Bochnak - Real Algebraic Geometry

ashiato45 take notes

2016 年 3 月 22 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 $\mathbb{R}$.[*1]
  - X is smaller than any positive real number.
  - X is positive.

  $\because$We prove the ordering is unique if any first. Let $\mathrm{FC}(f)$ 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. ${}^\forall Q(X) \in \mathbb{R}[X]^+\colon\ 0 < \frac{1}{Q(X)}$ $\because$think of
  $$Q'(X) = \left\{ 1/Q^2; Q > 0 (-1/Q)^2; Q < 0 \right. \quad . \tag{1}$$
  Or assume $0 \geq 1/Q$. Then multiplying Q, $0 \geq 1$. This contradicts to the axiom of fields.
  10. ${}^\forall P(X), Q(X) \in \mathbb{R}[X]^+\colon\ 0 < \frac{P(X)}{Q(X)}$
  11. ${}^\forall P(X) \in \mathbb{R}[X]^-, Q(X) \in \mathbb{R}[X]^+\colon\ \frac{P(X)}{Q(X)} < 0$

[*1] This come from the axiom of fields. Or, for $a \in \mathbb{R}$, $0 < X < a$.

12.

$$
{}^{\forall}P(X),R(X)\in\mathbb{R}[X],Q(X),S(X)\in\mathbb{R}[X]^{+}\colon\ \begin{cases}\mathrm{FC}(PS-RQ)>0 & \to \frac{P}{Q}>\frac{R}{S}\\ \mathrm{FC}(PS-RQ)=0 & \to \frac{P}{Q}=\frac{R}{S}\\ \mathrm{FC}(PS-RQ)<0 & \to \frac{P}{Q}<\frac{R}{S}\end{cases}. \tag{2}
$$

This requirement defines a binary relation $\le$ (check the sign of FC of the numerator[*2]). We prove it is exactly an ordering.

- (Reflexivity): Obvious.
- (Anti-symmetry): Obvious.
- (Total): Obvious.
- (Non-negative and mult.): Assume $\frac{P}{Q}\ge 0$ and $\frac{R}{S}\ge 0$. $\mathrm{FC}(P)\ge 0$ and $\mathrm{FC}(R)\ge 0$ hold. Paying attention to managing lowest terms, $\mathrm{FC}(PR)=\mathrm{FC}(P)\mathrm{FC}(R)\ge 0$. This means $\frac{PR}{QS}\ge 0$.
- (Transitivity): Assume $\frac{P}{Q}\le\frac{R}{S},\frac{R}{S}\le\frac{T}{U}$ and $Q,S,U\in\mathbb{R}[X]^{+}$. By (Non-negative and mult.), they are equivalent to $PSU\le RQU$ and $RQU\le TQS$. 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 $f_0=g_0,\dots,f_{n-1}=g_{n-1}$, $f_n\ne g_n$. (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 $(PSU)_0=(RQU)_0=(TQS)_0,\dots,(PSU)_{N-1}=(RQU)_{N-1}=(TQS)_{N-1}$ holds. Moreover, $(PSU)_N\le(RQU)_N$ and $(RQU)_N\le(TQS)_N$ hold. This means $PSU\le TQS$.
- (Addition): Obvious.

- Define $\le$ of $\mathbb{R}(X)$ as
  1.
  $$
  [a_kX^k+\cdots+a_nX^n\ge 0,\ a_k\ne 0,\ k\le n]\iff[a_k>0] \tag{3}
  $$
  2.
  $$
  [P(X)/Q(X)>0]\iff[P(X)Q(X)>0] \tag{4}
  $$
- This implies immediately
$$
\cdots<X^2<X<1<X^{-1}<X^{-2}<\dots. \tag{5}
$$
- (Small prop.): These two rules generates an ordering of a field (Def. 1.1.1). ∵TODO.
- (Small prop.): $\mathbb{R}(X)$ is not archimedean [*3] i.e.
$$
{}^{\exists}P(X)\in\mathbb{R}(X)\colon\ {}^{\forall}n\in\mathbb{N}\colon\ n<P(X). \tag{6}
$$
∵Take $P(X)=1/X$. Fix $n\in\mathbb{N}$. $X<1/n$ holds.
$$
\begin{aligned}
X<\frac{1}{n} &\iff \frac{1}{n}-X>0 && (7)\\
&\iff \frac{1-nX}{n}>0 && (8)\\
&\iff 1-nX>0 && (9)\\
&\iff \frac{1}{X}-n>0 && (10)\\
&\iff \frac{1}{X}>n. && (11)
\end{aligned}
$$
- This implies $1/X$ is "infinitely large", and X is "infinitely small".

