

Bochnak - Real Algebraic Geometry

ashiato45 take notes

2016 年 4 月 18 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.): $x \leq y, z \geq 0 \implies xz \leq yz$. $0 \leq y \iff 0 \leq y - x \iff 0 \leq (y - x)z \leq 0 \leq yz - xz \iff xz \leq yz$.
- 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.

○We prove the ordering is unique if any first. Let $\text{FC}(f)$ 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 $\mathbb{R}[X]^+ = \{f \in \mathbb{R}[X]; \text{FC}(\cdot)\}$

1. $0 < X$ ○Requirement.
2. $\forall a > 0: X < a$ ○Requirement.
3. \leq preserves the ordering of \mathbb{R} . ○Requirement.
4. $\forall a > 0: \forall n \geq 0: X^{n+1} < aX^n$
5. $\forall a > 0: \forall m > n \geq 0: X^m < aX^n$
6. $\forall a > 0, b \in \mathbb{R}: \forall m > n \geq 0: bX^m < aX^n$
7. $\forall a > 0, b \in \mathbb{R}: \forall m > n \geq 0: 0 < bX^m + aX^n$
8. $\forall P(X) \in \mathbb{R}[X]^+: 0 < P(X)$
9. $\forall Q(X) \in \mathbb{R}[X]^+: 0 < \frac{1}{Q(X)}$ ○think of

$$Q'(X) = \left\{ 1/Q^2; Q > 0(-1/Q)^2; Q < 0 \right\} . \quad (1)$$

Or assume $0 \geq 1/Q$. Then multiplying Q , $0 \geq 1$. This contradicts to the axiom of fields.

10. $\forall P(X), Q(X) \in \mathbb{R}[X]^+: 0 < \frac{P(X)}{Q(X)}$
11. $\forall P(X) \in \mathbb{R}[X]^-, Q(X) \in \mathbb{R}[X]^+: \frac{P(X)}{Q(X)} < 0$

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

12.

$$\forall P(X), R(X) \in \mathbb{R}[X], Q(X), S(X) \in \mathbb{R}[X]^+ : \begin{cases} \text{FC}(PS - RQ) > 0 & \rightarrow \frac{P}{Q} > \frac{R}{S} \\ \text{FC}(PS - RQ) = 0 & \rightarrow \frac{P}{Q} = \frac{R}{S} \\ \text{FC}(PS - RQ) < 0 & \rightarrow \frac{P}{Q} < \frac{R}{S} \end{cases} \quad (2)$$

This requirement defines a binary relation \leq (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 $\frac{P}{Q} \geq 0$ and $\frac{R}{S} \geq 0$. $\text{FC}(P) \geq 0$ and $\text{FC}(R) \geq 0$ hold. Paying attention to managing lowest terms, $\text{FC}(PR) = \text{FC}(P)\text{FC}(R) \geq 0$. 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 coefficient f_n . For a pair of polynomials (f, g) , let $\varphi(f, g)$ is an n such that $f_0 = g_0, \dots, f_{n-1} = g_{n-1}, f_n \neq g_n$. (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 $(PSU)_0 = (RQU)_0 = (TQS)_0, \dots, (PSU)_{N-1} = (RQU)_{N-1} = (TQS)_{N-1}$ 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.

$$[a_k X^k + \dots + a_n X^n \geq 0, a_k \neq 0, k \leq n] \iff [a_k > 0] \quad (3)$$

2.

$$[P(X)/Q(X) > 0] \iff [P(X)Q(X) > 0] \quad (4)$$

- This implies immediately

$$\dots < X^2 < X < 1 < X^{-1} < X^{-2} < \dots \quad (5)$$

- (Small prop.): These two rules generates an ordering of a field (Def. 1.1.1). \bigcirc TODO.
- (Small prop.): $\mathbb{R}(X)$ is not archimedean ^{*3} i.e.

$$\exists P(X) \in \mathbb{R}(X) : \forall n \in \mathbb{N} : n < P(X). \quad (6)$$

\bigcirc Take $P(X) = 1/X$. Fix $n \in \mathbb{N}$. $X < 1/n$ holds.

$$X < \frac{1}{n} \iff \frac{1}{n} - X > 0 \quad (7)$$

$$\iff \frac{1 - nX}{n} > 0 \quad (8)$$

$$\iff 1 - nX > 0 \quad (9)$$

$$\iff \frac{1}{X} - n > 0 \quad (10)$$

$$\iff \frac{1}{X} > n. \quad (11)$$

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

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

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

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 $\{\leq (\mathbb{R}(X))\}$; the cut of \leq is $-\infty$ and $\{\leq (\mathbb{R}(Y))\}$ 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 $Y < (\text{any positive})$. The other side is omitted.

