Modern Algebra

Chapter V. Fields and Galois Theory

V.1.Appendix. Ruler and Compass Constructions—Proofs of Theorems

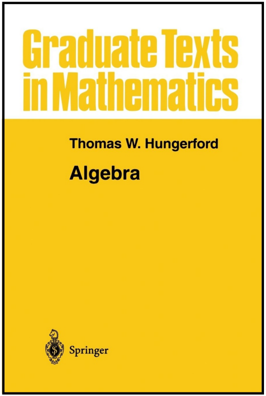

Table of contents

Lemma V.1.15

Lemma V.1.15. Let F be a subfield of the field $\mathbb{R}$ of real numbers and let L_1, L_2 be nonparallel lines in F and C_1, C_2 distinct circles in F. Then

(i) $L_1 \cap L_2$ is a point in the plane of F;

(ii) $L_1 \cap C_1 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$;

(iii) $C_1 \cap C_2 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$.

Proof. (i) Let L_1 have equation $a_1 x + b_1 y + c_1 = 0$ and let line L_2 have equation $a_2 x + b_2 y + c_2 = 0$.

Lemma V.1.15

Lemma V.1.15. Let F be a subfield of the field $\mathbb{R}$ of real numbers and let L_1, L_2 be nonparallel lines in F and C_1, C_2 distinct circles in F. Then

(i) $L_1 \cap L_2$ is a point in the plane of F;

(ii) $L_1 \cap C_1 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$;

(iii) $C_1 \cap C_2 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$.

Proof. (i) Let L_1 have equation $a_1x + b_1y + c_1 = 0$ and let line L_2 have equation $a_2x + b_2y + c_2 = 0$. Then we find that the only common point to L_1 and L_2 is $x = (b_1c_2 - b_2c_1)/(a_1b_2 - a_2b_1)$ and $y =)a_1c_2 - a_2c_1)/(a_2b_1 - a_1b_2)$ where $a_1b_2 - a_2b_1 \neq 0$ since L_1 and L_2 are nonparallel. Notice that $x, y \in F$ since F is a field.

Lemma V.1.15

Lemma V.1.15. Let F be a subfield of the field $\mathbb{R}$ of real numbers and let L_1, L_2 be nonparallel lines in F and C_1, C_2 distinct circles in F. Then

(i) $L_1 \cap L_2$ is a point in the plane of F;

(ii) $L_1 \cap C_1 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$;

(iii) $C_1 \cap C_2 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$.

Proof. (i) Let L_1 have equation $a_1x + b_1y + c_1 = 0$ and let line L_2 have equation $a_2x + b_2y + c_2 = 0$. Then we find that the only common point to L_1 and L_2 is $x = (b_1c_2 - b_2c_1)/(a_1b_2 - a_2b_1)$ and $y =)a_1c_2 - a_2c_1)/(a_2b_1 - a_1b_2)$ where $a_1b_2 - a_2b_1 \neq 0$ since L_1 and L_2 are nonparallel. Notice that $x, y \in F$ since F is a field.

Lemma V.1.15

Lemma V.1.15. Let F be a subfield of the field $\mathbb{R}$ of real numbers and let L_1, L_2 be nonparallel lines in F and C_1, C_2 distinct circles in F. Then

(ii) $L_1 \cap C_1 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$;

(iii) $C_1 \cap C_2 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$.

Proof. (iii) Let C_1 have equation $x^2 + y^2 + a_1x + b_1y + c_1 = 0$ and let C_2 have equation $x^2 + y^2 + a_2x + b_2y + c_2 = 0$ where $a_1, a_2, b_1, b_2, c_1, c_2 \in F$. Then if (x, y) lies on both C_1 and C_2, we also have that (x, y) lies on the line L with equation $(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0$ (from "subtracting C_2 from C_1"). So a point (x, y) lies on both C_1 and C_2 if and only if it lies on both C_1 and L. So case (iii) reduces to case (ii).

Lemma V.1.15

Lemma V.1.15. Let F be a subfield of the field $\mathbb{R}$ of real numbers and let L_1, L_2 be nonparallel lines in F and C_1, C_2 distinct circles in F. Then

(ii) $L_1 \cap C_1 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$;

(iii) $C_1 \cap C_2 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$.

Proof. (iii) Let C_1 have equation $x^2 + y^2 + a_1x + b_1y + c_1 = 0$ and let C_2 have equation $x^2 + y^2 + a_2x + b_2y + c_2 = 0$ where $a_1, a_2, b_1, b_2, c_1, c_2 \in F$. Then if (x, y) lies on both C_1 and C_2, we also have that (x, y) lies on the line L with equation $(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0$ (from "subtracting C_2 from C_1"). So a point (x, y) lies on both C_1 and C_2 if and only if it lies on both C_1 and L. So case (iii) reduces to case (ii).