[*2] denominator:分母、numerator:分子

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

- (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. ${}^\forall i \in I\colon\ {}^\forall j \in J\colon\ i < j$.
- An ordering of $\mathbb{R}(X)$ deterimnes a cut (I, J) where

$$I = \{x \in \mathbb{R}; x < X\}\,,\ J = \{x \in \mathbb{R}; X < x\}\,. \tag{12}$$

$$(\text{an ordering of } \mathbb{R}(X)) \rightsquigarrow (\text{a cut of } \mathbb{R}) \tag{13}$$

  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 $\{\leq (\mathbb{R}(Y))\text{of Def. 1.1.1}\}$. [*4]

  ∵The bijection of $\rightarrow$ 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

$$\{\text{all orderings of } \mathbb{R}(X)\} \simeq \{a_+; a \in \mathbb{R}\} \cup \{a_-; a \in \mathbb{R}\} \cup \{-\infty, +\infty\}\,. \tag{14}$$

- (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 [*5] 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.

[*4] $-\infty$ is the cut defined already. Def 1.1.1's cut is $(]-\infty, 0[\,, [0, \infty[)$.

[*5] Need not be ordered.

– (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 $x \leq x$.
– (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.

$$-a = \frac{x+1}{y} = \underbrace{y}_{\in P} \cdot \underbrace{\frac{1}{y^2}}_{\in P(\text{square})} \cdot (\underbrace{x}_{\in P} + \underbrace{1}_{\in P(\text{Square})}) \in P. \tag{15}$$

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

$$\mathbb{X} = \{Q' \subset F; P \subset Q', Q' \text{ is a proper cone}\}. \tag{16}$$

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 $x_1, \ldots, x_n \in F$,

$$\sum_{i=1}^{n} x_i^2 = 0 \implies x_1 = \cdots = x_n = 0. \tag{17}$$

∵

- (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
  $$-1 \in F - P \subset F - (\sum F^2). \tag{18}$$
  So
  $$-1 \notin \sum F^2. \tag{19}$$
- (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 $x_1 \neq 0$.)
  $$-1 = \underbrace{\frac{1}{x_1^2}}_{\in \sum F^2} \underbrace{\sum_{i=2}^{n} x_i^2}_{\in \sum F^2} \underbrace{\in}_{Cone!} \sum F^2. \tag{20}$$
- (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
  $$P = \bigcap \underbrace{\{Q; [\leq \text{ is an ordering of } F] \wedge [P \subset Q] \wedge [Q \text{ is a positive cone of } \leq]\}}_{:=\mathbb{X}}. \tag{21}$$
  ∵$\subset$ 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)
     $$a = \underbrace{\frac{1}{4}}_{\in \sum F^2} [\underbrace{(1+a)^2}_{\in \sum F^2} \underbrace{-}_{-1 \in P} \underbrace{(1-a)^2}_{\sum F^2}] \in \sum F^2 \overset{\boxed{\text{SoS is smallest}}}{\subset} P. \tag{22}$$

(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
$$-1 = \underbrace{-a^2}_{\in Q} \cdot \underbrace{(1/a^2)}_{\in Q} \in Q. \tag{23}$$
   (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
$$a \in F - Q \subset F - (\bigcap \mathbb{X}). \tag{24}$$
9. (End of 1):
$$F - P \subset F - (\bigcap \mathbb{X}). \tag{25}$$
   This means
$$\bigcap \mathbb{X} \subset P. \tag{26}$$