- (Small prop.): $a \in \mathbb{R}$. $Y = a - X$ is a bijection between $\{\leq (\mathbb{R}(X))\}$; the cut of \leq is a_- and $\{\leq (\mathbb{R}(Y))\}$ of Def. 1.1.1}.
- (Small prop.): $a \in \mathbb{R}$. $Y = X - a$ is a bijection between $\{\leq (\mathbb{R}(X))\}$; the cut of \leq is a_+ and $\{\leq (\mathbb{R}(Y))\}$ of Def. 1.1.1}.
- (Small prop.): $Y = 1/X$ is a bijection between $\{\leq (\mathbb{R}(X))\}$; the cut of \leq is $+\infty$ and $\{\leq (\mathbb{R}(Y))\}$ 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

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

- (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.

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

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

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

2. Q : \mathbb{X} is not empty because $P \in \mathbb{X}$. For a chain of \mathbb{X} , its union is an 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 $x_1, \dots, x_n \in F$,

$$\sum_{i=1}^n x_i^2 = 0 \implies x_1 = \dots = x_n = 0. \quad (17)$$

○

- (i \Rightarrow ii): By Prop. 1.1.5., the positive cone of F is proper. So the positive cone satisfies the requirement.
- (ii \Rightarrow 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

$$-1 \in F - P \subset F - (\sum F^2). \quad (18)$$

So

$$-1 \notin \sum F^2. \quad (19)$$

- (iii \Rightarrow 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. Dividing both side by x_1^2 (by a, we can divide by $x_1 \neq 0$.)

$$-1 = \underbrace{\frac{1}{x_1^2}}_{\in \sum F^2} \underbrace{\sum_{i=2}^n x_i^2}_{\in \sum F^2} \underbrace{\in}_{\text{Cone!}} \sum F^2. \quad (20)$$

- (iv \Rightarrow iii):

1. We prove the contraposition. Assume $-1 \in \sum F^2$.
2. There exists $a_1, \dots, a_n \in F$ 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

$$P = \bigcap \underbrace{\{Q; [\le \text{ is an ordering of } F] \wedge [P \subset Q] \wedge [Q \text{ is a positive cone of } \le]\}}_{:=\mathbb{K}}. \quad (21)$$

○ \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)

$$a = \underbrace{\frac{1}{4}}_{\in \sum F^2} \underbrace{[(1+a)^2]}_{\in \sum F^2} \underbrace{-}_{-1 \in P} \underbrace{(1-a)^2}_{\in \sum F^2} \in \sum F^2 \overset{\boxed{\text{SoS is smallest}}}{\subset} P. \quad (22)$$

(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

$$-1 = \underbrace{-a^2}_{\in Q} \cdot \underbrace{(1/a^2)}_{\in Q} \in Q. \quad (23)$$

- (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

$$a \in F - Q \subset F - (\bigcap \mathbb{X}). \quad (24)$$

- 9. (End of 1):

$$F - P \subset F - (\bigcap \mathbb{X}). \quad (25)$$

This means

$$\bigcap \mathbb{X} \subset P. \quad (26)$$

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

$$\sum F^2 = \bigcap \{Q; [\leq \text{ is an ordering of } F] \wedge [Q \text{ is a positive cone of } \leq]\} \quad (27)$$

○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 $B = \{1, \dots, \alpha^{n-1}\}$ 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 \Rightarrow 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 $x_i, y_i \in F$

$$-1 = \sum_{i=1}^n (x_i + \sqrt{a}y_i)^2. \quad (28)$$

5. Hence 1 and \sqrt{a} are linearly independent in vector space $F[\sqrt{a}]$ ^{*7}, picking the coefficients of 1,

$$-1 = \sum_{i=1}^n x_i^2 + a \left(\sum_{i=1}^n y_i^2 \right) \quad (29)$$

in F .

6. Since F is real and (Theorem 1.1.8, iii)

$$\underbrace{-1 - \sum_{i=1}^n x_i^2}_{\neq 0} = a \sum_{i=1}^n y_i^2. \quad (30)$$

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 $\sum_{i=1}^n y_i^2$,

$$-a = \frac{1 + \sum_{i=1}^n x_i^2}{\sum_{i=1}^n y_i^2} \in \sum F^2. \quad (31)$$

8. (End of 1): For all $a \in F$,
 * if a is a square $\rightarrow a \in \sum F^2$,
 * (by 1-7) if a is not a square $\rightarrow a \in -\sum F^2$.

