Quadratic Extensions in ACL2

Ruben Gamboa [1] John Cowles [1] Woodrow Gamboa [2]

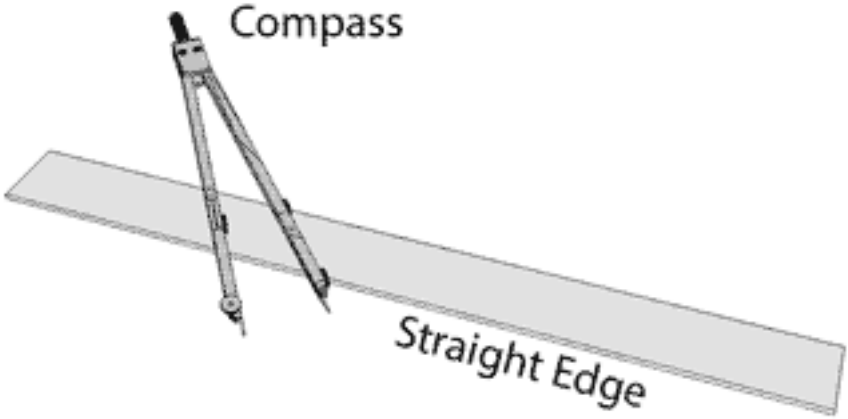
[1]Department of Computer Science
University of Wyoming
Laramie, Wyoming 82071
{ruben,cowles}@uwyo.edu

