Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

October 26, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 The Degree of a Field Extension

Degree of Field Extension

Definition 0.1.0.1. Let K be a field extension of a field F. We can always regard K as a vector space over F where addition is field addition and multiplication by F is simply multiplication.

We say that the degree of K as an extension of F is the dimension of the vector space (denoted $[K : F]$).

Extensions of degree 2 are called quadratic, of degree are called cubic, ect.

The term degree comes from the case when $K = F(\alpha)$

for an algebraic α over F and so $(1, \alpha, \ldots, \alpha^{n-1})$ form a basis for the vector space (where n is the degree of the irreducible polynomial).

In this case we also call the degree the degree of α over F

Degree of Field Extension vs. Dimension of V

Theorem 0.1.0.2. *If α is algebraic over F then $[F(\alpha) : F]$ is the degree of the irreducible polynomial of α.*

Proof. Immediate. □

Adjoining a Square Root

Theorem 0.1.0.3. *Suppose F does not have characteristic 2. Then any extension $F \subset K$ of degree 2 can be obtained by adjoining a square root: $K = F(\delta)$, where $\delta^2 = D \in F$. Conversely if δ is an element of*

an extension of F and if $\delta^2 \in F$, but $\delta \notin F$ then $F(\delta)$ is a quadratic extension.

Proof. We first show that every quadratic extension is obtained by adjoining a root of a quadratic polynomial $f(x) \in F[x]$. To do this, we choose any element α of K which is not in F. Then $(1, \alpha)$ is a linearly independent set over F. Since K has dimension 2 as a vector space over F $(1, \alpha)$ is a basis for K over F and $K = F[\alpha]$. It follows that α^2 is a linear combination of $(1, \alpha)$ say $\alpha^2 = -b\alpha - c$, with $b, c \in F$. Then α is a root of $f(x) = x^2 + bx + c$.

Since $2 \neq 0$ in F, we can use the quadratic formula $\alpha = \frac{1}{2}(-b\sqrt{b^2 - 4ac})$ to solve the equation $x^2 + bx + c = 0$. This is proved by direct calculation. There are two choices for the square root, one of which gives our chosen root α. Let δ denote that choice: $\delta = \sqrt{b^2 - 4ac} =$

$2\alpha + b$. Then $\delta \in K$ and it also generates K over F. Its square is the discriminant $b^2 - 4ac$ which is in F.

The last proposition is clear. □

Product of Degrees

Theorem 0.1.0.4. *Let $F \subset K \subset L$ be fields. Then $[L : F] = [L : K][K : F]$. These are called towers of field extensions*

Proof. Let $B = (y_1, \ldots, y_n)$ be a bsis for L as a K-vector space and let $C = (x_1, \ldots, x_m)$ be a basis for K as an F vector space. So $[L : K] = n$ and $[K : F] = m$. We will show that the set of mn products $P = (\ldots, x_i y_j, \ldots)$ is a basis of L as an F-vector space, and this will prove the proposition. The same reasoning will work if B or C is infinite.

Let α be an element of L. Since B is a basis for L

over K we can write $\alpha = \beta_1 y_1 + \cdots + \beta_n y_n$ with $\beta_i \in K$, in a unique way. Since C is a basis for K over F each $\beta_i = a_{1i}x_1 + \cdots a_{mi}x_m$ for some $a_{ij} \in F$.

Thus $\alpha = \Sigma_{i,j} a_{ij} x_i y_j$. This shows that P spans L as an F vector space.

However we also know that the β_j is uniquely determined by α, and since B is a basis for K over F the elements a_{ij} are uniquely determined by β_j. So they are uniquely determined by α. This shows that P is linearly independent. Hence P is a basis for L as an F-vector space and we are done. □

One case to observe is the case where $F \subset K$ and $\alpha \in K$. Then we have $F \subset F(\alpha) \subset K$. And $F(\alpha)$ is an intermediary field.

Corollary 0.1.0.5. *Let K be an extension of F of finite degree n and let $\alpha \in K$. Then α is algebraic over F and it's degree divides n.*

Proof. Immediate ****MAYBE GIVE AS HOMEWORK **** □

Corollary 0.1.0.6. *Every irreducible polynomial in $\mathbb{R}[x]$ has degree 1 or 2*

Proof. □

Algebraic Subfield

Theorem 0.1.0.7. *Let K be an extension of F. The elements of K which are algebraic over F form a subfield of K.*

Proof. Let α, β be algebraic elements of K. We must show $\alpha + \beta$, $\alpha\beta$, $-\alpha$, α^{-1} are all algebraic also.

Note that since α is algebraic that $[F(\alpha) : F] < \infty$. Moreover β is algebraic over F and hence also algebraic over $F(\alpha)$. Hence $F(\alpha, \beta)$ which is generated by β over $F(\alpha)$ is a finite extension of $F(\alpha)$. I.e. $[F(\alpha, \beta) : F(\alpha)] < \infty$ and hence we know that $[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] < \infty$.