Lemma V.1.15

Lemma V.1.15. Let F be a subfield of the field $\mathbb{R}$ of real numbers and let L_1, L_2 be nonparallel lines in F and C_1, C_2 distinct circles in F. Then

(ii) $L_1 \cap C_1 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$.

Proof. **(ii)** Suppose line L_1 has the equation $dx + ey + f = 0$ where $d, e, f \in F$ (and C_1 has the equation given above).

Lemma V.1.15

Lemma V.1.15. Let F be a subfield of the field $\mathbb{R}$ of real numbers and let L_1, L_2 be nonparallel lines in F and C_1, C_2 distinct circles in F. Then

(ii) $L_1 \cap C_1 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$.

Proof. (ii) Suppose line L_1 has the equation $dx + ey + f = 0$ where $d, e, f \in F$ (and C_1 has the equation given above).
If $d = 0$ then $e \neq 0$ and the only (x, y) on both L and C_1 satisfies $ey + f = 0$ and $x^2 + y^2 + a_1x + b_1y + c_1 = 0$. Then we have $y = -f/e$ and so $x^2 + (-f/e)^2 + a_1x + b_1(-f/e) + c_1 = 0$ or $e^2x^2 + e^2a_1x + (f^2 - efb_1 + e^2c_1) = 0$.

Lemma V.1.15

Lemma V.1.15. Let F be a subfield of the field $\mathbb{R}$ of real numbers and let L_1, L_2 be nonparallel lines in F and C_1, C_2 distinct circles in F. Then

(ii) $L_1 \cap C_1 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$.

Proof. (ii) Suppose line L_1 has the equation $dx + ey + f = 0$ where $d, e, f \in F$ (and C_1 has the equation given above).
If $d = 0$ then $e \neq 0$ and the only (x, y) on both L and C_1 satisfies $ey + f = 0$ and $x^2 + y^2 + a_1x + b_1y + c_1 = 0$. Then we have $y = -f/e$ and so $x^2 + (-f/e)^2 + a_1x + b_1(-f/e) + c_1 = 0$ or $e^2x^2 + e^2a_1x + (f^2 - efb_1 + e^2c_1) = 0$. The quadratic equation then gives

$$x = \frac{-e^2a_1 \pm \sqrt{(e^2a_1)^2 - 4(e^2)(f^2 - efb_1 + e^2c_1)}}{2e^2}.$$

Lemma V.1.15

Lemma V.1.15. Let F be a subfield of the field $\mathbb{R}$ of real numbers and let L_1, L_2 be nonparallel lines in F and C_1, C_2 distinct circles in F. Then

(ii) $L_1 \cap C_1 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$.

Proof. (ii) Suppose line L_1 has the equation $dx + ey + f = 0$ where $d, e, f \in F$ (and C_1 has the equation given above).
If $d = 0$ then $e \neq 0$ and the only (x, y) on both L and C_1 satisfies $ey + f = 0$ and $x^2 + y^2 + a_1 x + b_1 y + c_1 = 0$. Then we have $y = -f/e$ and so $x^2 + (-f/e)^2 + a_1 x + b_1(-f/e) + c_1 = 0$ or $e^2 x^2 + e^2 a_1 x + (f^2 - efb_1 + e^2 c_1) = 0$. The quadratic equation then gives

$$x = \frac{-e^2 a_1 \pm \sqrt{(e^2 a_1)^2 - 4(e^2)(f^2 - efb_1 + e^2 c_1)}}{2e^2}.$$

Let $u = (e^2 a_1)^2 - 4(e^2)(f^2 - efb_1 + e^2 c_1)$. If $u < 0$ then $L_1 \cap C_1 = \varnothing$.

Lemma V.1.15

Lemma V.1.15. Let F be a subfield of the field $\mathbb{R}$ of real numbers and let L_1, L_2 be nonparallel lines in F and C_1, C_2 distinct circles in F. Then

(ii) $L_1 \cap C_1 = \varnothing$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$ where $u \geq 0$.