Hence

$$a \in \sum F^2 \cup -\sum F^2. \quad (32)$$

- 9.

$$F = \sum F^2 \cup -\sum F^2. \quad (33)$$

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

$$F \stackrel{\boxed{9}}{=} \sum F^2 \cup -\sum F^2 \subset P \cup -P = F. \quad (34)$$

So $\sum F^2 \cup -\sum F^2 = P \cup -P$. Asserting $\sum F^2 \cap -\sum F^2 = \emptyset$ and $P \cap -P = \emptyset$, $\sum F^2 = P$. 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. \circ 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

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

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

$$d + \deg(g) = \deg(f) + \deg(g) \quad (36)$$

$$= \deg(fg) \quad (37)$$

$$= \deg(-1 - \sum_{i=1}^n h_i^2) \quad (38)$$

$$\leq \max_i \deg(h_i^2) \quad (39)$$

$$= 2 \max_i \deg(h_i) \quad (40)$$

$$\leq 2(d-1) \quad (41)$$

$$= 2d-2. \quad (42)$$

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).

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

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 \Rightarrow 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 $F[X]$

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

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

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

$$\deg g_h = {}_d C_2 = \frac{d(d-1)}{2} = \frac{2^m n \cdot (2^m n - 1)}{2} = 2^{m-1} \underbrace{(2^m n - 1)}_{\text{odd}} n. \quad (45)$$

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

$$\forall h \in \mathbb{Z}: \exists 1 \leq \lambda_h < \mu_h \leq d: y_{\lambda_h} + y_{\mu_h} + h y_{\lambda_h} y_{\mu_h} \in F[i]. \quad (46)$$

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) .

$$y_\lambda + y_\mu + h y_\lambda y_\mu, \quad y_\lambda + y_\mu + h' y_\lambda y_\mu \in F[i]. \quad (47)$$

- 13.

$$y_\lambda + y_\mu \in F[i], \quad y_\lambda y_\mu \in F[i]. \quad (48)$$

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

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

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

- iii. $q^2 = a + bi$ holds. \bigcirc

$$q^2 = \frac{4}{(L+a)^2 + b^2} \cdot \frac{(L+a+bi)^2}{4} \cdot L \quad (50)$$

$$= \frac{(L+a)^2 - b^2 + 2(L+a)bi}{L^2 + 2aL + a^2 + b^2} L \quad (51)$$

$$= \frac{L^2 + 2aL + a^2 - b^2 + 2(L+a)bi}{2L^2 + 2aL} L \quad (52)$$

$$= \frac{2a^2 + 2aL + 2(L+a)bi}{2L + 2a} \quad (53)$$

$$= a + bi. \quad (54)$$

^{*9} By assumption ii, we can determine 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. $y_\lambda, y_\mu \in \bar{F}$ 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. $f\bar{f} \in F[X]$ holds. ○ Write f as $\sum_j (a_j + ib_j)x^j$.

$$f\bar{f} = \left[\sum_j (a_j + ib_j)x^j \right] \cdot \left[\sum_k (a_k + ib_k)x^k \right] \quad (55)$$

$$= \left[\sum_j (a_j + ib_j)(a_j - ib_j)x^{2j} \right] + \left[\sum_{j>k} (a_j + ib_j)(a_k - ib_k)x^{j+k} \right] + \left[\sum_{j<k} (a_j - ib_j)(a_k + ib_k)x^{j+k} \right] \quad (56)$$

$$= \sum_j (a_j^2 + b_j^2)x^{2j} + 2 \sum_{j>k} (a_j a_k + b_j b_k)x^{j+k} \quad (57)$$

$$\in F[X]. \quad (58)$$

19. By (1-16), $f\bar{f}$ has a root x in $F[i]$. So x is a root of f or a root of \bar{f} ^{*10}. If x is a root of f , we complete the proof. If x is a root of \bar{f} , \bar{x} is a root of f (Take an allover conjugate).
- (iii \Rightarrow 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 $c^2 + d^2$. ○

$$x^2 = (c^2 + d^2)^2 \quad (59)$$

$$= c^4 + 2c^2 d^2 + d^4 \quad (60)$$

$$= (c^2 - d^2)^2 + 4c^2 d^2 \quad (61)$$

$$\stackrel{\text{ii}}{=} a^2 + b^2. \quad (62)$$

- (d) By (b) and (c), $-1 \notin \sum F^2$.
- (e) 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 \Rightarrow 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。

^{*10} Assume x is not a root of neither. $f(x) \neq 0$ and $\bar{f}(x) \neq 0$. So $f(x)\bar{f}(x) \neq 0$. But this is a contradiction.

^{*11} "Since $F[i]$ is a field." is nonsense to me.