- (Corollary 1.1.11.): Let F be a field containing $\mathbb{Q}$. Then
$$\sum F^2 = \bigcap \{Q; [\leq \text{ is an ordering of } F] \wedge [Q \text{ is a positive cone of } \leq]\} \tag{27}$$
  ∵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。[*6]
- (代数拡大って具体的には？): 次の命題がある。
  - (雪江 3.1.23): K を体、f を K 上既約で $\deg f = n$ とする。このとき、次の 3 つが成り立つ。
    (1) $L = K[x]/(f)$ は体で、$[L : K] = n$ である。
    (2) $\alpha = x + (f)$ とおくと、$f(\alpha) = 0$
    (3) L の K 上の基底として $B = \{1, \ldots, \alpha^{n-1}\}$ をとれる。

[*6] 戯言: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。)

– つまり、(1,2) 体について既約多項式を考えて、その根が含まれるような代数拡大体が存在する。(3) その基底は単項式たち。

- (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。[Yukie, Theorem 3.2.3, Corollary 3.2.4].
- (Gauss の対称式の定理): See [Cox].
- (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.):
  - (i⇒ii):
    1. (First half starts): Let $a \in F$ and a is not a square in F.
    2. $F[\sqrt{a}] = F[X]/(X^2 - a)$. Hence $X^2 - a$ is (by 1) irreducible, $F[X]/(X^2 - a)$ is a nontrivial algebraic extension of F.
    3. (2), (Definition 1.2.1) and (Assumption i) imply $F[\sqrt{a}]$ is not real.
    4. By (3) and (Theorem 1.1.8, iii), $-1 \in F[\sqrt{a}]$. So there exists $x_i, y_i \in F$
    $$-1 = \sum_{i=1}^{n} (x_i + \sqrt{a} y_i)^2. \tag{28}$$
    5. Hence 1 and $\sqrt{a}$ are linearly independent in vector space $F[\sqrt{a}]$ [*7], picking the coefficients of 1,
    $$-1 = \sum_{i=1}^{n} x_i^2 + a(\sum_{i=1}^{n} y_i^2) \tag{29}$$
    in F.
    6. Since F is real and (Theorem 1.1.8, iii)
    $$\underbrace{-1 - \sum_{i=1}^{n} x_i^2}_{\neq 0} = a \sum_{i=1}^{n} y_i^2. \tag{30}$$
    So $\sum_{i=1}^{n} y_i^2 \neq 0$. (Strictly speaking, we need the fact F be an integral domain.)
    7. We can divide by $\sum_i y_i^2$,
    $$-a = \frac{1 + \sum_{i=1}^{n} x_i^2}{\sum_{i=1}^{n} y_i^2} \in \sum F^2. \tag{31}$$
    8. (End of 1): Forall $a \in F$,
       * if a is a square $\to a \in \sum F^2$,
       * (by 1-7) if a is not a square $\to a \in -\sum F^2$.

       Hence
    $$a \in \sum F^2 \cup -\sum F^2. \tag{32}$$
    9.
    $$F = \sum F^2 \cup -\sum F^2. \tag{33}$$
    10. By (Theorem 1.1.8), $\sum F^2$ is a proper cone. In this situation, (Proposition 1.1.5) says $\sum F^2$ generates an ordering of F. And $\sum F^2$.

[*7] Remember $F[\sqrt{a}]$ is a quotient of $F[X]$.

11. Assume if another ordering exists. Let its positive cone P. By (Theorem 1.1.5) $P \cup -P = F$. $\sum F^2$ is the smallest cone, so

$$F \overset{\boxed{9}}{=} \sum F^2 \cup -\sum F^2 \subset P \cup -P = F. \tag{34}$$

So $\sum F^2 \cup -\sum F^2 = P \cup -P$. Asserting $\sum F^2 \cap -\sum F^2 = \emptyset$ and $P \cap -P =$, $\sum F^2 = P$. This means the ordering of P and $\sum F^2$ coincides.

