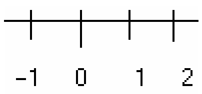
Constructible Numbers, Fields and Surds

Original Notes adopted from February 5, 2002 (Week 18)

  University of Toronto, Department of Mathematics typed by A. Ku Ong

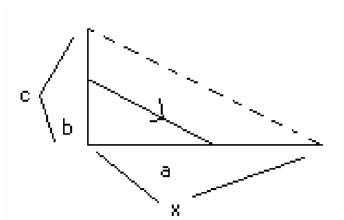
<u>Constructible Numbers</u>
If a,b,c are constructible & > 0,



if b<c

$\frac{c}{b} = \frac{x}{a}$

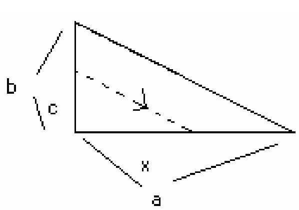
x = ac/b



if b> c

$\frac{b}{c} = \frac{a}{x}$

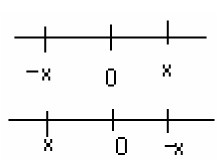
x = ac/b



So can construct ac/b for a,b,c positive constructed numbers. In particular, take b =1, shows can construct the product of any two constructible positive numbers.

Take c =1, show can construct quotient of any two constructible positive numbers.
Let C = set of all constructible numbers.

If x ∈ C, -x ∈ C.



$0,1 \in C$
If $a,b, \in C$, so is $a + b$.

Definition: A subset F of R is a number field if
1) $0,1 \in F$
2) If $x,y \in F$, so are $x + y$ & $x * y$.
3) If $x \in F$, so is $-x$.
4) If $x \in F$ & $x \neq 0$, then $1/x \in F$.

Above we showed: C is a number field.
$C \supset Q$

Eg. R,Q are number fields
$Q(\sqrt{2})$ is defined to be $\{a + b\sqrt{2} : a,b \in Q\}$

Obviously Properties 1,3,4 hold
Property 2:
$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (bc + ad)\sqrt{2} \in Q(\sqrt{2})$
Property 4:

$$\frac{1}{a + b\sqrt{2}} * \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

If $a^2 - 2b^2 = 0$
$a^2 - 2b^2 \; (a/b)^2 = 2 \Rightarrow \sqrt{2}$ rational, contradiction.
$\therefore$ If a,b not both 0, $1/a+b\sqrt{2} \in Q(\sqrt{2})$

More generally, if F any number field & $r \in F$, $r > 0$, but $\sqrt{r}$ F.
We define $F(\sqrt{r})$ (the field of F extended by square root of r
$= \{a + b\sqrt{r} : a,b \in F\}$

Lemma: If F, r as above, then $F(\sqrt{r})$ is a number field.
Proof: $0,1, \in F$.
closed under +, *, -

$$\frac{1}{a + b\sqrt{r}} * \frac{a - b\sqrt{r}}{a - b\sqrt{r}} = \frac{a - b\sqrt{r}}{a^2 - rb^2} = \frac{a}{a^2 - rb^2} - \frac{b}{a^2 - rb^2}\sqrt{r} \quad \text{if } a^2 - rb^2 \neq 0$$

But if $a^2 - rb^2 = 0$
$(a/b)^2 = r \Rightarrow r \in F$, contradiction

Eg. $F = Q(\sqrt{2})$, $r = \sqrt{3}$.

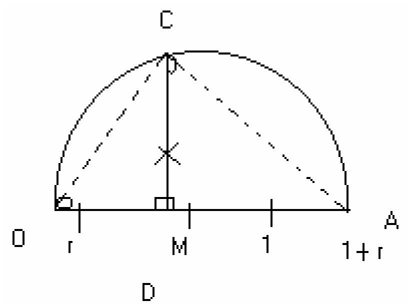
$F(\sqrt{3}) = (Q(\sqrt{2}))(\sqrt{3})$
$= \{a + b\sqrt{3} : a,b \in Q(\sqrt{2})\}$
$= \{a_1 + a_2\sqrt{2} + (b_1 + b_2\sqrt{2})\sqrt{3} : a_1, a_2, b_1, b_2 \in Q\}$

Definition: A tower of number fields is a finite collection of number fields which each obtained from the previous one by adjoining a square root:
F_0 a number field
$F_1 = F_0(\sqrt{r_0})$ with $r_0 \in F$, $r_0 > 0$. $\sqrt{r_0} \notin F_0$
$F_2 = F_1(\sqrt{r_1})$ with $r_1 \in F$, $r_1 > 0$. $\sqrt{r_1} \in F_1$