Proof. (ii) Suppose line L_1 has the equation $dx + ey + f = 0$ where $d, e, f \in F$ (and C_1 has the equation given above).
If $d = 0$ then $e \neq 0$ and the only (x, y) on both L and C_1 satisfies $ey + f = 0$ and $x^2 + y^2 + a_1x + b_1y + c_1 = 0$. Then we have $y = -f/e$ and so $x^2 + (-f/e)^2 + a_1x + b_1(-f/e) + c_1 = 0$ or $e^2x^2 + e^2a_1x + (f^2 - efb_1 + e^2c_1) = 0$. The quadratic equation then gives

$$x = \frac{-e^2a_1 \pm \sqrt{(e^2a_1)^2 - 4(e^2)(f^2 - efb_1 + e^2c_1)}}{2e^2}.$$

Let $u = (e^2a_1)^2 - 4(e^2)(f^2 - efb_1 + e^2c_1)$. If $u < 0$ then $L_1 \cap C_1 = \varnothing$.

Lemma V.1.15 (continued)

Proof (continued). (ii) If $u = 0$ then $x = -a_1/2$ and $y = -f/e$ and there is one point on both L_1 and C_1. If $u > 0$ then there are two points on L_1 and C_1 and x is in terms of $\sqrt{u}$; so the two points lie in $F(\sqrt{u})$.
If $d \neq 0$ then we can "normalize" the equation for L_1 and WLOG assume $d = 1$, so that $x + ey + f = 0$, or $x = -ey - f$. So a point (x, y) lies on both L_1 and C_1 then
$(-ey - f)^2 + y^2 + a_1(-ey - f) + b_1 y + c_1 = Ay^2 + By + C = 0$ where $A, B, C \in F$.

Lemma V.1.15 (continued)

Proof (continued). (ii) If $u = 0$ then $x = -a_1/2$ and $y = -f/e$ and there is one point on both L_1 and C_1. If $u > 0$ then there are two points on L_1 and C_1 and x is in terms of $\sqrt{u}$; so the two points lie in $F(\sqrt{u})$. If $d \neq 0$ then we can "normalize" the equation for L_1 and WLOG assume $d = 1$, so that $x + ey + f = 0$, or $x = -ey - f$. So a point (x, y) lies on both L_1 and C_1 then
$(-ey - f)^2 + y^2 + a_1(-ey - f) + b_1 y + c_1 = Ay^2 + By + C = 0$ where $A, B, C \in F$. If $A = 0$ then $y \in F$ and so $x \in F$. Then $x, y \in F = F(\sqrt{1})$.

Lemma V.1.15 (continued)

Proof (continued). (ii) If $u = 0$ then $x = -a_1/2$ and $y = -f/e$ and there is one point on both L_1 and C_1. If $u > 0$ then there are two points on L_1 and C_1 and x is in terms of $\sqrt{u}$; so the two points lie in $F(\sqrt{u})$. If $d \neq 0$ then we can "normalize" the equation for L_1 and WLOG assume $d = 1$, so that $x + ey + f = 0$, or $x = -ey - f$. So a point (x, y) lies on both L_1 and C_1 then $(-ey - f)^2 + y^2 + a_1(-ey - f) + b_1 y + c_1 = Ay^2 + By + C = 0$ where $A, B, C \in F$. If $A = 0$ then $y \in F$ and so $x \in F$. Then $x, y \in F = F(\sqrt{1})$. If $A \neq 0$ then again by normalizing we may assume $A = 1$ and we need $y^2 + By + C = 0$. Completing the square yields $(y + B/2)^2 + (C - B^2/4) = 0$. This gives $y = -B/2 \pm \sqrt{-C + B^2/4}$.

Lemma V.1.15 (continued)

Proof (continued). (ii) If $u = 0$ then $x = -a_1/2$ and $y = -f/e$ and there is one point on both L_1 and C_1. If $u > 0$ then there are two points on L_1 and C_1 and x is in terms of $\sqrt{u}$; so the two points lie in $F(\sqrt{u})$. If $d \neq 0$ then we can "normalize" the equation for L_1 and WLOG assume $d = 1$, so that $x + ey + f = 0$, or $x = -ey - f$. So a point (x, y) lies on both L_1 and C_1 then
$(-ey - f)^2 + y^2 + a_1(-ey - f) + b_1 y + c_1 = Ay^2 + By + C = 0$ where $A, B, C \in F$. If $A = 0$ then $y \in F$ and so $x \in F$. Then $x, y \in F = F(\sqrt{1})$. If $A \neq 0$ then again by normalizing we may assume $A = 1$ and we need $y^2 + By + C = 0$. Completing the square yields
$(y + B/2)^2 + (C - B^2/4) = 0$. This gives $y = -B/2 \pm \sqrt{-C + B^2/4}$. Let $u = -C + B^2/4$. Then $L_1 \cap C_1 = \varnothing$ if $u < 0$.