Hence every element of $F(\alpha, \beta)$ is algebraic over F and all the elements we needed to check were algebraic are in this field. □

Algebraic Extension

Definition 0.1.0.8. We say that an extension K of F is an algebraic extensions (and K is algebraic over F) if every element of K is algebraic over F.

Transitivity of Algebraic Extensions

Theorem 0.1.0.9. *Let $F \subset K \subset L$ be fields. If L is algebraic over K and K is algebraic over F, then L is algebraic over F.*

Proof. We need to show that every element $\alpha \in L$ is algebraic over F. We are given that F is algebraic over K and hence some equation of the form

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_n = 0$$

holds with $a_0, \ldots, a_{n-1} \in K$. Therefore α is algebraic over the field $F(a_0, \ldots, a_{n-1})$ generated by $a_0, \ldots, a_{n-1}$ over F. Note that each coefficient a_i, being in K is algebraic over F. We consider the chain of fields

$$F \subset F(a_0) \subset F(a_0, a_1) \subset \cdots \subset F(a_0, \ldots, a_{n-1}) \subset F(a_0, \ldots, a_{n-1}, \alpha$$

obtained by adjoining the elements $a_0, \ldots a_{n-1}, \alpha$ in succession. For each a_{i+1} is algebraic over $F(a_0, \ldots, a_i)$ because it is algebraic over F. Also α is algebraic over $F(a_0, \ldots, a_{n-1})$. So each extension in the chain is finite.

We therefore know that the degree of $F(a_0, \ldots, a_{n-1}, \alpha)$ over F is finite and hence α is algebraic over F. $\square$

0.2 Constructions with Ruler and Compass

In ancient Greece one of the favorite fields of study was constructions with a ruler and strait edge. The idea was that you started with two points one unit apart. Then given any two points you could draw a circle centered at one and going through the other and you could draw a line between to points. The questions then arose, what shapes could you make?

One of the most famous open questions from ancient Greece was, given a constructed angle, is it possible to trisect the angle (i.e. construct an angle 1/3 it's size).

Using what we know about fields, we will now show that

this is impossible. Specifically we have the following definitions

Ruler and Compass Constructions

Definition 0.2.0.10. (a) Two points in the plane are given to start with. These points are considered constructed.

(b) If two points are constructed we may draw a line through them or a circle with center at one and passing through the other. Such lines and circles are considered constructed

(c) The points and intersection of lines and circles which have been constructed are considered to be constructed.

All such constructed objects are said to be constructed with a strait edge and compass.

$\perp$ To A Line Through a Point

Theorem 0.2.0.11. *Given a constructed line l and a*

point p we can construct a line perpendicular to l and passing through p.

Proof. Construction 13.4.2 on Page 501 of the book □

Parallel Line Through A Point

Theorem 0.2.0.12. *Given a constructed line l and a point p not on l we can construct a line parallel to l and passing through p.*

Proof. Construction 13.4.3 on Page 502 of the book □

Translation of Distance

Theorem 0.2.0.13. *Given two points p, q and a constructed line l with a point r on l we can find a point s on l such that distance between r, s is the same as the distance between p and q.*

Proof. Construction 13.4.4 on Page 502 of the book □

Constructible Real Numbers

Definition 0.2.0.14. We say that a real number a s constructible if $|a|$ is the distance between two constructible points.

Theorem 0.2.0.15. *A point $p = (a, b)$ is constructible if and only if a and b ar constructible numbers.*

Proof. Given a point p we can construct its coordinates by dropping perpendiculars to the axes. Conversely if a, b are constructible numbers we can construct p by marking off a, b on the axes and constructing perpendiculars. □

Constructible Subfield of $\mathbb{R}$

Theorem 0.2.0.16. *The constructible numbers for a subfield of $\mathbb{R}$.*

Proof. We will show that if $a, b \in \mathbb{R}$ are constructible numbers then $a + b$, ab, $a - b$ (if $a > b$) and a^{-1} (if $a \neq 0$) are constructible numbers.

Addition and subtraction are dong by marking lengths on a line and using Construction 13.4.4 on page 502.

For inverses and multiplication see Proof of Proposition 13.4.6 (p. 503).

□

Constructible Subfield Is Closed Under Squar

Theorem 0.2.0.17. *If a is constructible then so is $\sqrt{|a|}$*

Proof. ********Proposition 13.4.7 Page 503 ******** □

Enlarging Constructible Subfields

Theorem 0.2.0.18. *Suppose four points are given whose coordinates are in a subfield F of $\mathbb{R}$. Let A, B be lines or circles drawn using the given points. Then*

the points of intersection of A and B have coordinates in F or in a field of the form $F(\sqrt{|r|})$ where $r \in F$.