* 「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, \dots, 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, \dots, 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}_{alg}):

* (Field): Let $a, b \in \mathbb{R}_{\text{alg}}$. $\mathbb{Q} \subset \mathbb{Q}[a, b] \subset \mathbb{R}_{\text{alg}}$ and $\mathbb{Q}[a, b]$ is an algebraic extension of \mathbb{Q} . So $a + b \in \mathbb{Q}[a, b] \subset \mathbb{R}_{\text{alg}}$ and $ab \in \mathbb{Q}[a, b]$. If $a \neq 0$ then $a^{-1} \in \mathbb{Q}[a] \subset \mathbb{R}_{\text{alg}}$.

* (point): \mathbb{R}_{alg} -coefficient polynomial's roots are in \mathbb{R}_{alg} . $\bigcirc x$ is a root of $a_n x^n + \dots + a_0 = 0$ ($a_i \in \mathbb{R}_{\text{alg}}$).

$$a_0, \dots, a_n \in \mathbb{Q}[a_0, \dots, a_n]. \quad (63)$$

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

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

So $\mathbb{Q}(a_0, \dots, a_n, x)$ is an algebraic extension of \mathbb{Q} (think of $1, x, x^2, \dots$. We have a linearly dependent.). So x is algebraic over \mathbb{Q} , then $x \in \mathbb{R}_{\text{alg}}$.

* (unique ordering): We will prove $\sum (\mathbb{R}_{\text{alg}})^2 = \mathbb{R}_{\text{alg} \geq 0}$. If $a \in \mathbb{R}_{\text{alg}}$ and $a \geq 0$ then $\sqrt{a} \in \mathbb{R}$. Because a is a root of \mathbb{R}_{alg} -coefficient $X^2 - a$. So $\sqrt{a} \in \mathbb{Q}[\sqrt{a}] \subset \mathbb{R}_{\text{alg}}$. We have $\sum (\mathbb{R}_{\text{alg}})^2 \cup -\sum (\mathbb{R}_{\text{alg}})^2 = \mathbb{R}_{\text{alg} \geq 0} \cup \mathbb{R}_{\text{alg} \leq 0} = \mathbb{R}_{\text{alg}}$. So induced ordering by \mathbb{R} is the unique ordering of \mathbb{R}_{alg} .

* (odd polynomial): $f = a_n x^n + \dots + a_0$ is odd degree ($a_i \in \mathbb{R}_{\text{alg}}$). f have a root in \mathbb{R} . By (point), the root in \mathbb{R}_{alg} .

* (real closed): Use (ii).

– (Puiseux series with real coefficients): $\mathbb{R}(X)^\wedge$ is a set of formal series:

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

$\mathbb{C}(X)^\wedge$ is similar. $\mathbb{R}(X)^\wedge$ is real closed. \bigcirc It is known that $\mathbb{C}(X)^\wedge$ is algebraically closed. $\mathbb{C}(X)^\wedge = \mathbb{R}(X)^\wedge[i]$ because

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

- A positive element of $\mathbb{R}(X)^\wedge$ 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 $\mathbb{R}(X)^\wedge$.

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

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

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

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

$$f = (X - a)^m (X - b)^n g \quad (70)$$

where g never vanishes in $]a, b[$.

3. Differentiate f (algebraic derivative)

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

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

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 $f(b) - f(a) = (b - a)f'(c)$. \circ

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

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

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 $[a, b]$.

\circ Obvious from (Corollary 1.2.6).

- (Definition 1.2.8):
 - R : real closed field
 - $f, g \in R[X]$

The strum sequence of f and g is the sequence of polynomials (f_0, \dots, f_k) define as follows

- $f_0 = f$
- $f_1 = f'g$
- $f_2 = f_1q_2 - f_0$ with $q_2 \in R[X]$ and $\deg(f_2) < \deg(f_1)$.
- $f_i = f_{i-1}q_i - f_{i-2}$ with $q_i \in R[X]$ and $\deg(f_i) < \deg(f_{i-1})$
- f_k is a GCD of f and $f'g$. ^{*12}

\circ The Strum sequence is determined by f and g because for $i \geq 2$, f_i is determined by division algorithm.

The stop of the sequence is Euclid algorithm. ($\text{GCD}(f_0, f_1) = \text{GCD}(f_1, f_2) = \dots$)

- (Definition, sign change): Define for an sequence (a_0, \dots, a_k) where $a_0 \neq 0$. count one sign change $a_i a_l < 0$
 - with $l = i + 1$
 - $l < i + 1$ and $a_j = 0$ for every $j(i < j < l)$.

i.e. the number of successive subsequence such that $ab < 0$ and

- (a, b)
- $(a, 0, b)$
- $(a, 0, 0, b)$
- \vdots

I write the sign change of a sequence (a_0, \dots, a_k) as $\text{SC}(a_0, \dots, a_k)$ on my own.

