "infinitely small".
- (Definition, cut): (This is probably not the normal definiton...) A pair of subsets of $\mathbb{R}$ (I, J) is a cut $\iff$
  - $I \cap J = \emptyset$
  - $I \cup J = \mathbb{R}$
  - $I < J$ i.e. $^{\forall}i \in I:\ ^{\forall}j \in J:\ i < j$.
- An ordering of $\mathbb{R}(X)$ deterimnes a cut (I, J) where
$$I = \{x \in \mathbb{R}; x < X\},\ J = \{x \in \mathbb{R}; X < x\}. \tag{11}$$

[*2] Accumulating $1_{\mathbb{R}(X)}$ finitely overwhelms any fixed element of $\mathbb{R}(X)$

$$\text{(an ordering of } \mathbb{R}(X)) \rightsquigarrow \text{(a cut of } \mathbb{R}) \tag{12}$$

Pay attention to forall $x \in \mathbb{R}$ either $x < X$ or $X < x$ holds because the ordering is total.

- (Definition, $-\infty, a_-, a_+, \infty$): Let $a \in \mathbb{R}$. $-\infty, a_-, a_+, \infty$ are defined with cuts.
  - $-\infty := (\emptyset, \mathbb{R})$
  - $a_- := ([-\infty, a[\,, [a, \infty[)$
  - $a_+ := (]-\infty, a]\,,]a, \infty])$
  - $+\infty := (\mathbb{R}, \emptyset)$
- (Small prop.): $Y = -1/X$ is a bijection between $\{\leq (\mathbb{R}(X)); \text{the cut of } \leq \text{ is } -\infty\}$ and $\{\leq (\mathbb{R}(Y))\text{of Def. 1.1.1}\}$. [*3]

  ∵The bijection of $\to$ part is defining a ordering $\mathbb{R}(Y)$ from a fixed ordering $\mathbb{R}(X)$ whose cut is $-\infty$. Define it as $P(Y) \geq 0 \iff P(-1/X) \geq 0$. We have to check the cut of $P(Y)$ is $(]-\infty, 0]\,,]0, \infty[)$. We have to check if $0 < Y$ and $Y <$ (any positive). The other side is omitted.
- (Small prop.): $a \in \mathbb{R}$. $Y = a - X$ is a bijection between $\{\leq (\mathbb{R}(X)); \text{the cut of } \leq \text{ is } a_-\}$ and $\{\leq (\mathbb{R}(Y))\text{of Def. 1.1.1}\}$.
- (Small prop.): $a \in \mathbb{R}$. $Y = X - a$ is a bijection between $\{\leq (\mathbb{R}(X)); \text{the cut of } \leq \text{ is } a_+\}$ and $\{\leq (\mathbb{R}(Y))\text{of Def. 1.1.1}\}$.
- (Small prop.): $Y = 1/X$ is a bijection between $\{\leq (\mathbb{R}(X)); \text{the cut of } \leq \text{ is } +\infty\}$ and $\{\leq (\mathbb{R}(Y))\text{of Def. 1.1.1}\}$.
- (Small prop.): These props states that for each cut, there exists the unique ordering.

  ∵At Def. 1.1.1., we have already seen for cut $(]-\infty, 0]\,,]0, \infty[)$ the ordering whose cut is it is unique. These props states that the number of ordering whose cut is $-\infty, a_-, a_+, \infty$ equals to the number of Def. 1.1.1.'s ordering.
- (Small prop.): This is stated as: there exists bijection

$$\{\text{all orderings of } \mathbb{R}(X)\} \simeq \{a_+; a \in \mathbb{R}\} \cup \{a_-; a \in \mathbb{R}\} \cup \{-\infty, +\infty\}\,. \tag{13}$$

- (Abuse of term.): By the above bijection, we also the orderings by cuts.
- (TODO, p8): Note that the sign of $f \in \mathbb{R}(X)$ for the ordering a_- is the sign of f on some small open interval $]a - \epsilon, a[$.
- (Definition 1.1.3., cone): A cone P of a field [*4] F is a subset P of F such that
  - (Addition): $x, y \in P \implies x + y \in P$
  - (Multiply): $x, y \in P \implies xy \in P$
  - (Square): $x \in K \implies x^2 \in P$