12. (First half end): (10) and (11) says there exists unique ordering for F and its positive cone is $\sum F^2$.
13. (Last half starts) : Let $f \in F[X]$ has odd degree. We want to prove f have a root in F, so we negate this proposition. Assume f have no roots in F. Let $d = \deg f$.
14. We can assume $d > 1$ because if $d = 1$ then obviously f have the root in F.
15. We can assume that polynomials whose degree is $< d$ have a root in F. [*8]
16. (**ODD**) f is irreducible. $\because$Assume f is reducible and there exists decomposition $f = gh$ $(\deg g, \deg h > 0)$. Then $\deg g, \deg h < d$. $\deg g + \deg h = \deg f$ and $\deg f$ is odd, so Either $\deg g$ or $\deg h$ is odd. Without loss of generality, we can assume $\deg g$ is odd. So by (15) g have a root in F. So f have a root as the root of g. This contradicts to (13).
17. $F[X]/(f)$ is a nontrivial extension of F. By (Assumption i), $F[X]/(f)$ is not real. So $-1 \bmod (f) \in \sum (F[X]/(f))^2$.
18. There exists $h_i \in F[X], \deg(h_i) < d$ and $g \in F[X]$ such that

$$-1 = \sum_{i=1}^{n} h_i^2 + fg. \tag{35}$$

Pay attention to $\deg(h_i) < d \iff \deg(h_i) \leq d - 1$. (the assumption $\deg(h_i) < d$ is from the fact that the ring is a quotient of f.)

19. Calculate the degree of both sides of $-1 - \sum_{i=1}^{n} h_i^2 = fg$.

$$\begin{aligned} d + \deg(g) &= \deg(f) + \deg(g) && (36)\\ &= \deg(fg) && (37)\\ &= \deg(-1 - \sum_{i=1}^{n} h_i^2) && (38)\\ &\leq \max_i \deg(h_i^2) && (39)\\ &= 2 \max_i \deg(h_i) && (40)\\ &\leq 2(d-1) && (41)\\ &= 2d - 2. && (42) \end{aligned}$$

20. $\deg(g) \leq d - 2$.
21. Seeing the equation of (18), $\deg(-1) = 0$, $\deg(\sum_i h_i^2)$ is odd and $\deg(f)$ is odd, so $\deg(g)$ is odd.
22. By (19), (20) and (15), g has a root in F. Let the root x.
23. Substitute x in the equation of (18).

$$-1 = \sum_{i=1}^{n} h_i^2(x) + f(x)g(x) \overset{\boxed{22}}{=} \sum_{i=1}^{n} h_i^2(x). \tag{43}$$

24. This means $-1 \in \sum F^2$. This contradicts to F be the real. (by (12), $\sum F^2$ is a positive cone.)

– (ii ⇒ iii):

[*8] Strictly, this is proved by the well-ordering set. $\{d; f \text{has no roots}\}$ is not empty because the assumption. This have the smallest element. Take a polynomial that realize the smallest element.

1. (First half starts): Let $f \in F[X]$. Set $d = \deg f$. We will prove that f have a root in $F[i]$.
2. Write $d = 2^m n$ (n is odd).
3. Prove f has a root in $F[i]$ by induction on m. The case of $m = 0$ is obvious from the assumption. Assume that the case of $m - 1$ holds.
4. Take $y_1, \dots, y_d$ to be the roots of f in $\overline{F}$.
5. Define for all $h \in \mathbb{Z}$ an element of $F[X]$

$$g_h = \prod_{1 \leq \lambda < \mu \leq d} (X - y_\lambda - y_\mu - h y_\lambda y_\mu). \tag{44}$$

X6 g_h is symmetry in $y_1, \dots, y_d$, so (by Gauss) $g_h \in F[(y_1 + \cdots + y_d), \dots, (y_1 \dots y_d)]$.

