Part II – Galois Theory

Based on lectures by Dr C. Brookes
Notes taken by Bhavik Mehta

Michaelmas 2017

Contents

0 Introduction

The primary motivation of this course is to study the solutions of polynomial equations in one variable to wander whether there is a formula involving roots, a solution by radicals. Quadratics were typically studied in school, while the solution in radicals for cubics and quartics has been known for a long time and studied in particular in 1770 by Lagrange.

In 1799, Ruffini claimed that there were some quintics that can't be solved by radicals, that is, there is no general formula, but it took until 1824 before Abel used existing ideas about permutations to produce the first accepted proof of insolubility, before dying in 1829. Galois' main contribution was in 1831, when he gave the first explanation as to why some polynomials are soluble by radicals and others are not. He made use of the group of permutations of the roots of a polynomial, and realised in particular the importance of *normal* subgroups.

Galois' work was not known generally in his lifetime - it was only published by Liouville in 1846, who realised that it tied in well with the work of Cauchy on permutations. Galois had submitted his work for various competitions and for entry into the Ecole Polytechnique in Paris. Unfortunately Galois died in a duel in 1832, leaving a six and a half page letter indicating his thoughts about the future development of his theory.

0.1 Course overview

Most of this course is Galois Theory, but presented in a more modern fashion- in terms of field extensions. Recall from GRM that if $f(t)$ is an irreducible polynomial in $k[t]$ where k is a field, then $k[t]/(f(t))$ is a field, where $(f(t))$ denotes the ideal of $k[t]$ generated by $f(t)$,

and this new field contains k. In this way, we can see the field $k[t]/(f(t))$ as a field extension of k.

Prerequisites Quite a lot of the Groups, Rings and Modules course, but no modules except in one place where it's useful to know the structure of finite abelian groups. The DPMMS website has a Galois Theory page with a long history of example sheets and notes, in particular see Tony Scholl's 2013-4 course page.

1 Field Extensions

Definition 1.1. A **field extension** $K \leq L$ is the inclusion of a field K into another field L with the same 0, 1, and where the restriction of + and . (in L) to K gives the + and . of K.

Example.

(i) $\mathbb{Q} \leq \mathbb{R}$

(ii) $\mathbb{R} \leq \mathbb{C}$

(iii) $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) = \{ \lambda + \mu\sqrt{2} \mid \lambda, \mu \in \mathbb{Q} \}$

(iv) $\{ \lambda + \mu i \mid \lambda, \mu \in \mathbb{Q} \} = \mathbb{Q}(i) \leq \mathbb{C}$

Suppose $K \leq L$ is a field extension. Then L is a K-vector space using the addition from the field structure and scalar multiplcation given by the multiplication in the field L.

Definition 1.2. The **degree** of L over K is $\dim_K L$, the K-vector space dimension of L. This may not be finite. We typically denote this by $|L : K|$. If $|L : K| < \infty$, then the extension is **finite**, otherwise the extension is **infinite**.

Example.

(i) $|\mathbb{C} : \mathbb{R}| = 2$, with $\mathbb{R}$-basis $1, i$

(ii) $|\mathbb{Q}(i) : \mathbb{Q}| = 2$, with $\mathbb{Q}$-basis $1, i$

(iii) $\mathbb{Q} \leq \mathbb{R}$ is an infinite extension.

Theorem 1.3 (Tower law)**.** Suppose $K \leq L \leq M$ are field extensions. Then $|M : K| = |M : L|\,|L : K|$.

Proof. Assume that $|M : L| < \infty$, and $|L : K| < \infty$. Take an L-basis of M, given by $\{ f_1, \ldots, f_b \}$, and a K-basis of L given by $\{ e_1, \ldots, e_a \}$. Take $m \in M$, so $m = \sum_{i=1}^{b} \mu_i f_i$ for some $\mu_i \in L$. Similarly, $\mu_i = \sum_{j=1}^{a} \lambda_{ij} e_j$ for some $\lambda_{ij} \in K$, so

$$m = \sum_{i=1}^{b} \sum_{j=1}^{a} \lambda_{ij} e_j f_i$$

Thus $\{ e_j f_i \mid 1 \leq j \leq a, 1 \leq i \leq a \}$ span M.