- (Definition, $v(f, g; a)$):
 - $f, g \in R[X]$
 - $a \in R$: a is not a root of f (To satisfy the hypothesis of the definition of sign change.)
 - (f_0, \dots, f_k) : the Strum sequence of f and g
- (Theorem 1.2.9, Sylvester's Theorem):
 - R : real closed field
 - $f, g \in R[X]$
 - $a, b \in R$: $a < b$, neither a nor b are roots of f

^{*12} GCD has an ambiguity of unit.

then

$$\# \{x \in]a, b[; f(x) = 0 \wedge g(x) > 0\} - \# \{x \in]a, b[; f(x) = 0 \wedge g(x) < 0\} = v(f, g; a) - v(f, g; b). \quad (74)$$

(We don't care of multiplicity.)

- 1. Define (g_\bullet) as

$$(g_0, \dots, g_k) := (f_0/f_k, \dots, f_k/f_k). \quad (75)$$

- 2. Let x is not a root of f . Because $f_k|f$, x is not a root of f_k . So division by $f_k(x)$ is reasonable and a sequence $(g_0(x), \dots, g_k(x))$ makes sense.

- 3. The signs of $(f_0(x), \dots, f_k(x))$ and $(g_0(x), \dots, g_k(x))$ coincide for each $x \in R$.

(Book: This implies for all $x \in R \setminus \{\text{roots of } f\}$)*¹³

$$\text{SC}(f_0(x), f_1(x)) = \text{SC}(g_0(x), g_1(x)), \quad \text{SC}(f_{i-1}(x), f_i(x), f_{i+1}(x)) = \text{SC}(g_{i-1}(x), g_i(x), g_{i+1}(x)). \quad (76)$$

)

- 4.

$$\{\text{roots of } g_0\} = \{\text{roots of } f\} \setminus \{\text{roots of } g\} \quad (77)$$

?

(a) Calculate g_0 .

(b) Assume

$$f = (x - a_1)^{A_1} \dots (x - a_l)^{A_l} (x - b_1)^{B_1} \dots (x - b_m)^{B_m} F(x) \quad (78)$$

$$g = (x - b_1)^{C_1} \dots (x - b_m)^{C_m} (x - c_1)^{D_1} \dots (x - c_n)^{D_n} G(x) \quad (79)$$

where $a_\bullet, b_\bullet, c_\bullet$ are different and F, G don't have root in R . $A_\bullet, B_\bullet, C_\bullet, D_\bullet \geq 1$. (b_\bullet are the common roots of f and g , a_\bullet are the roots only of f , c_\bullet are the roots only of g .)

(c) There exists $F_1(x) \in R[x]$ such that

$$f' = (x - a_1)^{A_1-1} \dots (x - a_l)^{A_l-1} (x - b_1)^{B_1-1} (x - b_m)^{B_m-1} F_1(x). \quad (80)$$

where F_1 doesn't disappear at a_\bullet, b_\bullet (Calculate!).

(d)

$$f'g = (x - a_1)^{A_1-1} \dots (x - a_l)^{A_l-1} (x - b_1)^{B_1+C_1-1} (x - b_m)^{B_m+C_m-1} F_1(x)G(x). \quad (81)$$

(e)

$$\text{GCD}(f, f'g) = (x - a_1)^{A_1-1} \dots (x - a_l)^{A_l-1} (x - b_1)^{B_1} \dots (x - b_m)^{B_m} \quad (82)$$

$$\times \underbrace{\text{GCD} \left(\underbrace{(x - a_1) \dots (x - a_l) F_1(x)}_{H_1(x) :=}, \underbrace{(x - b_1)^{C_1-1} \dots (x - b_m)^{C_m-1} F_1(x) G(x)}_{H_2(x) :=} \right)}_{H(x) :=}. \quad (83)$$

(by (b), $C_\bullet - 1 \geq 0$)

(f) By the definition of GCD ($H|H_1$ and $H|H_2$), the roots of H is a root of H_1 and H_2 .

(g) If ξ is not a root of H_1 or not a root of H_2 then ξ is not a root of H .

(h) By (c), b_\bullet are not roots of H_1 .

*¹³ the exclusion of roots is needed for the definition of $\text{SC}(f_0(x), f_1(x)) = \text{SC}(f(x), f'g(x))$.