[2]Stanford University
Stanford, California 94305
woodrowg@stanford.edu

ACL2 Workshop 2020

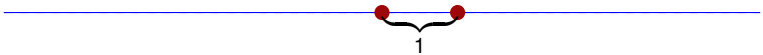
Outline

Geometric Straight Edge and Compass Constructions

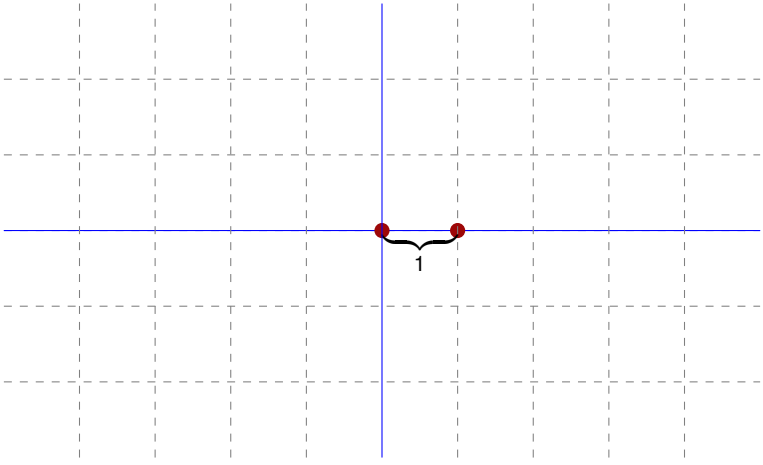


Basics of Geometric Constructions

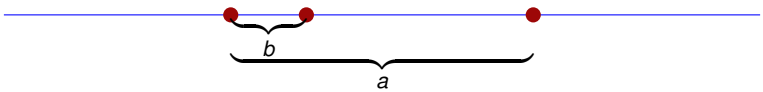
Basics of Geometric Constructions



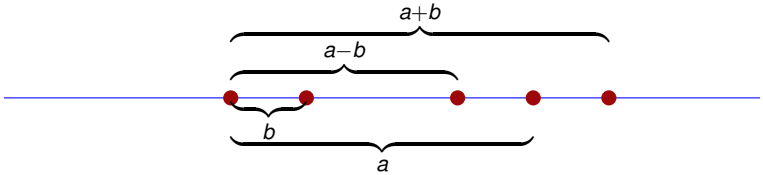
Basics of Geometric Constructions



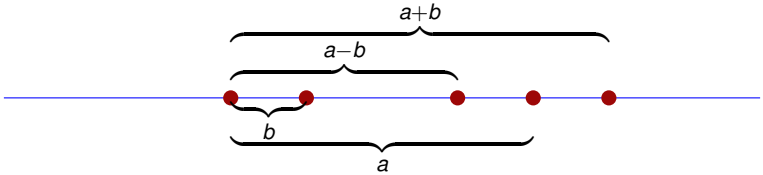
Addition and Subtraction



Addition and Subtraction

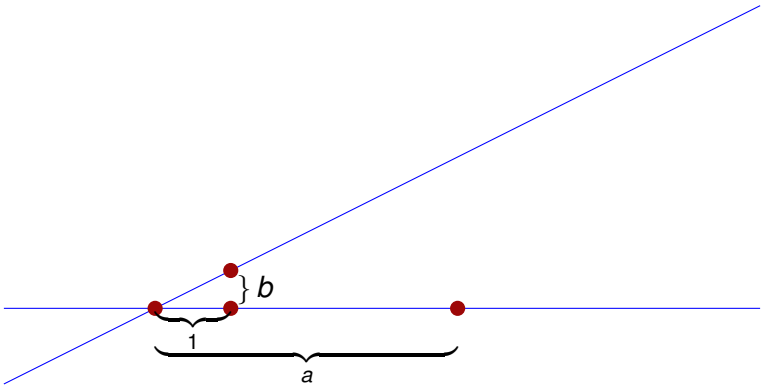


Addition and Subtraction

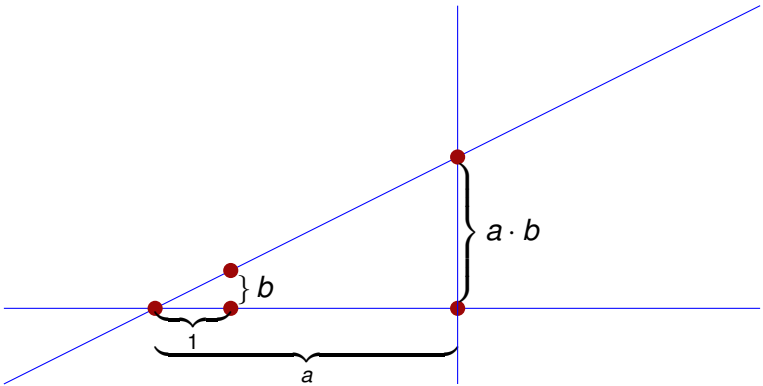


We can find all the integer points!

