GRV, facts about field extensions.

1. Let F be a field and let $\alpha \in K$ where K is a field extension of F (field extension means: F and K are fields, and $F \subseteq K$).
   The following conditions are equivalent, and we say that α is *algebraic over* F when these equivalent conditions hold:

   (a) There is a nonzero polynomial $f(x) \in F[x]$ for which $f(\alpha) = 0$.

   (b) There is an irreducible polynomial $f(x) \in F[x]$ for which $f(\alpha) = 0$.

   Notation: this polynomial is denoted as $m_{\alpha,F}(x)$. It is the monic polynomial $f(x) \in F[x]$ of minimal degree for which $f(\alpha) = 0$.

   (c) $F[\alpha] = F(\alpha)$.

   (d) $F[\alpha]$ is a field.

   (e) $[F(\alpha) : F]$ is finite.

   Definition: $[F(\alpha) : F]$ is the dimension of $F(\alpha)$ as a vector space over F. If this dimension $n = [F(\alpha) : F]$ is finite (if α is algebraic) then $n = \text{degree}(m_{\alpha,F}(x))$. We can use the minimal polynomial $m_{\alpha,F}(x)$ to write $\alpha^n, \alpha^{n+1}, \ldots$ as F-linear combinations of $1, \alpha, \ldots, \alpha^{n-1}$. So $1, \alpha, \ldots, \alpha^{n-1}$ will be a basis of $F[\alpha] = F(\alpha)$ as an F-vector space. Another important fact is:

   $$F(\alpha) \cong F[x]/(m_{\alpha,F}(x)) \tag{1}$$

2. Given a field F and an element $\alpha \in K$ where K is a field extension of F, how do we find, if it exists, a nonzero polynomial $f \in F[x]$ for which $f(\alpha) = 0$?
   Answer: Compute $1, \alpha, \alpha^2, \ldots$ and try to find a linear relation. If $\sum a_i \alpha^i = 0$ then $f(x) = \sum a_i x^i$.
   For example, suppose that $\alpha = a + b$ where a is a solution of $x^2 + x + 1 = 0$ (i.e. $a^2 = -a - 1$) and $b = 2^{1/3}$ (i.e. b is a solution of $x^3 - 2$, so $b^3 = 2$). Lets take $F = \mathbb{Q}$. Looking at powers of a, you see that $a^2, a^3, \ldots$ can be simplified to $\mathbb{Q}$-linear combinations of $1, a$. Likewise, $b^3, b^4, \ldots$ can be simplified to $\mathbb{Q}$-linear combinations of $1, b, b^2$. Therefore, any product of the form $a^k b^l$ can be simplified to a $\mathbb{Q}$-linear combination of these six numbers: $B = \{a^i b^j \mid i \in \{0, 1\},\ j \in \{0, 1, 2\}\}$. So if we think of $\mathbb{Q}[a, b]$ (same as $\mathbb{Q}(a, b)$, use item 1c twice) as a $\mathbb{Q}$-vector space then B is a basis. Then you compute $1, \alpha, \alpha^2, \ldots$ and if you expand these then you get combinations of $a^k b^l$. When you simplify those, you get linear combinations of the elements of B. But since B has only 6 elements, the moment you write down 7 linear combinations of elements of B, you must get a linear dependence. Hence, $1, \alpha, \ldots, \alpha^6$ must be linearly dependent over $\mathbb{Q}$. So we use linear algebra (find linear equations for the a_i and then solve them) to find such a linear relation $\sum_{i=0}^{n} a_i \alpha^i = 0$ (in this example $n = 6$ suffices). Then we can take $p(x) = \sum_{i=0}^{n} a_i x^i$.
   In this example, we find $p(x) = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9$.