- (i) By (b) and (c), a_\bullet are not roots of H_2 .
(j) (g,h,i) implies a_\bullet, b_\bullet are not roots of H .
(k) By (e, j),

$$\frac{f}{\text{GCD}(f, f'g)} = (x - a_1) \dots (x - a_l) \underbrace{\frac{F(x)}{H(x)}}_{\in R[x]}. \quad (84)$$

because $f/\text{GCD}(f, f'g) \in R[x]$. By (b), $\frac{F}{H}$ have no root at a_\bullet .

- (l) By definition of g_0 , $g_0 = \pm f/\text{GCD}(f, f'g)$. a_\bullet were the roots of f which are not roots of g .
5. $i \in \{0, \dots, k\}$, $g_{i-1} \perp g_i$ \circ Because $f_k = \pm \text{GCD}(f, f'g)$, $\text{GCD}(g_0, g_1) = 1$. Next $f_i = f_{i-1}q_i - f_{i-2}$, so $(f_{i-1}, f_{i-2}) = (f_{i-1}, f_{i-1}q_i - f_i) = (f_{i-1}, f_i) = (1)$.
6. Let c be a polynomial g_i .

(a) When $g_i = g_0$. c is a root of g_0 . (Pay attention to Proposition 1.2.4 intermediate-value theorem from here!)

- i. By (5), c is not a root of g_1 . (the sign change happens immediately!)
- ii. By (4), $f(c) = 0$ and $g(c) \neq 0$.
- iii. We define the sign of $f'(c_-)$ as the sign of f' immediately to the left of c . We can take "immediate left" because the roots of f' are finite and intermediate-value theorem. We define $f'(c_+)$ similarly.
- iv. $f'(c_-) \neq 0$ and $f'(c_+) \neq 0$. \circ Assume $f'(c_-) = 0$. We have infinitely many "immediate left" points, so f' vanishes at infinitely many points. Polynomial $f' \equiv 0$. $f(c) = 0$ (ii) and $f' \equiv 0$ imply $f \equiv 0$. This contradicts to "neither a nor b are roots of f ".
- v. By (ii,iv), we have eight cases:

$$(g(c), f'(c_-), f'(c_+)) = (+++), (++-), (+-+), (+--), (-++), (-+-), (-+-), (---). \quad (85)$$

vi. In every case as x passes through c^{*14} , the number of sign changes in $(f_0(x), f_1(x))$

– $g(c) > 0 \implies$ decreases by 1

– $g(c) < 0 \implies$ increases by 1

(We don't have to think of the case of $g(c) = 0$ because ii)

- (b) i. When $i = 1, \dots, k$.
ii. $g_i(c) = 0$
iii. By (5), $g_{i-1} \perp g_i$ and $g_i \perp g_{i+1}$. This means $g_{i-1}(c) \neq 0$ and $g_{i+1}(c) \neq 0$.
iv. $g_{i-1}(c)g_{i+1}(c) < 0$. \circ By definition of a sequence, $g_{i+1} = g_iq_{i+1} - g_{i-1}$

$$g_{i+1}(c) = g_i(c)q_{i+1}(c) - g_{i-1}(c) \stackrel{\text{ii}}{=} -g_{i-1}(c). \quad (86)$$

v. The signs of $(f_{i-1}(x), f_i(x), f_{i+1}(x))$ is $(++-), (-++), (+--), (-+-)$.

vi. The number of sign changes in $(f_{i-1}(x), f_i(x), f_{i+1}(x))$ does not change passing c .

7. By intermediate-value theorem and (6), the sign changes in intervals made by roots of g_\bullet . We can chase the sign changes only by watching roots of g_\bullet , and the way the change happens is (a) or (b) (may happen simultaneously).
8.

$$\# \{x \in]a, b[; f(x) = 0 \wedge g(x) > 0\} - \# \{x \in]a, b[; f(x) = 0 \wedge g(x) < 0\} = v(f, g; a) - v(f, g; b). \quad (87)$$

^{*14} Immediate left c_- and right c_+

- (Example of sign change):

$$(+-+--+ +, 6) \rightarrow (- - + - + - +, 5) \quad (88)$$

$$\rightarrow (- + + - + - +, 5) \quad (89)$$

$$\rightarrow (+ + + - + - +, 4). \quad (90)$$

- (TODO): Why "real closed"?
- (Corollary 1.2.10, Strum's Theorem):
 - R : real closed field
 - $f \in R[X]$
 - $a, b \in R$: $a < b$, $f(a) \neq 0$, $f(b) \neq 0$

then

$$\#\{\text{roots of } f\} = v(f, 1; a) - v(f, 1; b). \quad (91)$$

○Apply 1.2.9 with $g = 1$.