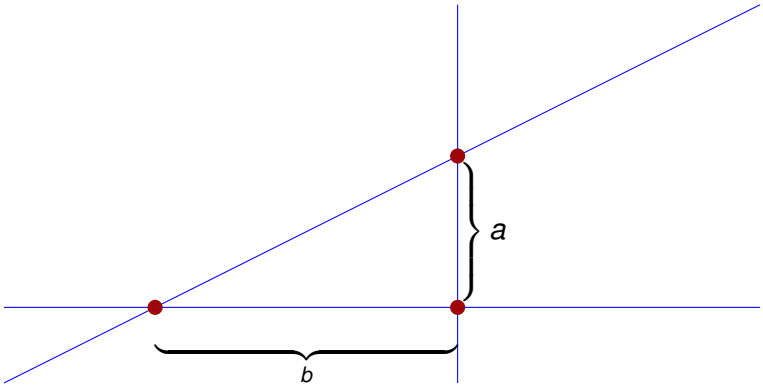
Multiplication



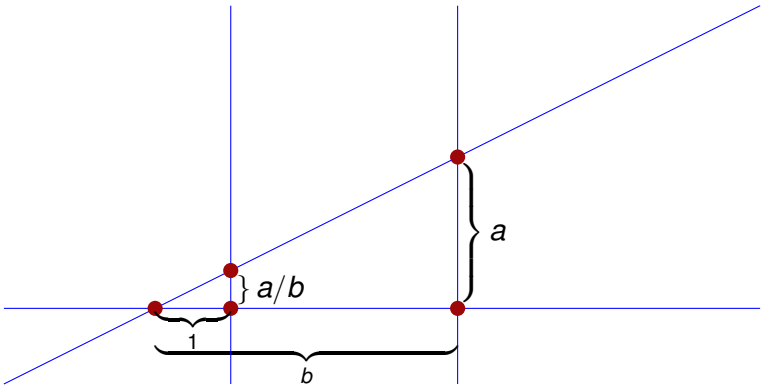
Multiplication



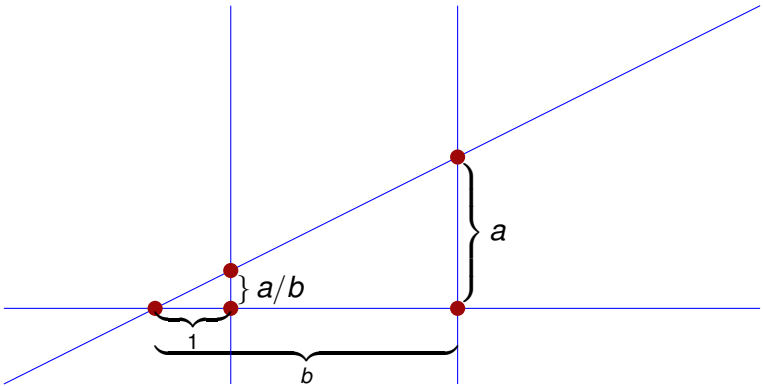
Division



Division

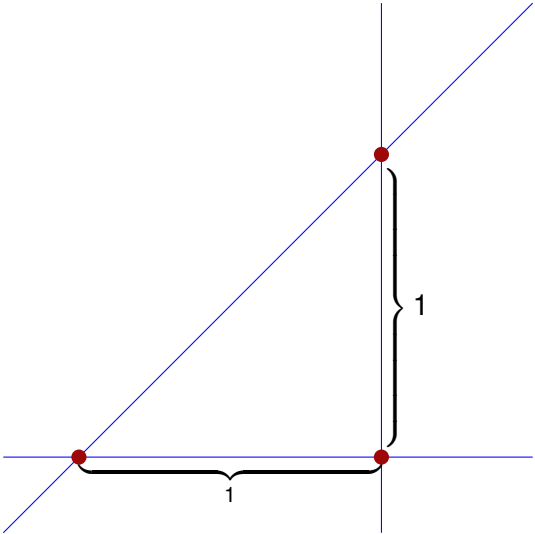


Division

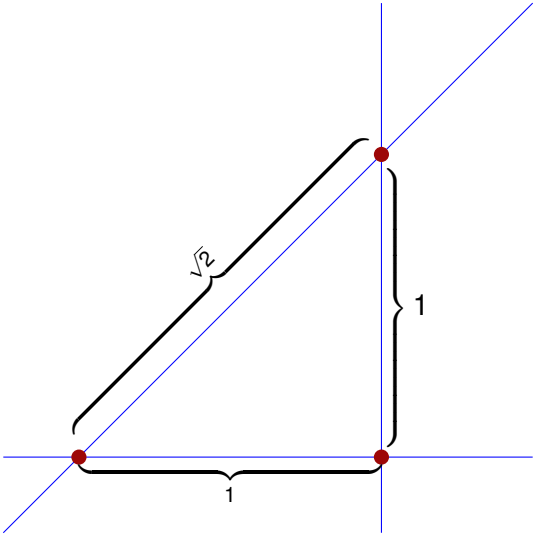


We have all the rationals!

Why We Need ACL2(r)



Why We Need ACL2(r)



From Geometry to Algebra

- Points on the plane determine lines and circles
- New points are found by intersecting
  - two lines
  - two circles
  - a line and a circle
- We care about the coordinates and/or the distance between points
- Those numbers can be added, subtracted, multiplied, divide

From Geometry to Algebra

- Points on the plane determine lines and circles
- New points are found by intersecting
  - two lines
  - two circles
  - a line and a circle
- We care about the coordinates and/or the distance between points
- Those numbers can be added, subtracted, multiplied, divide

- These **constructible** numbers form a field

From Geometry to Algebra

- Points on the plane determine lines and circles
- New points are found by intersecting
  - two lines
  - two circles
  - a line and a circle
- We care about the coordinates and/or the distance between points
- Those numbers can be added, subtracted, multiplied, divide

- These **constructible** numbers form a field

- The field of constructible numbers is larger than $\mathbb{Q}$
- Key question: Is the field of constructible numbers equal to $\mathbb{R}$?

Outline

Numeric Fields

- Fields support $+$, $-$, $\times$, and $/$ operations
- In numeric fields, these are just the common arithmetic operations

Numeric Fields

- Fields support $+$, $-$, $\times$, and $/$ operations
- In numeric fields, these are just the common arithmetic operations

- Formalized in ACL2 with an `encapsulate`
- Function `number-field-p` recognizes elements of the field
- ACL2 already knows about properties of arithmetic operators
- So the only constraints needed are
  - 0 and 1 are `number-field-p`
  - `number-field-p` is closed under the arithmetic operators

Field Extensions

- Extend a field K by adding a number α not already in K
- Resulting field is called $K(\alpha)$
- For quadratic field extensions, α is a root of a quadratic polynomial in K