Linear independence: It's enough to show that if $0 = m = \sum \sum \lambda_{ij} e_j f_i$ then λ_{ij} are all zero. However if $m = 0$ the linear independence of f_i forces each $\mu_i = 0$. Then the linear indepedence of e_j forces λ_{ij} all to be zero, as required. □

The tower law will not be proved for infinite extensions, but observe that if M is an infinite extension of L then it is an infinite extension of K, and similarly if L is an infinite extension of K then the larger field M must also be an infinite extension of K.

1.1 Motivatory Example

Observe $\mathbb{Q} \leq \mathbb{Q}\left(\sqrt{2}\right) \leq \mathbb{Q}\left(\sqrt{2}, i\right)$

(i) $\mathbb{Q}\left(\sqrt{2}\right)$ has basis $1, \sqrt{2}$ over $\mathbb{Q}$.

(ii) $\mathbb{Q}\left(\sqrt{2}, i\right)$ has basis $1, i$ as a $\mathbb{Q}\left(\sqrt{2}\right)$–vector space.

(iii) $\mathbb{Q}\left(\sqrt{2}, i\right)$ has basis $1, \sqrt{2}, i, i\sqrt{2}$ over $\mathbb{Q}$.

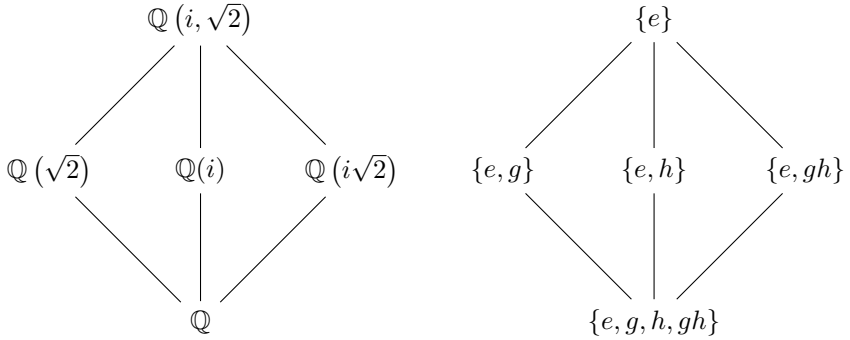
$$\left|\mathbb{Q}\left(i, \sqrt{2}\right) : \mathbb{Q}\right| = 4 = 2 \cdot 2 = \left|\mathbb{Q}\left(i, \sqrt{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right| \left|\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right|$$

Any intermediate field strictly between $\mathbb{Q}$ and $\mathbb{Q}\left(\sqrt{2}, i\right)$ must be of degree 2 by the tower law. What are these intermediate fields? There are $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathbb{Q}(i)$ and $\mathbb{Q}\left(i\sqrt{2}\right)$, but are these all?

The Galois correspodence arising in the Fundamental Theorem of Galois theory gives an order reversing bijection between the lattice of intermediate subfields and the subgroups of a group of ring automorphisms of the big field (in this case $\mathbb{Q}\left(i, \sqrt{2}\right)$) that fix the smaller field elementwise. For instance, consider the ring automorphisms of $\mathbb{Q}\left(i, \sqrt{2}\right)$ that fix $\mathbb{Q}$:

$$\begin{aligned} e : \sqrt{2} &\mapsto \sqrt{2} \\ i &\mapsto i \\ g : \sqrt{2} &\mapsto \sqrt{2} \\ i &\mapsto -i \\ h : \sqrt{2} &\mapsto -\sqrt{2} \\ i &\mapsto i \\ gh : \sqrt{2} &\mapsto -\sqrt{2} \\ i &\mapsto -i \end{aligned}$$

Notice that i and $-i$ play the same role in the field $\mathbb{Q}\left(\sqrt{2}, i\right)$, both roots of $t^2 + 1 = 0$, similarly $\sqrt{2}$ and $-\sqrt{2}$ are both roots of $t^2 - 2 = 0$. The automorphism e is seen to be identity, and g is conjugation. These four form the group of order $4 = \left|\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\right|$.



The recipe for producing an intermediate subfield from a subgroup is to take the elements of $\mathbb{Q}\left(i, \sqrt{2}\right)$ which are fixed by all elements of the subgroup. For instance, $\mathbb{Q}\left(i\sqrt{2}\right)$ is the field of elements fixed by both e and gh.