- (Lemma 1.2.11):
 - R : real closed field
 - $f = a_n X^n + \dots + a_0 \in R[X]$, $a_n \neq 0$
 - $M = 1 + |a_{n-1}/a_n| + \dots + |a_0/a_n|$

then

- f never vanishes on $[M, +\infty[$ and its sign is the sign of a_n .
- f never vanishes on $] -\infty, -M]$ and its sign is the sign of $(-1)^n a_n$.

- ○We prove the first one.

1. Let $x \in R$, $|x| \geq M$. (Aim: $f(x) \neq 0$ and $\text{sign} f(x) = \text{sign} a_n$)
2. Triangle ineq. holds.

$$\left| \frac{a_{n-1}}{a_n} x^{-1} + \dots + \frac{a_0}{a_n} x^{-n} \right| \stackrel{\boxed{M > 1}}{\leq} (|b_{n-1}| + \dots + |b_0|) M^{-1} < 1. \quad (92)$$

3.

$$-1 < \frac{a_{n-1}}{a_n} x^{-1} + \dots + \frac{a_0}{a_n} x^{-n} < 1. \quad (93)$$

4.

$$0 < 1 + \frac{a_{n-1}}{a_n} x^{-1} + \dots + \frac{a_0}{a_n} x^{-n}. \quad (94)$$

5.

$$f(x) = a_n x^n \underbrace{\left(1 + \frac{a_{n-1}}{a_n} x^{-1} + \dots + \frac{a_0}{a_n} x^{-n} \right)}_{>0}. \quad (95)$$

- (Corollary 1.2.12):
 - R : real closed field
 - $f, g \in R[X]$
 - (f_0, \dots, f_k) : the Strum sequence of f and g
 - $v(f, g; +\infty) = \text{SC}(\text{LC} f_0, \dots, \text{LC} f_k)$
 - $v(f, g; -\infty) = \text{SC}(\text{LC} f_0(-X), \dots, \text{LC} f_k(-X))$

then

$$\#\{x \in R; f(x) = 0 \wedge g(x) > 0\} - \#\{x \in R; f(x) = 0 \wedge g(x) < 0\} = v(f, g; -\infty) - v(f, g; +\infty). \quad (96)$$

• ○

1. Let M is larger than all the roots of f_0, \dots, f_k are in $] -M, M[$. (This is possible because the roots are finite.)
2. By 1.2.11 (the latter),

$$v(f, g, +\infty) = \text{SC}(\text{LC}f_0, \dots, \text{LC}f_k) \stackrel{1.2.11}{=} \text{SC}(f_0(M), \dots, f_k(M)) = v(f, g, M), \quad (97)$$

$$v(f, g, -\infty) = \text{SC}(\text{LC}f_0(-X), \dots, \text{LC}f_k(-X)) = \text{SC}((-1)^{\deg f_0} \text{LC}f_0, \dots, (-1)^{\deg f_k} \text{LC}f_k) \stackrel{1.2.11}{=} v(f, g, -M). \quad (98)$$

3. By 1.2.9,

$$\begin{aligned} \# \{x \in R; f(x) = 0 \wedge g(x) > 0\} - \# \{x \in R; f(x) = 0 \wedge g(x) < 0\} &= \# \{x \in] -M, M[; f(x) = 0 \wedge g(x) > 0\} - \# \{x \in] -M, M[; f(x) = 0 \wedge g(x) < 0\} \\ &= v(f, g; -M) - v(f, g; M) \quad (99) \\ &= v(f, g; -\infty) - v(f, g; +\infty). \quad (100) \\ &= v(f, g; -\infty) - v(f, g; +\infty). \quad (101) \end{aligned}$$

• (Remark 1.2.13):

– $f \in R[X]$: monic, square free, degree n ^{*15}

then f has n roots \iff the Sturm sequence of f and 1 have $n+1$ length $((\underbrace{f_0}_{=f}, \underbrace{f_1}_{=1 \cdot f' = f'}, \dots, f_n))$ and

leading coefficients of f_0, \dots, f_n are positive.

- $\circ \Rightarrow$: By 1.2.12, $v(f, 1; -\infty) - v(f, 1; +\infty) = n$. Because $\deg f = n$, the length of the Sturm sequence is $\leq n+1$. So $0 \leq v(f, 1; -\infty) \leq n$ and $0 \leq v(f, 1; +\infty) \leq n$. $v(f, 1; -\infty)$ must be n and $v(f, 1; +\infty)$ must be 0. The signs of $(f_0(+\infty), \dots, f_n(+\infty))$ ^{*16} are $(++ \dots +)$ because f is monic.