6. The coefficients of g_h are symmetry in $y_1, \dots, y_d$, so (by Gauss) the coefficients of g_h are in $F[(y_1 + \cdots + y_d), \dots, (y_1 \dots y_d)]$.
7. $y_1, \dots, y_d$ are the roots of $f \in F[X]$, so $(y_1 + \cdots + y_d), \dots, (y_1 \dots y_d) \in F$.
8. By (5) and (6), $g_h \in F$.
9.

$$\deg g_h = {}_dC_2 = \frac{d(d-1)}{2} = \frac{2^m n \cdot (2^m n - 1)}{2} = 2^{m-1} \underbrace{(2^m n - 1) n}_{\text{odd}}. \tag{45}$$

10. Assumption of induction says g_h have a root in $F[i]$.
11.

$$^\forall h \in \mathbb{Z}\colon\ ^\exists 1 \leq \lambda_h < \mu_h \leq d\colon\ y_{\lambda_h} + y_{\mu_h} + h y_{\lambda_h} y_{\mu_h} \in F[i]. \tag{46}$$

12. The pairs of (λ_h, μ_h) is finite, but h runs over $\mathbb{Z}$. By pigeonhole principle, there exist different integers h, h' such that $(\lambda_h, \mu_h) = (\lambda_{h'}, \mu_{h'})$. We call this pair (λ, μ).

$$y_\lambda + y_\mu + h y_\lambda y_\mu, \quad y_\lambda + y_\mu + h' y_\lambda y_\mu \in F[i]. \tag{47}$$

13.

$$y_\lambda + y_\mu \in F[i], \quad y_\lambda y_\mu \in F[i]. \tag{48}$$

14. 2nd degree equation with $F[i]$ coefficients have their roots in $F[i]$?
    (a) $x^2 = a + bi$ ($a, b \in F$) have a root in $F[i]$?
        i. If $b = 0$ and $a \geq 0$ [*9] then we can take the square root of $a \in F_+ = \sum F^2$ (assumption ii). We call the positive square root of $a \in F_+$ as $\sqrt{a}$. If $b = 0$ and $a \leq 0$ then we can take the square root $\sqrt{-a} i$. So we can assume $b \neq 0$.
        ii. Set

$$L = \sqrt{a^2 + b^2}, \quad p = \frac{L + (a + bi)}{2}, \quad M = \frac{\sqrt{(L+a)^2 + b^2}}{2}, \ q = \frac{p}{M}\sqrt{L}. \tag{49}$$

$M \neq 0$ because $b \neq 0$.

        iii. $q^2 = a + bi$ holds. ∵

$$\begin{aligned} q^2 &= \frac{4}{(L+a)^2 + b^2} \cdot \frac{(L + a + bi)^2}{4} \cdot L & (50)\\ &= \frac{(L+a)^2 - b^2 + 2(L+a)bi}{L^2 + 2aL + a^2 + b^2} L & (51)\\ &= \frac{L^2 + 2aL + a^2 - b^2 + 2(L+a)bi}{2L^2 + 2aL} L & (52)\\ &= \frac{2a^2 + 2aL + 2(L+a)bi}{2L + 2a} & (53)\\ &= a + bi. & (54) \end{aligned}$$

[*9] By assumption ii, we can detrermine if a number is positive or negative.

(b) $ax^2+bx+c=0$ $(a,b,c \in F[i])$ have a root in $F[i]$. ∵If $a=0$ then obvious. If $a \neq 0$, we can make the completing square, so we can solve the equation by (a).

15. $y_\lambda, y_\mu \in \overline{F}$ are the roots of $X^2-(y_\lambda+y_\mu)X+y_\lambda y_\mu$. This polynomial have $F[i]$ coefficients by (13). By (14), the roots are in $F[i]$, so $y_\lambda, y_\mu \in F[i]$.
16. (First half ends): Hence f has a root in $F[i]$.
17. (Last half starts): Let $f \in F[i][X]$.
18. $f\overline{f} \in F[X]$ holds. ∵Write f as $\sum_j (a_j+ib_j)x^j$.