Field Extensions

- Extend a field K by adding a number α not already in K
- Resulting field is called $K(\alpha)$
- For quadratic field extensions, α is a root of a quadratic polynomial in K

- All of the following are in $K(\alpha)$:
  - a, b
  - α
  - $a + b\alpha$
- In fact, all elements of $K(\alpha)$ can be written as $a + b\alpha$

Formalizing Field Extensions

- All elements of $K(\alpha)$ can be written as

$$a + b\alpha$$

- Use that to formalize field extensions:

$$(\exists a, b \in K)x = a + b\alpha$$

More Field Extensions

- Start with K and extend it with α and extend that with β

More Field Extensions

- Start with K and extend it with α and extend that with β
- Formalize that as
$$(\exists a, b \in K(\alpha))x = a + b\beta$$
- Recursive `defun-sk`??? (@MattK, does that even work?)

Formalizing Field Extensions

- Start with K and extend it with α
- All elements of $K(\alpha)$ can be written as

$$a + b\alpha$$

Formalizing Field Extensions

- Start with K and extend it with α
- All elements of $K(\alpha)$ can be written as

$$a + b\alpha$$

- Now extend it with β
- Are all elements of $K(\alpha, \beta)$ written as

$$a + b\alpha + c\beta$$

Formalizing Field Extensions

- Start with K and extend it with α
- All elements of $K(\alpha)$ can be written as

$$a + b\alpha$$

- Now extend it with β
- Are all elements of $K(\alpha, \beta)$ written as

$$a + b\alpha + c\beta$$

- Not quite, but they **can** be written as

$$a + b\alpha + c\beta + d\alpha\beta$$

Formalizing Field Extensions

- All elements of $K(\alpha, \beta)$ can be written as

$$a + b\alpha + c\beta + d\alpha\beta$$

Formalizing Field Extensions

- All elements of $K(\alpha, \beta)$ can be written as

$$a + b\alpha + c\beta + d\alpha\beta$$

- Function `(all-products '(α β))` finds all terms $1, \alpha, \beta, \alpha\beta$
- `(is-linear-combination x '(α β))` see if there exists coefficients such that x can be written as a combination of the products of α and β

Validating the Formalization

- Is `(is-linear-combination x '(`α β `...`ω`))` really a recognizer for $\mathbb{Q}(\alpha, \beta, \ldots, \omega)$?
- Trivially, all elements it recognizes are in $\mathbb{Q}(\alpha, \beta, \ldots, \omega)$
- If it recognizes a field, then it recognizes precisely $\mathbb{Q}(\alpha, \beta, \ldots, \omega)$

Validating the Formalization

- Is `(is-linear-combination x '(α β ...ω))` really a recognizer for $\mathbb{Q}(\alpha, \beta, \ldots, \omega)$?
- Trivially, all elements it recognizes are in $\mathbb{Q}(\alpha, \beta, \ldots, \omega)$
- If it recognizes a field, then it recognizes precisely $\mathbb{Q}(\alpha, \beta, \ldots, \omega)$

- Addition and subtraction, “trivial”
- Multiplication, “easy”
  - Key lemma: $\alpha^2 \in K$ when $K(\alpha)$ is a quadratic field extension of K
- Division, “tedious”
  - Key concept: $\overline{a + b\alpha} = a - b\alpha$, and then use the complex conjugate trick to define $1/z$

Outline

More on Conjugates

- Remember: $\overline{a + b\alpha} = a - b\alpha$

More on Conjugates

- Remember: $\overline{a + b\alpha} = a - b\alpha$
- Conjugates have many nice algebraic properties:
  - $\overline{x + y} = \overline{x} + \overline{y}$
  - $\overline{x - y} = \overline{x} - \overline{y}$
  - $\overline{xy} = \overline{x}\,\overline{y}$
  - $\overline{\frac{1}{x}} = \frac{1}{\overline{x}}$
  - $\overline{x^n} = \overline{x}^n$
  - $\overline{ax^n} = a\overline{x}^n$, for $a \in K$

Conjugates and Polynomial Roots

- Key property: $\overline{ax^n} = a\overline{x}^n$, for $a \in K$

Conjugates and Polynomial Roots

- Key property: $\overline{ax^n} = a\overline{x}^n$, for $a \in K$
- Payoff: $P(\overline{x}) = \overline{P(x)}$ for any polynomial P with coefficients in K