  The cone P is said to be proper if $-1 \notin P$.
- (Small example): $\{0\}$ is obviously a proper cone.
- (Definition 1.1.4., positive cone): Let $(F, \leq)$ be an ordered field. The subset $P = \{x \in F; x \geq 0\}$ is called the positive cone of $(F, \leq)$.
- (Proposition 1.1.5., ordering and cone): Let F be an ordered field. P be a cone.
  - (F is ordered $(F, \leq)$ and P is positive.) $\implies$ ($P \cup (-P) = \mathbb{R}(X)$ and P is proper.)
  - ($P \cup (-P) = \mathbb{R}(X)$ and P is proper.) $\implies$ (F is ordered and its ordering is defined by ($x \leq y \iff y - x \in P$))

  ∵Prove the first half. Proving $-1 \geq 0$ is false is sufficient. Assume $-1 \geq 0$. By (non-negative and mult.), $1 = (-1) \cdot (-1) \leq 0$. By (addition), adding $+1$ both sides yields $0 \leq 1$. Combining them, $1 \leq 0 \leq 1$. This means $0 = 1$. Contradiction.
  Prove the last half.
  - (Reflectivity): Let $x \in F$. Cones always contain $0 = x - x$. This means $x \leq x$.

[*3] $-\infty$ is the cut defined already. Def 1.1.1's cut is $(]-\infty, 0[\,, [0, \infty[)$.
[*4] Need not be ordered.

- (Anti-symmetry): Let $x, y \in F$ and $x \leq y$ and $y \leq x$. $y - x, x - y \in P$ holds. Assume $x - y \neq 0$. By (Multiply), $-(x-y)^2 = (y-x)(x-y) \in P$. Because $x - y \neq 0$, there exists $1/(x-y) \in F$. By (Square), $1/(x-y)^2 \in P$. $-(x-y)^2 \cdot 1/(x-y)^2 = -1 \in P$. This contradicts the properness, so $x - y = 0$.
- (Transitivity): Let $x \leq y \in F$ and $y \leq z \in F$. $y - x \in P$ and $z - y \in P$ hold. By (Addition), $z - x = (z-y) + (y-x) \in P$. This means $x \leq z$.
- (Total): Obvious from $P \cup (-P) = \mathbb{R}(X)$.
- (Addition): Obvious.
- (Non-negative and Mult.): Obvious.

• (Definition, sum of square): The set of sums of squares is denoted by $\sum F^2$.

• (Small prop.): $\sum F^2$ is a cone (not always proper). $\sum F^2$ is contained in every cone of F (smallest!). ∵Obvious.

• (Lemma 1.1.7.): Let P be a proper cone of F.
 (i) If $-a \notin P$ then $P[a] = \{x + ay; x, y \in P\}$ is a proper cone of F.
 (ii) There exists an ordering of F and its positive cone P' such that $P \subset P'$.

∵(i) Assume that $-1 \in P[a]$. There exists $x, y \in P$ such that $-1 = x + ay$. $(-a)y = x + 1$ holds.
- When $y = 0$: $-1 = x \in P$ holds, but this contradicts that P is proper and $-1 \notin P$.
- When $y \neq 0$: There exists $1/y \in F$ and $1/y^2 \in P$ by the property of cones.

$$-a = \frac{x+1}{y} = \underbrace{y}_{\in P} \cdot \underbrace{\frac{1}{y^2}}_{\in P(\text{square})} \cdot (\underbrace{x}_{\in P} + \underbrace{1}_{\in P(\text{Square})}) \in P. \tag{14}$$

This contradicts the assumption.

Both case lead to contradiction, so $-1 \in P[a]$ is false. $-1 \notin P[a]$.

∵(ii)
1. $\mathbb{X}$: Let

$$\mathbb{X} = \{Q' \subset F; P \subset Q',\, Q' \text{ is a proper cone}\}. \tag{15}$$

2. Q: $\mathbb{X}$ is not empty because $P \in \mathbb{X}$. For a chain of $\mathbb{X}$, its union is a upper bound of it. We can apply the Zorn's lemma now, and we obtain a maximal element of $\mathbb{X}$. We name it Q, Q is a maximal element of $\mathbb{X}$.
3. $Q \cup -Q = F$?
 (a) a: Let $a \in F - Q$.
 (b) By (i), $Q[-a]$ is a proper cone.
 (c) Q is maximal (by 2), and $Q[-a]$ is a proper cone containing Q (by b). Hence $Q = Q[-a]$.
 (d) Hence $-a \in Q$.
 (e) (End of a): $Q \cup -Q = F$.
4. Q is proper (by 2) and $Q \cup -Q = F$ (by 3) imply (by Prop. 1.1.5.) the existence of an ordering $\leq$ of F. And Q is positive in the ordering (by Prop. 1.1.5.).