3. Given a field F and an element $\alpha \in K$ where K is a field extension of F how do we find, if it exists, the minimal polynomial $m_{\alpha,F}(x)$.
Answer: Same as in item 2, except that we have to make sure that the n in the linear relation $\sum_{i=0}^{n} a_i \alpha^i = 0$ is as small as we can make it. In the example in item 2, for $m_{\alpha,\mathbb{Q}}$ we find the same polynomial $p(x)$. In general, for computing a minpoly we do have to be more careful than we need to be in item 2. Take for instance $\beta = ab$ where a, b are as in item 2. The same reasoning shows that $\beta^0, \ldots, \beta^6$ must be linearly dependent; after all, these seven numbers $\beta^0, \ldots, \beta^6$ are linear combinations of B, and B has only six elements. However, for finding a linear relation between $\beta^0, \beta^1, \ldots$, the number 6 is not minimal, because in fact $\beta^0, \ldots, \beta^3$ are already linearly dependent over $\mathbb{Q}$. The minpoly for β is $x^3 - 2$ (you can see this when you realize that $a^3 = 1$).
Since β has the same minpoly over $\mathbb{Q}$ as the number b, we get from the formula (1) above that both $\mathbb{Q}(\beta)$ and $\mathbb{Q}(b)$ are isomorphic to $\mathbb{Q}[x]/(x^3-2)$. Therefore these two fields must also be isomorphic to each other: $\mathbb{Q}(\beta) \cong \mathbb{Q}(b)$ despite the fact that the two fields are not equal (one of them is a subfield of $\mathbb{R}$ while the other is not).

   As another example, lets compute a polynomial for the same $\alpha = a + b$ as in item 2, but this time $F = \mathbb{Q}(a)$. If we do not care about minimality, then we can give the same polynomial as in item 2. However, if we look for a polynomial of minimal degree, then we can use this larger field F to give a lower degree polynomial. We can show that $x^3 - 2$ is still irreducible over F using equation (2) in item 5c below. Hence it must be the minpoly of b over F. But then $(x - a)^3 - 2 \in F[x]$ must also be irreducible since it is simply a shift of $x^3 - 2$, and since this polynomial has α as a solution, it will be the minpoly of α over F.

4. Let K be a field extension of F. Definitions

   (a) K is *finite* over F when $[K : F]$ is finite.

   (b) K is *algebraic* over F when every $\alpha \in K$ is algebraic over F.

   (c) K is *finitely generated* over F if there exist finitely many $\alpha_1, \ldots, \alpha_n \in K$ for which $K = F(\alpha_1, \ldots, \alpha_n)$.

5. Let $F \subseteq K \subseteq L$ be fields.
Notation: K/F does **not** mean K modulo F or something like it. When we write K/F that means that we are looking at the extension $F \subseteq K$.

   (a) K/F is finite $\Longleftrightarrow$ K/F is algebraic *and* finitely generated.

   (b) L/F is algebraic $\Longleftrightarrow$ both L/K and K/F are algebraic.

   (c) L/F is finite $\Longleftrightarrow$ both L/K and K/F are finite.

      This says that $[L : F]$ is finite iff both $[L : K]$ and $[K : F]$ are finite. In fact, we can say even more than that, namely the following:
If B_1 is a basis of L as a K-vector space, and if B_2 is a basis of

K as an F-vector space, then we get a basis of L as an F-vector space by multiplying every element of B_1 by every element of B_2. In particular, this means that

$$[L : F] = [L : K] \cdot [K : F]. \tag{2}$$

This formula implies the impossibility of trisecting an angle with ruler and compass constructions because, starting with points with rational x and y coefficients, the coefficients of the points we can encounter with n ruler/compass constructions are elements of a tower of n field extensions $\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n$ where $[F_{i+1} : F_i]$ is always either one or two (computing the coordinates of a point in one ruler/compass construction involves solving an equation of degree either 1 or 2). But trisections can produce a point with an x-coordinate such as $\alpha = \cos(2\pi/9)$. Now $[F_n : \mathbb{Q}]$ is a power of 2 so it is not divisible by $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Then equation (2) shows that $\mathbb{Q}(\alpha)$ can not be a subfield of F_n, which implies that $\alpha \notin F_n$. Hence α is not constructible with n ruler/compass constructions, for any n.