Conjugates and Polynomial Roots

- Key property: $\overline{ax^n} = a\overline{x}^n$, for $a \in K$
- Payoff: $P(\overline{x}) = \overline{P(x)}$ for any polynomial P with coefficients in K
- BIG payoff: If P is a polynomial with roots in K and $x \in K(\alpha)$ is root of P, so is $\overline{x}$
- I.e., roots come in conjugate pairs

Conjugates and Cubic Polynomials

- Roots come in conjugate pairs
- If a cubic polynomial with coefficients in K has a root $x_0 \in K(\alpha) \backslash K$, it can be factored as $(x - x_0)(x - \overline{x_0})(x - x_1)$
- And, in fact, $x_1 \in K$

Conjugates and Cubic Polynomials

- Roots come in conjugate pairs
- If a cubic polynomial with coefficients in K has a root $x_0 \in K(\alpha) \backslash K$, it can be factored as $(x - x_0)(x - \overline{x_0})(x - x_1)$
- And, in fact, $x_1 \in K$

- Cubic polynomials that have a root in $K(\alpha)$ have at least one root in K as well

Conjugates and Cubic Polynomials

- Roots come in conjugate pairs
- If a cubic polynomial with coefficients in K has a root $x_0 \in K(\alpha) \backslash K$, it can be factored as $(x - x_0)(x - \overline{x_0})(x - x_1)$
- And, in fact, $x_1 \in K$

- Cubic polynomials that have a root in $K(\alpha)$ have at least one root in K as well

- BIG Payoff: Cubic polynomials with rational coefficients, and with any root in $\mathbb{Q}(\alpha, \beta, \ldots, \omega)$ must also have a rational root

Rational Root Theorem

- Suppose $P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ with $a_i \in \mathbb{Z}$
- Then if p/q is a rational root of $P(x)$
  - q divides a_3
  - p divides a_0

A Special Case: $P(x) = x^3 - 2$

```
(defconst *poly-double-cube*   '(-2  0 0 1))
(defthmd possible-rational-roots-of-double-cube
  (implies (and (rationalp x)
                (equal (eval-polynomial *poly-double-cube* x) 0))
           (or (equal x 2)
               (equal x 1)
               (equal x -1)
               (equal x -2)))
  :hints ...)
```

A Little Payoff: $P(x) = x^3 - 2$

```
(defthm no-rational-roots-of-double-cube
  (implies (rationalp x)
           (not (equal (eval-polynomial *poly-double-cube* x) 0)))
  :hints ...)
```

A Little Payoff: $P(x) = x^3 - 2$

```
(defthm no-rational-roots-of-double-cube
  (implies (rationalp x)
           (not (equal (eval-polynomial *poly-double-cube* x) 0)))
  :hints ...)
I

(defthmd cube-root-of-two-is-root-of-poly-double-cube
  (equal (eval-polynomial *poly-double-cube* (raise-to 2 1/3)) 0)
  :hints ...)
I
```

A Little Payoff: $P(x) = x^3 - 2$

```
(defthm no-rational-roots-of-double-cube
  (implies (rationalp x)
           (not (equal (eval-polynomial *poly-double-cube* x) 0)))
  :hints ...)
I

(defthmd cube-root-of-two-is-root-of-poly-double-cube
  (equal (eval-polynomial *poly-double-cube* (raise-to 2 1/3)) 0)
  :hints ...)
I

(defthm cube-root-of-two-is-not-in-quadratic-extension
  (implies (quadratic-extensions-p exts)
           (not (is-linear-combination-p (raise-to 2 1/3) exts)))
  :hints ...)
(defthm cube-root-of-two-is-irrational
  (and (realp (raise-to 2 1/3))
       (not (rationalp (raise-to 2 1/3))))
  :hints ...)
```

Outline

Conclusion and Future Work

- We formalized quadratic field extensions in ACL2(r)
- We showed that some numbers (e.g., $\sqrt[3]{2}$) are not in any quadratic field extension
- Hence, these numbers are irrational

Conclusion and Future Work

- We formalized quadratic field extensions in ACL2(r)
- We showed that some numbers (e.g., $\sqrt[3]{2}$) are not in any quadratic field extension
- Hence, these numbers are irrational

- All points that can be found using a straight edge and compass construction are in a quadratic field extension
- That means it is impossible to

Construction	**Polynomial**	**Root**
Double a cube	$x^3 - 2$	$\sqrt[3]{2}$
Trisect an angle	$8x^3 - 6x - 1$	$\cos \frac{\pi}{9}$
Square a circle	Because π is transcendental	