\Leftarrow : By the definition of Sturm sequences, $\deg f_i = n-i$. The signs of $(f_0(+\infty), \dots, f_n(+\infty)) = (++ \dots +)$. These two imply $(f_0(-\infty), \dots, f_n(-\infty)) = (\dots \pm \mp)$.

• (Proposition 1.2.14, Descartes's Lemma):

– R : real closed field

– $f = a_n X^n + \dots + a_k X^k \in R[X]$ with $a_n a_k \neq 0$

then

$$\# \{x \in]0, +\infty[; f(x) = 0\} \leq \text{SC}(a_n, \dots, a_k). \quad (102)$$

• ○

1. Think of $n = 1$.

(a) f has the form of $f = a_1 X + a_0$ or $f = a_1 X$.

(b) If $f = a_1 + a_0$,

- $a_1 > 0$ and $a_0 < 0$: f has one positive root. SC is 1.
- $a_1 > 0$ and $a_0 > 0$: f has no positive roots. SC is 0.
- $a_1 < 0$ and $a_0 < 0$: f has no positive roots. SC is 0.
- $a_1 < 0$ and $a_0 > 0$: f has one positive root. SC is 1.

OK.

(c) If $f = a_1 X$, f has no positive roots (it is zero!) and SC is 0. OK.

2. So if $n = 1$, OK.

3. We prove the statement by induction. The base case is already proved in (1-2). We assume the case of $n - 1$.

^{*15} $f \perp f'$, or have no multiple roots

^{*16} leading coefficients

4. We can assume X does not divide f , i.e. $a_0 \neq 0$, because we can divide X as many as possible. The division doesn't change the SC nor positive roots. So $f = a_n X^n + \dots + a_q X^q + a_0$ where $a_n \neq 0, a_q \neq 0, a_0 \neq 0$.
5. $f' = na_n X^{n-1} + \dots + qa_q X^{q-1}$.
6. We can apply the hypothesis of induction,

$$\# \{x \in]0, +\infty[; f'(x) = 0\} \leq \text{SC}(a_n, \dots, a_q). \quad (103)$$

7. Let $c \in R$ be the smallest positive root of f' . If it does not exist, let $c = +\infty$.
8. By interval theorem,

$$\text{sign} a_q = \underbrace{\text{sign }]0, c[}_{\text{interval}} \quad (104)$$

9. $f(0) = a_0$.
10. – The case f has a root in $]0, c[$:
 - (a) Seeing the variation of f , $a_q a_0 < 0$ is necessary for the case.
 - (b)

$$\text{SC}(a_n, \dots, a_q) + 1 = \text{SC}(a_n, \dots, a_q, a_0). \quad (105)$$

- (c) By Rolle's theorem, there is exactly one root in $]0, c[$. ○ If any, the property of c in (7) is wrong.

- (d) So by interval theorem

$$\# \{\text{positive roots of } f\} - 1 \leq \# \{\text{positive roots of } f'\}. \quad (106)$$

(for a interval of f 's roots, there exist at least one root of f' ^{*17})

- (e)

$$\# \{\text{positive roots of } f\} \stackrel{\boxed{\text{d}}}{\leq} \# \{\text{positive roots of } f'\} + 1 \quad (107)$$

$$\stackrel{\boxed{\text{e}}}{\leq} \text{SC}(a_n, \dots, a_q) + 1 \quad (108)$$

$$\stackrel{\boxed{\text{b}}}{=} (\text{SC}(a_n, \dots, a_0) - 1) + 1 \quad (109)$$

$$= \text{SC}(a_n, \dots, a_0). \quad (110)$$

- Otherwise:

- (a) By assumption, there are no roots in $]0, c[$.

- (b) So (similar to 10-d)

$$\# \{\text{positive roots of } f\} \leq \# \{\text{positive roots of } f'\}. \quad (111)$$

- (c)

$$\# \{\text{positive roots of } f\} \stackrel{\boxed{\text{b}}}{\leq} \# \{\text{positive roots of } f'\} \quad (112)$$

$$\stackrel{\boxed{\text{e}}}{\leq} \text{SC}(a_n, \dots, a_q) \quad (113)$$

$$\leq \text{SC}(a_n, \dots, a_0). \quad (114)$$

11. In both cases of (10),

$$\# \{\text{positive roots of } f\} \leq \text{SC}(a_n, \dots, a_0). \quad (115)$$

^{*17} Assume f is not zero.

1.3 Real Closure of an Ordered Field

- (Definition 1.3.1):

- (F, \leq) : ordered field
- R : algebraic extension of F

R is a real closure of $F \iff$

- R is real closed
- R 's unique ordering extends the ordering of F . i.e. $F \hookrightarrow R$ preserves ordering.