Lemma V.1.15 (continued)

Proof (continued). (ii) If $u = 0$ then $x = -a_1/2$ and $y = -f/e$ and there is one point on both L_1 and C_1. If $u > 0$ then there are two points on L_1 and C_1 and x is in terms of $\sqrt{u}$; so the two points lie in $F(\sqrt{u})$.
If $d \neq 0$ then we can "normalize" the equation for L_1 and WLOG assume $d = 1$, so that $x + ey + f = 0$, or $x = -ey - f$. So a point (x, y) lies on both L_1 and C_1 then
$(-ey - f)^2 + y^2 + a_1(-ey - f) + b_1 y + c_1 = Ay^2 + By + C = 0$ where $A, B, C \in F$. If $A = 0$ then $y \in F$ and so $x \in F$. Then $x, y \in F = F(\sqrt{1})$.
If $A \neq 0$ then again by normalizing we may assume $A = 1$ and we need $y^2 + By + C = 0$. Completing the square yields
$(y + B/2)^2 + (C - B^2/4) = 0$. This gives $y = -B/2 \pm \sqrt{-C + B^2/4}$.
Let $u = -C + B^2/4$. Then $L_1 \cap C_1 = \varnothing$ if $u < 0$. If $u = 0$ then there is one point (x, y) on $L_1 \cap C_1$ where $x, y \in F = F(0)$.

Lemma V.1.15 (continued)

Proof (continued). (ii) If $u = 0$ then $x = -a_1/2$ and $y = -f/e$ and there is one point on both L_1 and C_1. If $u > 0$ then there are two points on L_1 and C_1 and x is in terms of $\sqrt{u}$; so the two points lie in $F(\sqrt{u})$. If $d \neq 0$ then we can "normalize" the equation for L_1 and WLOG assume $d = 1$, so that $x + ey + f = 0$, or $x = -ey - f$. So a point (x, y) lies on both L_1 and C_1 then
$(-ey - f)^2 + y^2 + a_1(-ey - f) + b_1 y + c_1 = Ay^2 + By + C = 0$ where $A, B, C \in F$. If $A = 0$ then $y \in F$ and so $x \in F$. Then $x, y \in F = F(\sqrt{1})$. If $A \neq 0$ then again by normalizing we may assume $A = 1$ and we need $y^2 + By + C = 0$. Completing the square yields
$(y + B/2)^2 + (C - B^2/4) = 0$. This gives $y = -B/2 \pm \sqrt{-C + B^2/4}$. Let $u = -C + B^2/4$. Then $L_1 \cap C_1 = \varnothing$ if $u < 0$. If $u = 0$ then there is one point (x, y) on $L_1 \cap C_1$ where $x, y \in F = F(0)$. If $u > 0$ then there are two points (x, y) on $L_1 \cap C_1$ both of which satisfy $x, y \in F(\sqrt{u})$. □

Lemma V.1.15 (continued)

Proof (continued). (ii) If $u = 0$ then $x = -a_1/2$ and $y = -f/e$ and there is one point on both L_1 and C_1. If $u > 0$ then there are two points on L_1 and C_1 and x is in terms of $\sqrt{u}$; so the two points lie in $F(\sqrt{u})$. If $d \neq 0$ then we can "normalize" the equation for L_1 and WLOG assume $d = 1$, so that $x + ey + f = 0$, or $x = -ey - f$. So a point (x, y) lies on both L_1 and C_1 then
$(-ey - f)^2 + y^2 + a_1(-ey - f) + b_1 y + c_1 = Ay^2 + By + C = 0$ where $A, B, C \in F$. If $A = 0$ then $y \in F$ and so $x \in F$. Then $x, y \in F = F(\sqrt{1})$. If $A \neq 0$ then again by normalizing we may assume $A = 1$ and we need $y^2 + By + C = 0$. Completing the square yields
$(y + B/2)^2 + (C - B^2/4) = 0$. This gives $y = -B/2 \pm \sqrt{-C + B^2/4}$. Let $u = -C + B^2/4$. Then $L_1 \cap C_1 = \varnothing$ if $u < 0$. If $u = 0$ then there is one point (x, y) on $L_1 \cap C_1$ where $x, y \in F = F(0)$. If $u > 0$ then there are two points (x, y) on $L_1 \cap C_1$ both of which satisfy $x, y \in F(\sqrt{u})$. □

Proposition V.1.16

Proposition V.1.16. If a real number c is constructible, then c is algebraic of degree a power of 2 over the field $\mathbb{Q}$ or rationals.