$$\begin{aligned}
f\overline{f} &= [\sum_j (a_j+ib_j)x^j] \cdot [\sum_k (a_k+ib_k)x^k] && (55)\\
&= [\sum_j (a_j+ib_j)(a_j-ib_j)x^{2j}] + [\sum_{j>k}(a_j+ib_j)(a_k-ib_k)x^{j+k}] + [\sum_{j<k}(a_j-ib_j)(a_k+ib_k)x^{j+k}] && (56)\\
&= \sum_j (a_j^2+b_j^2)x^{2j} + 2\sum_{j>k}(a_ja_k+b_jb_k)x^{j+k} && (57)\\
&\in F[X]. && (58)
\end{aligned}$$

19. By (1-16), $f\overline{f}$ has a root x in $F[i]$. So x is a root of f or a root of $\overline{f}$ [*10] . If x is a root of f, we complete the proof. If x is a root of $\overline{f}$, $\overline{x}$ is a root of f (Take an allover conjugate).

– (iii ⇒ i):
  1. F is real? (We will prove $-1 \notin F$ and use Theorem 1.1.8)
     (a) The solutions of $X^2=-1$ are only $i, -i$. [*11]
     (b) $i, -i \notin F$, so $-1 \notin F^2$.
     (c) $F^2 = \sum F^2$? ($\subset$ is obvious. We will prove only $\supset$.)
        i. It is sufficient to prove for all $a, b \in F$ there exists $x \in F$ such that $a^2+b^2=x^2$.
        ii. Let $c, d \in F$ as $a+ib=(c+id)^2$. Take c, d exists because $F[i]$ is algebraically closed.
        iii. We can take x as c^2+d^2.∵

$$\begin{aligned}
x^2 &= (c^2+d^2)^2 && (59)\\
&= c^4+2c^2d^2+d^4 && (60)\\
&= (c^2-d^2)^2+4c^2+d^2 && (61)\\
&\overset{\boxed{\text{ii}}}{=} a^2+b^2. && (62)
\end{aligned}$$

     (d) By (b) and (c), $-1 \notin \sum F^2$. By Theorem 1.1.8, F is real.
  2. $F[i]$ is the only nontrivial algebraic extension because $F[i]$ is (by assumption iii) algebraically closed. (If we intend to add a root x of f to F, $x \in F[i]$.)
  3. $-1 \in \sum (F[i])^2$ because $i^2=-1 \in F[i]$.
  4. $F[i]$ is not real.
  5. By (2) and (4), all the algebraic extensions of F are not real.
  6. By (1) nad (5), F is real closed.

- (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」:

[*10] Assume x is not a root of neither. $f(x) \neq 0$ and $\overline{f}(x) \neq 0$. So $f(x)\overline{f}(x) \neq 0$. But this is a contradiction.
[*11] "Since $F[i]$ is a field." is nonsense to me.

$\sum F^2$ 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。)

- (Example 1.2.3):
  - ($\mathbb{R}$): $\mathbb{C} = \mathbb{R}[i]$, and $\mathbb{C}$ is algebraically closed. Use (iii).
  - ($\mathbb{R}_{\mathrm{alg}}$):
    * (Field): Let $a, b \in \mathbb{R}_{\mathrm{alg}}$. $\mathbb{Q} \subset \mathbb{Q}[a, b] \subset \mathbb{R}_{\mathrm{alg}}$ and $\mathbb{Q}[a, b]$ is an algebraic extension of $\mathbb{Q}$. So $a + b \in \mathbb{Q}[a, b] \subset \mathbb{R}_{\mathrm{alg}}$ and $ab \in \mathbb{Q}[a, b]$. If $a \neq 0$ then $a^{-1} \in \mathbb{Q}[a] \subset \mathbb{R}_{\mathrm{alg}}$.
    * (point): $\mathbb{R}_{\mathrm{alg}}$-coefficient polynomial's roots are in $\mathbb{R}_{\mathrm{alg}}$. $\because x$ is a root of $a_n x^n + \cdots + a_0 = 0$ ($a_i \in \mathbb{R}_{\mathrm{alg}}$).