• (Theorem 1.1.8): Let F be a field. The following properties are equivalent:
 (i) F can be ordered.
 (ii) The field F has a proper cone.
 (iii) $-1 \notin \sum F^2$.
 (iv) For every $x_1, \ldots, x_n \in F$,

$$\sum_{i=1}^{n} x_i^2 = 0 \implies x_1 = \cdots = x_n = 0. \tag{16}$$

∵

- (i⇒ ii): By Prop. 1.1.5., the positive cone of F is proper. So the positive cone satisfies the requirement.
- (ii ⇒ iii):
  1. Let the proper cone P.
  2. By (Small prop.), $\sum F^2$ is the smallest cone, so $\sum F^2 \subset P$.
  3. Hence
$$-1 \in F - P \subset F - (\sum F^2). \tag{17}$$
     So
$$-1 \notin \sum F^2. \tag{18}$$
- (iii ⇒ iv):
  1. We prove the contraposition. Assume $\sum_i x_i^2 = 0$ and $x_1 \neq 0$.
  2. $-x_1^2 = \sum_{i=2}^n x_i^2$.
  3. Deviding both side by x_1^2 (by a, we can divide by $x_1 \neq 0$.)
$$-1 = \underbrace{\frac{1}{x_1^2}}_{\in \sum F^2} \underbrace{\sum_{i=2}^n x_i^2}_{\in \sum F^2} \underbrace{\in}_{Cone!} \sum F^2. \tag{19}$$
- (iv ⇒ iii):
  1. We prove the contraposition. Assume $-1 \in \sum F^2$.
  2. There exists $a_1, \ldots, a_n \in F$ such that $-1 = \sum_{i=1}^n a_i^2$ (by 1).
  3. Hence $\sum_{i=1}^n a_i^2 + 1^2 = 0$.

- (Definition 1.1.9.): A field satisfying (Proposition 1.1.8.) is called real.
- (Small prop.): A real field has characteristic 0. ∵Assume the characteristic is finite n. $\sum_{i=1}^n 1^2 = 0$. This contradicts to (Proposition 1.1.8)'s (iv).
- (Proposition 1.1.10.):
  - F: a field such that $\mathbb{Q} \subset P$ (characteristic 0)
  - P: a cone of F

  Then
$$P = \bigcap \underbrace{\{Q; [\leq \text{ is an ordering of } F] \wedge [P \subset Q] \wedge [Q \text{ is a positive cone of } \leq]\}}_{:=\mathbb{X}}. \tag{20}$$
  ∵$\subset$ is obvious. We prove $\supset$.
  1. a: Let $a \in F - P$.
  2. P is proper?
     (a) Assume $-1 \in P$. (Proof by contradiction)
     (b)
$$a = \underbrace{\frac{1}{4}}_{\in \sum F^2} [\underbrace{(1+a)^2}_{\in \sum F^2} \underbrace{-}_{-1 \in P} \underbrace{(1-a)^2}_{\sum F^2}] \in \sum F^2 \overset{\boxed{\text{SoS is smallest}}}{\subset} P. \tag{21}$$
     (the assumption $\mathbb{Q} \subset F$ supports the existence of 1/4)
     (c) This contradicts to 1.
  3. $a \notin P$ (by 1), the properness of P (by 2) and (Lemma 1.1.7.) show that $P[-a]$ is proper.
  4. By (Lemma 1.1.7), there exists an order $\leq$ and its positive cone Q such that $P[-a] \subset Q$ (because $P[-a]$ is proper by 3).
  5. $a \notin Q$?