Proof. From the fact that every integer is constructible, along with the previous note, shows that $\mathbb{Q}$ consists of constructible numbers and so we take the plane of $\mathbb{Q}$ as given. The only way to construct new points is to find the intersection of lines and/or circles.

Proposition V.1.16

Proposition V.1.16. If a real number c is constructible, then c is algebraic of degree a power of 2 over the field $\mathbb{Q}$ or rationals.

Proof. From the fact that every integer is constructible, along with the previous note, shows that $\mathbb{Q}$ consists of constructible numbers and so we take the plane of $\mathbb{Q}$ as given. The only way to construct new points is to find the intersection of lines and/or circles. Now to construct a line or circle we need two points (the center P and radius PT for a circle). The two points must either lie in the plane of $\mathbb{Q}$ or be points previously constructed through a finite sequence of intersections of lines and/or circles.

Proposition V.1.16

Proposition V.1.16. If a real number c is constructible, then c is algebraic of degree a power of 2 over the field $\mathbb{Q}$ or rationals.

Proof. From the fact that every integer is constructible, along with the previous note, shows that $\mathbb{Q}$ consists of constructible numbers and so we take the plane of $\mathbb{Q}$ as given. The only way to construct new points is to find the intersection of lines and/or circles. Now to construct a line or circle we need two points (the center P and radius PT for a circle). The two points must either lie in the plane of $\mathbb{Q}$ or be points previously constructed through a finite sequence of intersections of lines and/or circles.

Let c be constructible. Then c results from a finite sequence of intersections of constructible lines and/or circles (starting with the plane or $\mathbb{Q}$).

Proposition V.1.16

Proposition V.1.16. If a real number c is constructible, then c is algebraic of degree a power of 2 over the field $\mathbb{Q}$ or rationals.

Proof. From the fact that every integer is constructible, along with the previous note, shows that $\mathbb{Q}$ consists of constructible numbers and so we take the plane of $\mathbb{Q}$ as given. The only way to construct new points is to find the intersection of lines and/or circles. Now to construct a line or circle we need two points (the center P and radius PT for a circle). The two points must either lie in the plane of $\mathbb{Q}$ or be points previously constructed through a finite sequence of intersections of lines and/or circles.

Let c be constructible. Then c results from a finite sequence of intersections of constructible lines and/or circles (starting with the plane or $\mathbb{Q}$). By Lemma V.1.15, the first point so constructed lies in the plane of an extension field $\mathbb{Q}(\sqrt{u})$ of $\mathbb{Q}$ with $u \in \mathbb{Q}$, or equivalently in the plane of $\mathbb{Q}(v)$ with $v^2 \in \mathbb{Q}$. Such an extension has degree 1 or degree 2 over $\mathbb{Q}$.

Proposition V.1.16

Proposition V.1.16. If a real number c is constructible, then c is algebraic of degree a power of 2 over the field $\mathbb{Q}$ or rationals.

Proof. From the fact that every integer is constructible, along with the previous note, shows that $\mathbb{Q}$ consists of constructible numbers and so we take the plane of $\mathbb{Q}$ as given. The only way to construct new points is to find the intersection of lines and/or circles. Now to construct a line or circle we need two points (the center P and radius PT for a circle). The two points must either lie in the plane of $\mathbb{Q}$ or be points previously constructed through a finite sequence of intersections of lines and/or circles.

Let c be constructible. Then c results from a finite sequence of intersections of constructible lines and/or circles (starting with the plane or $\mathbb{Q}$). By Lemma V.1.15, the first point so constructed lies in the plane of an extension field $\mathbb{Q}(\sqrt{u})$ of $\mathbb{Q}$ with $u \in \mathbb{Q}$, or equivalently in the plane of $\mathbb{Q}(v)$ with $v^2 \in \mathbb{Q}$. Such an extension has degree 1 or degree 2 over $\mathbb{Q}$.

Proposition V.1.16 (continued)

Proposition V.1.16. If a real number c is constructible, then c is algebraic of degree a power of 2 over the field $\mathbb{Q}$ or rationals.

Proof (continued). Similarly, the next new point constructed lies in the plane of $Q(v, w)$ with $w^2 \in \mathbb{Q}(v)$ (again, by Lemma V.1.15). So $(c, 0)$ lies in the plane of $F = \mathbb{Q}(v_1, v_2, \ldots, v_n)$ for some $n \in \mathbb{N}$ where $\mathbb{Q} \subset \mathbb{Q}(v_1) \subset \mathbb{Q}(v_1, v_2) \subset \cdots \subset \mathbb{Q}(v_1, v_2, \ldots, v_n)$ with $v_i^2 \in \mathbb{Q}(v_1, v_2, \ldots, v_{i-1})$ and by Lemma V.1.15, $[\mathbb{Q}(v_1, v_2, \ldots, v_i) : \mathbb{Q}(v_1, v_2, \ldots, v_{i-1})] \in \{1, 2\}$ for $2 \leq i \leq n$. By Theorem V.1.2, $[F : \mathbb{Q}]$ is the product of these dimensions and so $[F : \mathbb{Q}]$ is a power of two.