6. Let K_1, K_2 be intermediate fields of K/F (so $F \subseteq K_i \subseteq K$ for $i = 1, 2$). Notation: K_1K_2 is the smallest subfield of K that contains K_1 and K_2. Then

$$[K_1K_2 : F] \leq [K_1 : F] \cdot [K_2 : F] \tag{3}$$

Proof: Assume $n = [K_1 : F]$ and $m = [K_2 : F]$ are finite. Let $b_1, \ldots, b_n$ be a basis of K_1 as F-vector space, and $c_1, \ldots, c_m$ be a basis of K_2 as F-vector space. Then $S = \{b_ic_j \,|\, i \in \{1, \ldots, n\},\, j \in \{1, \ldots, m\}\,\}$ is a *spanning set* for K_1K_2 with nm elements. Now $[K_1K_2 : F]$ is the number of elements of a basis, and this is always $\leq$ to the number of elements of a spanning set.
Note: if S is linearly independent, then the $\leq$ becomes an equality. But S might be dependent (e.g. when $K_1 \bigcap K_2 \neq F$).

7. If α and β are algebraic over F then so are $\alpha + \beta, \alpha - \beta, \alpha\beta$, as well as α/β if $\beta \neq 0$.
In particular, if you take the subset $S \subseteq K$ of all elements of K that are algebraic over F, then this set S is closed under $+, -, \cdot, /$ and hence this S is a field. This S is called the *algebraic closure of F in K*, it is the largest subfield of K that is still algebraic over F.

Note: the example in item 2 explains computationally why $\alpha + \beta$ should be algebraic over F when α, β are algebraic over F.

8. A field K is called *algebraically closed* when the following equivalent conditions hold:

   (a) Every non-constant polynomial $f \in K[x]$ has at least one root in K.

   (b) Every non-constant polynomial $f \in K[x]$ splits over K (meaning: can be written as a product of linear factors with coefficients in K).

   (c) Whenever $K \subseteq L$ is an algebraic extension we have $K = L$.

9. An *algebraic closure* of F is a field, lets denote it as $\overline{F}$, with the following properties:

   (a) $\overline{F}$ is an algebraic extension of F, and

   (b) $\overline{F}$ is algebraically closed

   For any field F we can prove (if you accept the axiom of choice) that an algebraic closure exists, and that it is unique up to isomorphism, so we can call it *the* algebraic closure. We can think of $\overline{F}$ as "the largest field that is algebraic over F". But we can also describe $\overline{F}$ as "the smallest algebraically closed field that contains F".

   Note: If $F \subseteq K$ then these two fields

   (a1) The algebraic closure of F, and

   (a2) The algebraic closure of F in K

   are not the same, because (a1) is the largest algebraic extension of F that can be found anywhere, whereas (a2) is the largest algebraic extension of F that can be found inside of K. The two field (a1),(a2) are the same if and only if every non-constant polynomial in $F[x]$ splits over K.
   For instance, $\overline{\mathbb{Q}}$ is not the same as the algebraic closure of $\mathbb{Q}$ in $\mathbb{R}$, but it is the same as (isomorphic to) the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

10. A field $\overline{F}$ is the algebraic closure of F when it satisfies these two properties:

    (a) $\overline{F}$ is an algebraic extension of F, and

    (b) Every non-constant polynomial in $F[x]$ splits in $\overline{F}[x]$.

    Note: condition (10b) appears to be weaker than condition (9b), which says that every non-constant polynomial in $\overline{F}[x]$ splits in $\overline{F}[x]$. However, it turns out that, if we assume condition (9a), then the two conditions (9b) and (10b) become equivalent.

11. (you don't really need to know this). Construction of $\overline{F}$. Let S be the set of all monic irreducible polynomials in $F[x]$. For each polynomial $f_n \in S$, if the degree is d then introduce d new variables, say $u_{n,1}, \ldots, u_{n,d}$, and compute $f - (x - u_{n,1}) \cdots (x - u_{n,d})$ and write it as $\sum_{k=0}^{d-1} v_{n,k} x^k$ for some polynomials $v_{n,k} \in F[u_{n,1}, \ldots, u_{n,d}]$. For instance, $v_{n,0}$ is the constant term of f_n minus the product of the $-u_{n,i}$, $i = 1, \ldots, d$. Now let R be