(a) Assume $a \in Q$. (proof by contradiction)
(b) $-a \in Q$ because $-a \in P[-a] \subset Q$ (by 4).
(c) $-a^2 \in Q$ because Q is a cone (by 4), 1 and 2.
(d) $a \neq 0$ because $a \notin P$, P is a cone (cones always contain zero).
(e) $1/a^2$ is valid and $1/a^2 \in Q$ because Q is a cone.
(f) (c) and (e) say

$$-1 = \underbrace{-a^2}_{\in Q} \cdot \underbrace{(1/a^2)}_{\in Q} \in Q. \tag{22}$$

(g) This contradicts to the properness of Q ((Prop. 1.1.5) says the positive cone is proper.)

6. $P \subset P[-a] \subset Q$.
7. 4 and 6 says $Q \in \mathbb{X}$.
8. This shows

$$a \in F - Q \subset F - (\bigcap \mathbb{X}). \tag{23}$$

9. (End of 1):

$$F - P \subset F - (\bigcap \mathbb{X}). \tag{24}$$

This means

$$\bigcap \mathbb{X} \subset P. \tag{25}$$

- (Corollary 1.1.11.): Let F be a field containing $\mathbb{Q}$. Then

$$\sum F^2 = \bigcap \{Q; [\leq \text{ is an ordering of } F] \wedge [Q \text{ is a positive cone of } \leq]\} \tag{26}$$

∵Use (Prop. 1.1.10.) to $\sum F^2$.

1.2 Real Closed Fields

- (Fact): 体 F と、F 係数既約多項式 $f \in F[X]$ について、$F/(f)$ は体になる。
- (代数拡大): 体 F' が F の代数拡大体であるとは、F' のすべての元が、F 係数多項式の根になっていること。
体 F に、F 係数既約多項式 f の根を追加して体にすることができる。これは、「F にシンボル X を追加して、その X が $f(X) = 0$ となる」という規則を追加することに外ならないので、$F[X]/(f)$ は F の代数拡大となる。(ただし、拡大したつもりでできていないことはありえる。)
- (Fact:代数的閉包): 体 F について、その代数拡大体で、代数的閉体になっているものが存在し、しかも一意である。これを $\overline{F}$ と書くことがある。
- (Definition 1.2.1): real field F が real closed field である $\iff$ F が 非自明な real algebraic extension を持たない i.e. F の真の代数的拡張 $F_1 \supset F$ で、
  - F_1 が real field であり、
  - F_1 が algebraic extension である

  というようなものは存在しない。
- (Theorem 1.2.2.):キモだけ。
  - (i⇒ii):
    - 「hence, $F[\sqrt{a}]$ is not real」: 真に拡張してしまっているので、「real field である」という方がおかしいということになる。
    - 「only one possible ordering」:
      $\sum F^2$ について、F は real なので、$-1 \notin \sum F^2$ となり、$\sum F^2$ は proper cone になっている。よって、Proposition 1.1.5. より、proper cone によって ordering が定まってしまう。

* 「it remains to show that, if $f \in F[X]$ has...」: 奇数次を持つ $f \in F[X]$ が F に根を持たなかったとする。$\deg f = 1$ だと根を持つにきまっているから $\deg f > 1$ としてよい。さらに、$d = \deg f$ として、d より小さい奇数次までは根を持っていたとしてもよい。
  すると、f は既約であるということになる。なぜなら、仮に分解できたら、奇数次を分解するのだから分解した因子のほうに d 次より小さい奇数次の多項式が出てきて、それが仮定より根を持つからである。
* 「The polynomial g_h is symmetric in ...」: Fact として、対称多項式は、その係数の基本対称式の和と積 (つまり多項式) として書くことができる。
  さらに、$y_1, \ldots, y_d$ を根に持つ多項式が f であり、f は F 係数だったのだから、根と係数の関係から $y_1, \ldots, y_d$ の基本対称式は $\in F$ であり、したがって $g_h \in F[X]$ である。
* (range over $\mathbb{Z}$): ハトノスを使う。
* (The field F is real...): なぜか順序が逆に書いてあるので、$a^2 + b^2 = (c^2 + d^2)^2$ まで読めばできる。c, d は、代数的閉体と仮定したので存在する。
* (To conclude..): F の代数的拡張は、$F[X]/(f)$ だが、$F[i]$ は代数的閉体という仮定から、f が既約ならそれは 2 次以下であることがわかる (共役を根に持つから。)。(cf, $\mathbb{C}$ の 2 次拡大はない。)