Proposition V.1.16 (continued)

Proposition V.1.16. If a real number c is constructible, then c is algebraic of degree a power of 2 over the field $\mathbb{Q}$ or rationals.

Proof (continued). Similarly, the next new point constructed lies in the plane of $Q(v, w)$ with $w^2 \in \mathbb{Q}(v)$ (again, by Lemma V.1.15). So $(c, 0)$ lies in the plane of $F = \mathbb{Q}(v_1, v_2, \ldots, v_n)$ for some $n \in \mathbb{N}$ where $\mathbb{Q} \subset \mathbb{Q}(v_1) \subset \mathbb{Q}(v_1, v_2) \subset \cdots \subset \mathbb{Q}(v_1, v_2, \ldots, v_n)$ with $v_i^2 \in \mathbb{Q}(v_1, v_2, \ldots, v_{i-1})$ and by Lemma V.1.15, $[\mathbb{Q}(v_1, v_2, \ldots, v_i) : \mathbb{Q}(v_1, v_2, \ldots, v_{i-1})] \in \{1, 2\}$ for $2 \leq i \leq n$. By Theorem V.1.2, $[F : \mathbb{Q}]$ is the product of these dimensions and so $[F : \mathbb{Q}]$ is a power of two. So by Theorem V.1.11, c is algebraic over $\mathbb{Q}$. Now (as fields) $\mathbb{Q} \subset \mathbb{Q}(c) \subset F$ and so by Theorem V.1.2, $[\mathbb{Q}(c) : \mathbb{Q}][F : \mathbb{Q}(c)] = [F : \mathbb{Q}]$ and so $[\mathbb{Q}(c) : \mathbb{Q}]$ divides $[F : \mathbb{Q}]$.

Proposition V.1.16 (continued)

Proposition V.1.16. If a real number c is constructible, then c is algebraic of degree a power of 2 over the field $\mathbb{Q}$ or rationals.

Proof (continued). Similarly, the next new point constructed lies in the plane of $Q(v, w)$ with $w^2 \in \mathbb{Q}(v)$ (again, by Lemma V.1.15). So $(c, 0)$ lies in the plane of $F = \mathbb{Q}(v_1, v_2, \ldots, v_n)$ for some $n \in \mathbb{N}$ where $\mathbb{Q} \subset \mathbb{Q}(v_1) \subset \mathbb{Q}(v_1, v_2) \subset \cdots \subset \mathbb{Q}(v_1, v_2, \ldots, v_n)$ with $v_i^2 \in \mathbb{Q}(v_1, v_2, \ldots, v_{i-1})$ and by Lemma V.1.15, $[\mathbb{Q}(v_1, v_2, \ldots, v_i) : \mathbb{Q}(v_1, v_2, \ldots, v_{i-1})] \in \{1, 2\}$ for $2 \leq i \leq n$. By Theorem V.1.2, $[F : \mathbb{Q}]$ is the product of these dimensions and so $[F : \mathbb{Q}]$ is a power of two. So by Theorem V.1.11, c is algebraic over $\mathbb{Q}$. Now (as fields) $\mathbb{Q} \subset \mathbb{Q}(c) \subset F$ and so by Theorem V.1.2, $[\mathbb{Q}(c) : \mathbb{Q}][F : \mathbb{Q}(c)] = [F : \mathbb{Q}]$ and so $[\mathbb{Q}(c) : \mathbb{Q}]$ divides $[F : \mathbb{Q}]$. So the degree $[\mathbb{Q}(c) : \mathbb{Q}]$ of c over $\mathbb{Q}$ is a power of 2. □

Proposition V.1.16 (continued)

Proposition V.1.16. If a real number c is constructible, then c is algebraic of degree a power of 2 over the field $\mathbb{Q}$ or rationals.