This correspondence doesn't always work for all finite field extensions. It works for Galois extensions. In the correspondence, normal extensions correspond to normal subgroups. In this example, all subgroups are normal and the extensions are normal. We'll also prove the Primitive Element Theorem, which in the context of finite extensions of $\mathbb{Q}$ tells us that they are necessarily of the form $\mathbb{Q}(\alpha)$ for some α, for instance $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2})$.

1.2 Review of GRM

Definition 1.4. Suppose $K \leq L$ is a field extension. Take $\alpha \in L$ and define

$$I_\alpha = \{\, f \in K(t) \mid f(\alpha) = 0 \,\}$$

We say α is **algebraic** over K if $I_\alpha \neq 0$. Otherwise α is **transcendental**. We say L is algebraic over K if α is algebraic over K for all $\alpha \in L$.

Remark. We can see I_α is an ideal of $K[t]$ since it is the kernel of the ring homomorphism $K[t] \to L$ given by $f(t) \mapsto f(\alpha)$.

Example.

(i) $\sqrt{2}$ is algebraic over $\mathbb{Q}$

(ii) π is algebraic over $\mathbb{Q}$

Lemma 1.5. Let $K \leq L$ be a finite field extension. Then L is algebraic over K.

Proof. Let $|L : K| = n$, and take $\alpha \in L$. Consider $1, \alpha, \alpha^2, \ldots, \alpha^n$, which must be linearly dependent in the n-dimensional K–vector space L. So, $\sum_{i=0}^{n} \lambda_i \alpha^i = 0$ for some $\lambda \in K$ not all zero, and hence α is a root of $f(t) = \sum_{i=0}^{n} \lambda_i t^i$, so α is algebraic over K. α was arbitrary, so L is algebraic over K. □

Definition 1.6. The non-zero ideal I_α (where α is algebraic over K) is principal since $K[t]$ is a principal ideal domain. In particular, we can say $I_\alpha = (f_\alpha(t))$ where $f_\alpha(t)$ can be assumed to be monic. Such a monic $f_\alpha(t)$ is the **minimal polynomial** of α over K.

Remark. Multiplication by α within the field L gives a K–linear map $L \to L$, an automorphism (if $\alpha \neq 0$). In GRM, we have seen the minimal polynomial of a linear map is unique.

Example.

(i) The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $t^2 - 2$.

(ii) The minimal polynomial of $\sqrt{2}$ over $\mathbb{R}$ is $t - \sqrt{2}$.

Lemma 1.7. Suppose $K \leq L$ is a field extension, $\alpha \in L$ and α is algebraic over K. Then the minimal polynomial $f_\alpha(t)$ of α over K is irreducible in $K[t]$ and I_α is a prime ideal.

Proof. Suppose $f_\alpha(t) = p(t)q(t)$. We aim to show $p(t)$ or $q(t)$ is a unit in $K[t]$. But $0 = f_\alpha(\alpha) = p(\alpha)q(\alpha)$, so $p(\alpha) = 0$ or $q(\alpha) = 0$, without loss of generality take $p(\alpha) = 0$, thus $p(t) \in I_\alpha$. But $I_\alpha = (f_\alpha(t))$, so $p(t) = f_\alpha(t)r(t)$, giving $f_\alpha(t) = f_\alpha(t)r(t)q(t)$ and so $r(t)q(t) = 1$ in $K[t]$, and $q(t)$ is a unit, as required. Recall from GRM that irreducible elements of $K[t]$ are prime and hence generate prime ideals of $K[t]$. So I_α is a prime ideal. □

Definition 1.8. Suppose $K \leq L$ is a field extension and $\alpha \in L$. $K(\alpha)$ is defined to be the smallest subfield of L containing K and α. It's called the field **generated** by K and α. We say that L is a **simple extension** if $L = K(\beta)$ for some $\beta \in L$.

Given $\alpha_1, \ldots, \alpha_n \in L$, $K \leq L$. $K(\alpha_1, \ldots \alpha_n)$ is the smallest field containing $\alpha_1, \ldots, \alpha_n$. It is the field generated by K and $\alpha_1, \ldots, \alpha_n$.

On the other hand $K[\alpha]$ is the ring generated by K and
alpha, in particular the image of $K[t]$ under the map $f(t) \mapsto f(\alpha)$.