Proof. The line through $(a_0, b_0), (a_1, b_1)$ has linear equation

$$(a_1 - a_0)(y - b_0) = (b_1 - b_0)(x - a_0)$$

The circle with center at (a_0, b_0) and passing through (a_1, b_1) has quadratic equation

$$(x - a_0)^2 + (y - b_0)^2 = (a_1 - a_0)^2 + (b_1 - b_0)^2$$

The intersection of two lines can be found by solving two linear equations with coefficients in F and hence is in F.

To find the intersection of a line and a circle we use the linear equation to eliminate one variable from the equation of the circle leaving a quadratic equation in one unknown with coefficients in F. Hence the solutions to the equation are in $F(\sqrt{D})$ where D is the discriminant of

the equation (and if $D < 0$ the line and the circle don't intersect).

Now consider the intersection of two circles say

$(x-a_1)^2+(y-b_1)^2 = r_1^2$ and $(x-a_2)^2+(y-b_2)^2 = r_2^2$

where $a_i, b_i, r_i \in F$. In general the solutions to a pair of quadratic equations is an equation of degree 4. However in this case we see that the difference between the two equations is linear and hence can be used to eliminate one of the variables in one of the equations (as in the case of a circle and a line). □

Chain Of Constructible Subfields

Theorem 0.2.0.19. *Let $a_1, \ldots, a_m$ be constructible real numbers. There is a chain of subfields $\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = K$ such that*

(a) K is a subfield of $\mathbb{R}$

(b) $a_1, \ldots, a_m \in K$.

(c) For each $i = 0, \ldots, n-1$, *the field* F_{i+1} *is obtained form* F_i *by adjoining a square rot of a positive number* $r_i \in F_i$ *which is not a square in* F_i.

Conversely let $\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = K$ *be a chain of subfields of* $\mathbb{R}$ *satisfying* (c). *Then every element of* K *is constructible.*

Proof. Introduce coordinates so that the initial points have coordinates in $\mathbb{Q}$. If we construct a number a this is done in a series of drawing lines and circles and taking their intersections. But each single intersection produces adds at most one more level to the tower (by previous results).

Similarly if we have such a tower all elements must be constructible. Also by previous results. □

Degree of Constructible Real Numbers

Corollary 0.2.0.20. *If a is a constructible real number, then it is algebraic and its degree of $\mathbb{Q}$ is a power of 2.*

Proof. In the chain of fields in the previous theorem $[F_{i+1} : F_i] = 2$ and hence if $K = F(a)$ we see that $[K : \mathbb{Q}]$ must be a power of 2. □

Now lets turn to the trisection of the angle. We have to be a little careful in how we define this as it is the case that some angles can be trisected.

Constructibility Angle

Definition 0.2.0.21. We say an angle θ is constructible if the length $cos(\theta)$ is constructible.

Trisecting The Angle

Now in general to solve the trisection problem we want to take an angle θ

and, once we are given $cos(\theta)$ to start wiht, we want to come up with a method for showing $\frac{1}{3}\theta$ is constructible from it.

So in order to show that the trisection problem has no solution it suffices to find a single constructible angle θ such that $\frac{1}{3}\theta$ is not constructible.

The angle we we will choose is $\theta = 60°$ and so we will show that it is impossible to construct a $20°$ angle. We will do this by showing that $cos(20°)$ is an algebraic number of degree 3.

The addition formulas for sin and cos can be used to prove

$$cos(3\theta) = 4coss(\theta) - 3cos(\theta)$$

Setting $\alpha = 20^\circ$ we get

$$\frac{1}{2} = 4\alpha^3 - 3\alpha$$

or

$$0 = 8\alpha^3 - 3\alpha - 1$$

Lemma 0.2.0.22. *The polynomial* $f(x) = 8x^3 - 6x - 1$ *is irreducible over* $\mathbb{Q}$.

Proof. It suffices to check for factors $(ax+b)$ where $a, b \in \mathbb{Z}$. But then we must have a divides 8 and b divides 1 (i.e. is ± 1). It isn't hard to see that none of these work. □

This then tells us that in α is of degree 3 and hence can't be constructed.

A similar technique can be used to show the following

Constructing A Regular p-gon

Corollary 0.2.0.23. *Let* p *be a prime integer. If the*

regular p-gon can be constructed by ruler and compass then $p = 2^r + 1$ *for some integer* r.

Proof. Let θ be the angle $2\pi/p$. Let $\zeta = cos(\theta) + isin(\theta)$. Then ζ is a root of $x^{p-1} + x^{p-2} + \cdots + 1 = 0$ which is irreducible. If the $p - gon$ is constructible then so are $sin(\theta), cos(\theta)$ and hence ζ lies in a real field extension of degree 2^n over $\mathbb{Q}$. Call this field K and consider $K(i)$. This extension has degree 2 over K and hence $[K(i) : \mathbb{Q}] = 2^{n+1}$. But $\zeta = cos(\theta) + isin(\theta)$ and hence is in $K(i)$. So the degree of ζ must divide 2^{n+1}. Hence $p - 1 = 2^r$ for some r □