$$a_0, \ldots, a_n \in \mathbb{Q}[a_0, \ldots, a_n]. \tag{63}$$

Because $a_0, \ldots, a_n$ are algebraic over $\mathbb{Q}$, $\mathbb{Q}(a_0, \ldots, a_n)$ is an algebraic extension of $\mathbb{Q}$. So $[\mathbb{Q}(a_0, \ldots, a_n) : \mathbb{Q}] < \infty$. $\mathbb{Q}(a_0, \ldots, a_n)(x)$ is an algebraic extension of $\mathbb{Q}(a_0, \ldots, a_n)$. So $[\mathbb{Q}(a_0, \ldots, a_n, x) : \mathbb{Q}(a_0, \ldots, a_n)] < \infty$. By a fact,

$$[\mathbb{Q}(a_0, \ldots, a_n, x) : \mathbb{Q}] = [\mathbb{Q}(a_0, \ldots, a_n, x) : \mathbb{Q}(a_0, \ldots, a_n)][\mathbb{Q}(a_0, \ldots, a_n), \mathbb{Q}] < \infty. \tag{64}$$

So $\mathbb{Q}(a_0, \ldots, a_n, x)$ is an algebraic extension of $\mathbb{Q}$ (think of $1, x, x^2, \ldots$. We have a linearly dependent.). So x is algebraic over $\mathbb{Q}$, then $x \in \mathbb{R}_{\mathrm{alg}}$.
    * (unique ordering): We will prove $\sum(\mathbb{R}_{\mathrm{alg}})^2 = \mathbb{R}_{\mathrm{alg}_{\geq 0}}$. If $a \in \mathbb{R}_{\mathrm{alg}}$ and $a \geq 0$ then $\sqrt{a} \in \mathbb{R}$. Because a is a root of $\mathbb{R}_{\mathrm{alg}}$-coefficient $X^2 - a$. So $\sqrt{a} \in \mathbb{Q}[\sqrt{a}] \subset \mathbb{R}_{\mathrm{alg}}$. We have $\sum(\mathbb{R}_{\mathrm{alg}})^2 \cup -\sum(\mathbb{R}_{\mathrm{alg}})^2 = \mathbb{R}_{\mathrm{alg}_{\geq 0}} \cup \mathbb{R}_{\mathrm{alg}_{\leq 0}} = \mathbb{R}_{\mathrm{alg}}$. So induced ordering by $\mathbb{R}$ is the unique ordering of $\mathbb{R}_{\mathrm{alg}}$.
    * (odd polynomial): $f = a_n x^n + \cdots + a_0$ is odd degree ($a_i \in \mathbb{R}_{\mathrm{alg}}$). f have a root in $\mathbb{R}$. By (point), the root in $\mathbb{R}_{\mathrm{alg}}$.
    * (real closed): Use (ii).
  - (Puiseux series with real coefficients): $\mathbb{R}(X)\hat{}$ is a set of formal series:

$$\mathbb{R}(X)\hat{} = \left\{ \sum_{i=k}^{\infty} a_i X^{i/q} ; k \in \mathbb{Z}, q \in \mathbb{N} - \{0\}, a_i \in \mathbb{R} \right\}. \tag{65}$$

$\mathbb{C}(X)\hat{}$ is similiar. $\mathbb{R}(X)\hat{}$ is real closed. $\because$It is known that $\mathbb{C}(X)\hat{}$ is algebraically closed. $\mathbb{C}(X)\hat{} = \mathbb{R}(X)\hat{}[i]$ because

$$\sum_{i=k}^{\infty} (a_i + \sqrt{-1} b_i) X^{i/q} = \sum_{i=k}^{\infty} a_i X^{i/q} + \sqrt{-1} \sum_{i=k}^{\infty} b_i X^{i/q}. \tag{66}$$

- A positive element of $\widehat{\mathbb{R}(X)}$ is a Puiseux series of the form $\sum_{i=k}^{\infty} a_i x^{i/q}$ with $a_k > 0$. ∵We need to prove that it is square. Think of a square of an element of $\widehat{\mathbb{R}(X)}$.