Theorem 1.9. Suppose $K \leq L$ is a field extension and $\alpha \in L$ is algebraic over K. Then

(i) $K(\alpha) = K[\alpha]$

(ii) $|K(\alpha) : K| = \deg f_\alpha(t)$ where $f_\alpha(t)$ is the minimal polynomial of α over K.

Proof.

(i) Clearly $K[\alpha] \leq K(\alpha)$. We aim to show that any non-zero element β of $K[\alpha]$ is a unit, so $K[\alpha]$ is a field.

By definition of $K[\alpha]$, $\beta = g(\alpha)$ for some $g(t) \in K[t]$. Since $\beta = g(\alpha) \neq 0$, $g(t) \notin I_\alpha = (f_\alpha(t))$. Thus $f_\alpha(t) \nmid g(t)$. From lemma 1.7, $f_\alpha(t)$ is irreducible and $K[t]$ is a PID, we know $\exists r(t), s(t) \in K[t]$ with $r(t)f_\alpha(t) + s(t)g(t) = 1$ in $K[t]$. Hence $s(\alpha)g(\alpha) = 1$ in $K[\alpha]$, and so $\beta = g(\alpha)$ is a unit as required.

(ii) Let $n = \deg f_\alpha(t)$ We'll show that $T = \{ 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \}$ is a K–vector space.

Spanning: If $f_\alpha(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ with $a_i \in K$, then $\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$. This implies α^n is a linear combination of $\{ 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \}$, and an easy induction shows that α^m for $m \geq n$ is likewise a linear combination of $\{ 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \}$, so we have spanning.

Linear independence: Suppose $\lambda_{n-1}\alpha^{n-1} + \ldots + \lambda_0 = 0$. Let $g(t) = \lambda_{n-1}t^{n-1} + \ldots + \lambda_0$. Since $g(\alpha) = 0$, we have $g(t) \in I_\alpha = (f_\alpha(t))$. So $g(t) = 0$ or $f_\alpha(t) \mid g(t)$. The latter is not possible since $\deg f_\alpha(t) > \deg g_\alpha(t)$ so $g(t) = 0$ in $K[t]$ and all the λ_i's are zero.

□

Corollary 1.10. If $K \leq L$ is a field extension and $\alpha \in L$, then α is algebraic over K if and only if $K \leq K(\alpha)$ is finite.

Proof. $\Rightarrow$ By theorem 1.9, $|K(\alpha) : K| = \deg f_\alpha(t) \leq \infty$.
$\Leftarrow$ Lemma 1.5 □

Corollary 1.11. Let $K \leq L$ be a field extension with $|L : K| = n$. Let $\alpha \in L$, then $\deg f_\alpha(t) \mid n$.

Proof. Use the Tower Law on $K \leq K(\alpha) \leq L$. We deduce that $|K(\alpha) : K|$ divides $|L : K|$. Theorem 1.9(ii) gives $\deg f_\alpha(t) = |K(\alpha) : K|$. □

1.3 Digression on (Non-)Constructibility

Schedules mention 'other classical problems' and we are now in a position to tackle some of these using corollary 1.11.

A classical question from Greek geometry concerns the existence or otherwise of constructions using ruler and compasses (where a ruler refers to a single unmarked straight edge). If you're an expert you can divide a line betwen 2 points into arbitrarily many equal segments, you can bisect an angle, or you can produce parallel lines. Given a polygon you can produce a square of the same area or double the area. However,

1. You cannot duplicate the cube using ruler and compasses (given a cube you can't produce a cube of double the volume)
2. You cannot trisect the angle $\pi/3$ using ruler and compasses.
3. The circle cannot be squared using ruler and compasses (given a circle you can't construct a square of the same area)

Assume we're given a set P_0 of points in $\mathbb{R}^2$, and we can formalise our operations.

Ruler operation Draw a straight line through any two points in P_0.

Compass operation Draw a circle with centre being a point in P_0 and radius the distance between a pair of points in P_0.

Definition 1.12 (Constructible)**.** The points of intersection of any two distinct lines or circles drawn using these operations are **constructible in one step** from P_0. More generally, a point $\mathbf{r} \in \mathbb{R}^2$ is **constructible** from P_0 if there is a finite sequence $\mathbf{r_1}, \mathbf{r_2}, \ldots, \mathbf{r_n} = \mathbf{r}$ such that $\mathbf{r_i}$ is constructible in one step from $P_0 \cup \{\, \mathbf{r_1}, \ldots, \mathbf{r_{i-1}} \,\}$.