Proof (continued). Similarly, the next new point constructed lies in the plane of $Q(v, w)$ with $w^2 \in \mathbb{Q}(v)$ (again, by Lemma V.1.15). So $(c, 0)$ lies in the plane of $F = \mathbb{Q}(v_1, v_2, \ldots, v_n)$ for some $n \in \mathbb{N}$ where $\mathbb{Q} \subset \mathbb{Q}(v_1) \subset \mathbb{Q}(v_1, v_2) \subset \cdots \subset \mathbb{Q}(v_1, v_2, \ldots, v_n)$ with $v_i^2 \in \mathbb{Q}(v_1, v_2, \ldots, v_{i-1})$ and by Lemma V.1.15, $[\mathbb{Q}(v_1, v_2, \ldots, v_i) : \mathbb{Q}(v_1, v_2, \ldots, v_{i-1})] \in \{1, 2\}$ for $2 \leq i \leq n$. By Theorem V.1.2, $[F : \mathbb{Q}]$ is the product of these dimensions and so $[F : \mathbb{Q}]$ is a power of two. So by Theorem V.1.11, c is algebraic over $\mathbb{Q}$. Now (as fields) $\mathbb{Q} \subset \mathbb{Q}(c) \subset F$ and so by Theorem V.1.2, $[\mathbb{Q}(c) : \mathbb{Q}][F : \mathbb{Q}(c)] = [F : \mathbb{Q}]$ and so $[\mathbb{Q}(c) : \mathbb{Q}]$ divides $[F : \mathbb{Q}]$. So the degree $[\mathbb{Q}(c) : \mathbb{Q}]$ of c over $\mathbb{Q}$ is a power of 2. □

Corollary V.1.17

Corollary V.1.17. Straight Edge and Compass Trisection of a General Angle is Impossible.
An angle of 60° cannot be trisected by ruler and compass constructions, and therefore a general angle cannot be trisected.

Proof. If it were possible to trisect a 60° angle, we would then be able to construct a right triangle with one acute angle of 20°.

Corollary V.1.17

Corollary V.1.17. Straight Edge and Compass Trisection of a General Angle is Impossible.
An angle of 60° cannot be trisected by ruler and compass constructions, and therefore a general angle cannot be trisected.

Proof. If it were possible to trisect a 60° angle, we would then be able to construct a right triangle with one acute angle of 20°. It would then be possible to construct the real number $\cos(20^\circ)$ (see Exercise V.1.25(b) or the the Lemma to Theorem 32.11 in my YouTube video online at `https://www.youtube.com/watch?v=S24GYj1rWGs`, accessed 12/20/2015).

Corollary V.1.17

Corollary V.1.17. Straight Edge and Compass Trisection of a General Angle is Impossible.
An angle of 60° cannot be trisected by ruler and compass constructions, and therefore a general angle cannot be trisected.

Proof. If it were possible to trisect a 60° angle, we would then be able to construct a right triangle with one acute angle of 20°. It would then be possible to construct the real number $\cos(20^\circ)$ (see Exercise V.1.25(b) or the the Lemma to Theorem 32.11 in my YouTube video online at `https://www.youtube.com/watch?v=S24GYj1rWGs`, accessed 12/20/2015). However for any angle α, elementary trigonometric shows that $\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha)$. With $\alpha = 20^\circ$, then $\cos(3\alpha) = \cos(60^\circ) = 1/2$ and $\cos(20^\circ)$ is a root of the polynomial equation $1/2 = 4x^3 - 3x$ or equivalently $8x^3 - 6x - 1 = 0$.

Corollary V.1.17

Corollary V.1.17. Straight Edge and Compass Trisection of a General Angle is Impossible.
An angle of 60° cannot be trisected by ruler and compass constructions, and therefore a general angle cannot be trisected.

Proof. If it were possible to trisect a 60° angle, we would then be able to construct a right triangle with one acute angle of 20°. It would then be possible to construct the real number $\cos(20^\circ)$ (see Exercise V.1.25(b) or the the Lemma to Theorem 32.11 in my YouTube video online at `https://www.youtube.com/watch?v=S24GYj1rWGs`, accessed 12/20/2015). However for any angle α, elementary trigonometric shows that $\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha)$. With $\alpha = 20^\circ$, then $\cos(3\alpha) = \cos(60^\circ) = 1/2$ and $\cos(20^\circ)$ is a root of the polynomial equation $1/2 = 4x^3 - 3x$ or equivalently $8x^3 - 6x - 1 = 0$.

Corollary V.1.17

Corollary V.1.17. Straight Edge and Compass Trisection of a General Angle is Impossible.
An angle of 60° cannot be trisected by ruler and compass constructions, and therefore a general angle cannot be trisected.