$F_0 \subset F_1 \subset F_2 \subset$ .... $\subset F_k$

Theorem: If r ∈ C & r > 0, then √r ∈ C

Proof:



bisect r +1. constructing M = $\frac{r+1}{2}$

Make circle center M and radius M
Erect a perpendicular at r. Make Triangles.
$\angle OCA = 90^0$
$\angle COD + \angle OCD = 90^0$
$\angle DCA + \angle OCD = 90^0$
$\therefore \angle COD = \angle DCA$

∴ Triangle OCD is similar (~) to Triangle ACD
$\therefore x/1 = r / x, \quad x^2 = r$
$\therefore x = \sqrt{r}$, and $x \in C$, so $\sqrt{r} \in C$.

Corollary : If $Q \subset F_1 \subset F_2 \subset F_3 \ldots \subset F_k$ is any tower
(i.e. $F_j = F_{j-1}(\sqrt{r}_{j-1})$ with $r_{j-1} \in F_{j-1}$ $r_{j-1} > 0$, $\sqrt{r}_{j-1} \notin F_{j-1}$), then
$F_k \subset C$

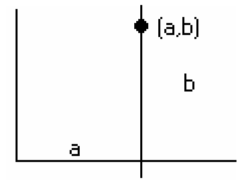
Definition: A surd is a number that is in some F_k that is in a tower starting at Q.
Corollary: The collection of surds is contained in C (or, every surd is constructible)

Let S = set of al surds
C = set of all constructible numbers.

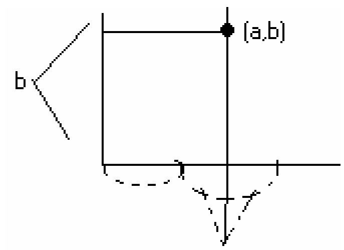
Proved: $S \subset C$.
Want: S = C.

To construct numbers: We start with 0,1, get Q
Note: Can construct point (a,b) in plane if and only if can construct numbers a &b.

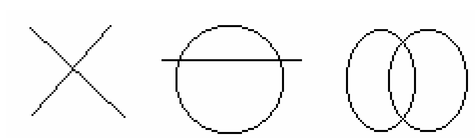
If we con construct a,b. We can construct the point (a,b).



Given the point (a,b) , we have a,b.



<u>Must show: $C \subset S$</u>



<u>Constructions consist of:</u>

1) joining line between 2 constructed points
2) making circle, center at constructed point, radius a constructed number.
3) taking points of intersection of the above.

To prove $C \subset S$, we'll show: if you start with points whose coordinates are in S, then any construction produces points whose coordinates are in S.

Suppose (a,b) & (c,d) are constructed & $a,b,c,d \in S$.
Note: There exists an extension (i.e. end of a tower) F of Q a,b,c & d.
$a,b,c,d, \in F$. Equation of line joining: (x,y)

$$\frac{y-b}{x-a} = \frac{d-b}{c-a}$$

All coefficients are in F. Equation of form $sx + ty = u$, with $s,t,u \in F$.
This proves: a line joining points whose coordinates are in a number field F has an equation with coefficients in F.
Note: If 2 lines have equations with coefficients in F, then the coordinates of points of intersection one in F. (solve simultaneously)
This proves: If a point is constructed as the intersection of 2 lines, both of which are determined by points with coefficients in S, then that point has coefficients in S.

Given a circle with center (a,b) and radius r, & if $a,b, r \in F$ (F number field) an equation of circle: $(x-a)^2 + (y-b)^2 = r^2$... coefficients in F.

<u>Lemma:</u> Points constructed by intersecting a line determined by surd points & a circle with surd radius and surd center has surd coordinates.

Proof: Circle has equation
$x^2 + b x + y^2 + cy + d = 0$. $b,c,d \in S$
Line has equation $ex + fy + g = 0$. $e,f,g \in S$.
Simultaneous solution keeps within surd field:
$y = sx + t$... $s,t \in S$
$x^2 + bx + (sx + t)^2 + c(sx + t) + d = 0$.
Get quadratic in x, use quadratic formula $\Rightarrow$ within $F(\sqrt{r})$ if coefficients in F & $r = b^2 - 4ac$. Stay in surds.

<u>2 circles intersecting</u>
$x^2 + ax + y^2 + by + c = 0$
$x^2 + dx + y^2 + ey + f = 0$
$(a-d)x + (b-e)y + c-f = 0$ $\Rightarrow$ Simultaneously solve both .

S = C

(subtraction --- share intersection)