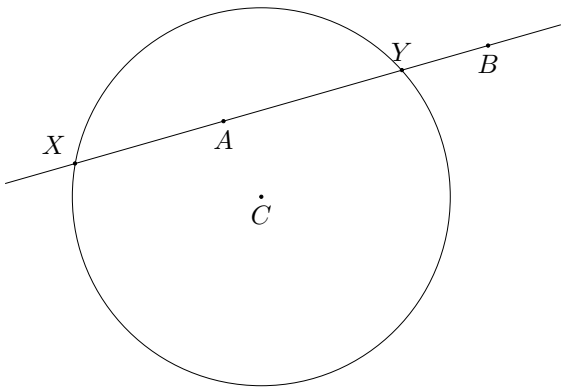
Exercise. Construct the midpoint of a line between two points.

Let K_0 be the subfield of $\mathbb{R}$ generated by $\mathbb{Q}$ and the co-ordinates of the points in P_0. Let $\mathbf{r_i} = (x_i, y_i)$ and set $K_i = K_{i-1}(x_i, y_i)$.

Thus $K_0 \leq K_1 \leq K_2 \leq \cdots \leq K_m \leq \mathbb{R}$.

Lemma 1.13. x_i, y_i are both roots in K_i of quadratic polynomials in $K_{i-1}[t]$.

Proof. There are three cases for $\mathbf{r_i}$: line meets line, line meets circle, circle meets circle. We do the second case only here.



The line is defined by two points $A = (p, q)$ and $B = (r, s)$ while the circle is defined with a centre $C = (t, u)$ and radius w. Then, points X and Y satisfy the equation of the line $\frac{x-p}{r-p} = \frac{y-q}{s-q}$, and the equation of the circle $(x-t)^2 + (y-u)^2 = w^2$. Solving these together gives coordinates of X and Y satisfying quadratic polynomials over K_{i-1}. The other two cases are left as an exercise for the reader. □

Theorem 1.14. If $\mathbf{r} = (x, y)$ is constructible from a set P_0 of points in $\mathbb{R}^2$ and if K_0 is the subfield of $\mathbb{R}$ generated by $\mathbb{Q}$ and the coordinates of the points in P_0, then the degrees $|K_0(x) : K_0|$ and $|K_0(y) : K_0|$ are powers of two.

Proof. Continue with the previous notation of $K_i = K_{i-1}(x_i, y_i)$. By the Tower Law,

$$|K_i : K_{i-1}| = |K_{i-1}(x, y) : K_{i-1}(x)|\,|K_{i-1}(x) : K_{i-1}|$$

But lemma 1.13 tells us that $|K_{i-1}(x) : K_{i-1}|$ must be $= 1$ or 2 depending on whether the quadratic polynomial arising in lemma 1.13 is reducible or not, using degree of the extension = degree of the minimal polynomial of x over K_{i-1}, and hence over $K_{i-1}(x)$, and so $|K_{i-1}(x, y) : K_{i-1}(x)| = 1$ or 2.

So $|K_i : K_{i-1}| = 1, 2$ or 4, (but in fact 4 cannot happen), hence by the Tower Law, $|K_n : K_0| = |K_n : K_{n-1}|\,|K_{n-1} : K_{n-2}| \ldots |K_1 : K_0|$ is a power of two.

If $r = (x, y)$ is constructible from P_0, then

$$\begin{aligned} x, y \in K_n \quad \text{and} \quad & K_0 \leq K_0(x) \leq K_n \\ & K_0 \leq K_0(y) \leq K_n \end{aligned}$$

and the Tower Law again gives that $|K_0(x) : K_0|$ and $|K_0(y) : K_0|$ are also powers of 2. □

To use this for proofs about non-constructibility we need to be reasonably expert at working out minimal polynomials.

Theorem 1.15. Let $f(t)$ be a primitive integral polynomial. Then $f(t)$ is irreducible in $\mathbb{Q}[t]$ if and only if it is irreducible in $\mathbb{Z}[t]$.