Proof. But $8x^3 - 6x - 1$ is irreducible in $\mathbb{Q}[x]$ by Proposition III.6.8 and the Factor Theorem (Theorem III.6.6). Therefore, $\cos(20^\circ)$ has degree 3 over $\mathbb{Q}$ and so $\cos(20^\circ)$ is not constructible by Proposition V.1.16, and whence a 20° angle is not constructible. □

Corollary V.1.17

Corollary V.1.17. Straight Edge and Compass Trisection of a General Angle is Impossible.
An angle of 60° cannot be trisected by ruler and compass constructions, and therefore a general angle cannot be trisected.

Proof. But $8x^3 - 6x - 1$ is irreducible in $\mathbb{Q}[x]$ by Proposition III.6.8 and the Factor Theorem (Theorem III.6.6). Therefore, $\cos(20^\circ)$ has degree 3 over $\mathbb{Q}$ and so $\cos(20^\circ)$ is not constructible by Proposition V.1.16, and whence a 20° angle is not constructible. □

Corollary V.1.18

Corollary V.1.18. Straight Edge and Compass Doubling of the Cube is Impossible.
It is impossible by ruler and compass constructions to duplicate a cube of side length 1 (that is, to construct the side of a cube of volume 2).

Proof. If s is the side length of a cube of volume 2, then s is a root of $x^3 - 2$ which is irreducible in $\mathbb{Q}[x]$ by Eisentein's Criterion (Theorem III.6.15).

Corollary V.1.18

Corollary V.1.18. Straight Edge and Compass Doubling of the Cube is Impossible.
It is impossible by ruler and compass constructions to duplicate a cube of side length 1 (that is, to construct the side of a cube of volume 2).

Proof. If s is the side length of a cube of volume 2, then s is a root of $x^3 - 2$ which is irreducible in $\mathbb{Q}[x]$ by Eisentein's Criterion (Theorem III.6.15). Therefore x is not constructible by Proposition V.1.16 since $\sqrt[3]{2}$ is of degree 3 over $\mathbb{Q}$. □

Corollary V.1.18

Corollary V.1.18. Straight Edge and Compass Doubling of the Cube is Impossible.
It is impossible by ruler and compass constructions to duplicate a cube of side length 1 (that is, to construct the side of a cube of volume 2).

Proof. If s is the side length of a cube of volume 2, then s is a root of $x^3 - 2$ which is irreducible in $\mathbb{Q}[x]$ by Eisentein's Criterion (Theorem III.6.15). Therefore x is not constructible by Proposition V.1.16 since $\sqrt[3]{2}$ is of degree 3 over $\mathbb{Q}$. □

Corollary V.1.19

Corollary V.1.19. Straight Edge and Compass Squaring of the Circle is Impossible.
It is impossible by ruler and compass constructions to construct a square with area equal to the area of a circle of radius 1 (that is, to construct a square with area π).

Proof. Consider a circle of radius 1, and so area π.

Corollary V.1.19

Corollary V.1.19. Straight Edge and Compass Squaring of the Circle is Impossible.
It is impossible by ruler and compass constructions to construct a square with area equal to the area of a circle of radius 1 (that is, to construct a square with area π).

Proof. Consider a circle of radius 1, and so area π. ASSUME a square of area π can be constructed. Then the length of a side of the square is $\sqrt{\pi}$ and this is a constructible number. Then π is constructible and so by Proposition V.1.16, π is algebraic over $\mathbb{Q}$.

Corollary V.1.19

Corollary V.1.19. Straight Edge and Compass Squaring of the Circle is Impossible.
It is impossible by ruler and compass constructions to construct a square with area equal to the area of a circle of radius 1 (that is, to construct a square with area π).

Proof. Consider a circle of radius 1, and so area π. ASSUME a square of area π can be constructed. Then the length of a side of the square is $\sqrt{\pi}$ and this is a constructible number. Then π is constructible and so by Proposition V.1.16, π is algebraic over $\mathbb{Q}$. But π is known to be transcendental by Lindemann's proof, a CONTRADICTION. So no such square is constructible. □

Corollary V.1.19

Corollary V.1.19. Straight Edge and Compass Squaring of the Circle is Impossible.
It is impossible by ruler and compass constructions to construct a square with area equal to the area of a circle of radius 1 (that is, to construct a square with area π).

Proof. Consider a circle of radius 1, and so area π. ASSUME a square of area π can be constructed. Then the length of a side of the square is $\sqrt{\pi}$ and this is a constructible number. Then π is constructible and so by Proposition V.1.16, π is algebraic over $\mathbb{Q}$. But π is known to be transcendental by Lindemann's proof, a CONTRADICTION. So no such square is constructible. □