$$(\sum_{i=k}^{\infty} b_i X^{i/2q})^2 = (\sum_{i=k}^{\infty} b_i X^{i/2q})(\sum_{i=k}^{\infty} b_i X^{i/2q}) \tag{67}$$

$$= \sum_{d=2k}^{\infty} \sum_{i=0}^{d-2k} b_{k+i} b_{(d-2k)-i} X^{d/2q} \tag{68}$$

$$= b_k^2 X^{2k/2q} + (b_k b_{k+1} + b_{k+1} b_k) X^{(2k+1)/2q} + \dots. \tag{69}$$

So we can set $b_k = \sqrt{a_k}$ and $b_{k+1}, \dots$ recursively. If $a_k < 0$, we cannot make such a process.

- We use the same interval symbols $[a, b]$, $]a, b[$.
- (Proposition 1.2.4):
  - $\mathbb{R}$: real closed field
  - $f \in R[X]$
  - $a, b \in R$: $a < b$
  - $f(a)f(b) < 0$

  then there exists $x \in]a, b[$ such that $f(x) = 0$.

  ∵

  1. By (iii) of the (Theorem 1.2.2), the irreducible factors of f are linear or have the form of $(X - (c + di))(X - (c - di)) = (X - c)^2 + d^2$ for $c, d \in R$.
  2. The latters don't yield opposite sign.
  3. There exists a linear factor of f who has opposite sign at a and b. Name it $g(X) = X - x$. Now, x is a root of f. $g(a)g(b) < 0$.
  4. g is strictly increasing, so $g(a) < 0$ and $g(b) > 0$. So $g(a) < g(x) = 0 < g(b)$. By increasingness, $a < x < b$.
- (Proposition 1.2.5):
  - R: real closed field
  - $f \in R[X]$
  - $a, b \in R$: $a < b$, $f(a) = f(b) = 0$

  then f' has a root in $]a, b[$.

  ∵

  1. We can suppose that a and b are two consecutive roots of f, i.e. f never vanishes in $]a, b[$. (We can replace nearer roots if they are not consecutive.)
  2. Factorize f as

  $$f = (X - a)^m (X - b)^n g \tag{70}$$

  where g never vanishes in $]a, b[$.
  3. Differentiate f (algebraic derivative)

  $$f' = m(X - a)^{m-1}(X - b)^n g + (X - a)^m n(X - b)^{n-1} g + (X - a)^m (X - b)^n g' \tag{71}$$

  $$= (X - a)^{m-1}(X - b)^{n-1} \underbrace{[m(X - b)g + n(X - a)g + (X - a)(X - b)g']}_{:=g_1}. \tag{72}$$

  4. $g(a)$ and $g(b)$ have the same signs because (2) and the contraposition of (Proposition 1.2.4).
  5. $g_1(a) = m(a - b)g(a)$ and $g_1(b) = n(b - a)g(b)$, hence $g_1(a)$ and $g_1(b)$ have opposite signs.
  6. By (Proposition 1.2.4), g_1 has a root in $]a, b[$ and so does f'.
- (Corollary 1.2.6):
  - R: real closed field

- $f \in R[X]$
- $a, b \in R$: $a < b$

then there exists $c \in]a, b[$ such that $f(b) - f(a) = (b - a)f'(c)$. ∵

1. Let $g(x) = f(x) - [\frac{f(b)-f(a)}{b-a}(x - a) + f(a)]$.
2. $g(a) = 0$ obviously holds.

$$g(b) = f(b) - [\frac{f(b) - f(a)}{b - a}(b - a) + f(a)] = 0. \tag{73}$$

3. Apply (Proposition 1.2.6) to g.

- (Corollary 1.2.7):
  - R: real closed field
  - $f \in R[X]$
  - $a, b \in R$: $a < b$
  - f' is positive (resp. negative) on $]a, b[$

  then f is strictly increasing (resp. strictly decreasing) on $[a, b]$.

  ∵Obvious from (Corollary 1.2.6).
-