Proof. A special case of Gauss' lemma from GRM. □

Theorem 1.16 (Eisenstein's criterion)**.** Let $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 \in \mathbb{Z}[t]$. Suppose there is a prime p such that

(i) $p \nmid a_n$

(ii) $p \mid a_{n-1}$, $p \mid a_{n-2}, \ldots, p \mid a_0$

(iii) $p^2 \mid a_0$

Then $f(t)$ is irreducible in $\mathbb{Z}[t]$

Proof. Recall from GRM. □

Example. For p a prime, consider $f(t) = t^{p-1} + t^{p-2} + \cdots + 1$. This is irreducible over $\mathbb{Q}$ by considering $f(t+1)$ and using p as the prime in Eisenstein's criterion.

Another method is to consider an integral polynomial $f(t) \pmod p$. If $f(t)$ is irreducible in $\mathbb{Z}[t]$ then it is reducible over $\mathbb{Z}/p\mathbb{Z}$. So, if we find a prime p such that $f(t) \pmod p$ is irreducible then $f(t)$ is irreducible in $\mathbb{Z}[t]$.

Example. $t^3 + t + 1$ is irreducible mod 2. If it were reducible it would have a linear factor and so the polynomial would have a root mod 2. But $0, 1$ are not roots. So, $t^3 + t + 1$ is irreducible in $\mathbb{Z}[t]$, hence irreducible in $\mathbb{Q}[t]$.

Remark. On later example sheet you'll meet an irreducible polynomial in $\mathbb{Z}[t]$ which is reducible mod p for all primes p.

Theorem 1.17. The cube cannot be duplicated by ruler and compasses.

Proof. The problem amounts to whether given a unit distance, one can construct points distance α apart, where α satisfies $t^3 - 2 = 0$. Starting with points $P_0 = \{(0,0), (1,0)\}$ can we produce $(\alpha, 0)$?

No. If we could, theorem 1.14 would say $|\mathbb{Q}\alpha : \mathbb{Q}|$ is a power of 2. But $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 3$ since $|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg f_\alpha(t)$ where $f_\alpha(t)$ is the [minimal polynomial] of α over $\mathbb{Q}$. α satisfies $t^3 - 2$. By Eisenstein's criterion this is irreducible over $\mathbb{Z}$ and hence over $\mathbb{Q}$. So $t^3 - 2$ is the minimal polynomial $f_\alpha(t)$. □

Theorem 1.18. The circle cannot be squared using ruler and compasses.

Proof. Starting with $(0,0)$ and $(1,0)$, we must construct $(\sqrt{\pi}, 0)$ so that we have a square of side length $\sqrt{\pi}$ and hence area π. But π and hence $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$. (Lindemann - not proved here) Theorem 1.14 tells us we can't do this construction. □

1.4 Return to theory development

Lemma 1.19. Let $K \leq L$ be a field extension. Then

(i) $\alpha_1, \ldots, \alpha_n \in L$ are algebraic over K if and only if $K \leq K(\alpha_1, \ldots \alpha_n)$ is a field extension.

(ii) If $K \leq M \leq L$ such that $K \leq M$ is finite, then there exist $\alpha_1, \ldots \alpha_n \in L$ such that $K(\alpha_1, \ldots \alpha_n) = M$.

Proof. 1. By corollary 1.10, α is algebraic over K if and only if $K \leq K[\alpha]$ is a finite field extension. α_i is algebraic over K and hence algebraic over $K(\alpha_1, \ldots \alpha_{i-1})$ and so $|K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})| < \infty$. By the tower law applied to $K \leq K(\alpha_1) \leq K(\alpha_1, \alpha_2) \leq \cdots \leq K(\alpha_1, \ldots \alpha_n)$, we get $|K(\alpha_1, \ldots \alpha_n) : K| < \infty$

Conversely, consider $K \leq K(\alpha_1) \leq K_(\alpha_1, \ldots \alpha_n)$. Then the tower law says that if $|K(\alpha_1, \ldots, \alpha_n) : K| \leq \infty$ then $|K(\alpha_1) : K| < \infty$ and corollary 1.10 gives α is algebraic over K.

2. If $|M : K| = n$ then M is an n-dimensional K-vector space, so there exists a K-basis $\alpha_1, \ldots, \alpha_n$ over M. Then $K(\alpha_1, \ldots, \alpha_n) \leq M$. However, any element of M is a K-linear ocmbination of $\alpha_1, \ldots, \alpha_n$ and so lies in $K(\alpha_1, \ldots, \alpha_n)$, so $M = K(\alpha_1, \ldots, \alpha_n)$. □