the polynomial ring over F generated by all these variables $v_{n,i}$ (for all $f_n \in S$ and all $i = 1, \ldots, \text{degree}(f_n)$). Let I be the ideal in R generated by all these polynomials $v_{n,k}$. Then we can embed $F \subseteq R/I$, and every irreducible polynomial $f_n \in F[x]$ will split in the ring $(R/I)[x]$. Problem is, this ring R/I will not be a field. To fix this, let M be a maximal ideal that contains I (to prove that such M exists, we need Zorn's lemma, which is equivalent to the Axiom of Choice). Then again every polynomial in $F[x]$ splits over R/M, but this time R/M is a field. It is generated over F by the $u_{n,i} + M$. Although there are infinitely many generators, they are all algebraic over F (by construction, $x - (u_{n,i} + M)$ is a linear factor of $f_n(x)$ and so $u_{n+i}+M$ is a root of $f(x)$) and that makes R/M an algebraic extension of F. Then R/M is the algebraic closure by item 10.
Take for example $F = \mathbb{Q}$, and $S = \{f_1, f_2 \ldots\}$ is the set of all irreducible polynomials in $\mathbb{Q}[x]$. For instance, $f_1 = x^2+2x+6$, $f_2 = x^2+1$, $f_3 = x^3-2$, etc. Now $f_1 - (x-u_{1,1})(x-u_{1,2}) = x^0 \cdot (6-u_{1,1}u_{1,2}) + x^1 \cdot (2+u_{1,1}+u_{1,2})$ and repeating this for every other irreducible polynomial $f_2, f_3, \ldots$ we get $R/I = \mathbb{Q}[u_{1,1}, u_{1,2}, u_{2,1}, \ldots]/(6 - u_{1,1}u_{1,2},\ 2 + u_{1,1} + u_{1,2},\ \ldots)$. Looking at I it is clear that in the ring $(R/I)[x]$ we can write f_1 as a product of linear factors $f_1 = (x - (u_{1,1} + I))(x - (u_{1,2} + I))$, and the same is true for $f_2, f_3, \ldots$ etc. If $I \subseteq M$ then we can do the same in $(R/M)[x]$.

12. If $f \in F[x]$ is a non-constant polynomial then a field K is called a *splitting field* for f over F if

    (a) $F \subseteq K$

    (b) f splits into linear factors over K

    (c) If $F \subseteq K' \subsetneq K$ then f does not split into linear factors over K'.

    We get an equivalent definition if we replace (c) by:

    (c') $K = F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the roots of f in K.

    Given two splitting fields of f over F, we can prove them to be isomorphic, and so we can call it *the* splitting field of f over F. We can think of the splitting field as the smallest extension of F over which f splits, that is, the smallest field that contains both F and all roots of f. Looking at (c') we see that the splitting field of f over F is an algebraic extension of F.

13. If S is a set of non-constant polynomials in $F[x]$, then the splitting field of S over F is the smallest algebraic extension of F over which every $f \in S$ splits into linear factors (such a field must exist, see item 11).

    As an example, the splitting field of $S = \{x^2 - 2, x^2 - 3, x^2 - 5, x^2 - 7, \ldots\}$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots)$.

14. A field extension $F \subseteq K$ is called a *normal extension* if the following two equivalent conditions hold:

    (a) there is some set of polynomials $S \subseteq F[x]$ such that K is the splitting field of S over F.

    (b) K/F is algebraic, and for every irreducible polynomial $f(x) \in F[x]$ we have the following

    $$f(x) \text{ has a root in } K \iff f(x) \text{ splits over } K.$$

    In other words: if f is irreducible in $F[x]$, and if K contains at least one root of f, then it has to contain every root of f! That's a rather strong condition, and this makes it easy to give an example of an extension that is algebraic but not normal: $\mathbb{Q} \subseteq \mathbb{Q}(2^{1/3})$ is not normal since it contains one root (but not every root) of the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$.
    However, using condition (a) we can also easily give examples of extensions that are normal, just take the splitting field of some polynomial. For instance the field $\mathbb{Q}(a, b)$ in item 2 is the splitting field of a polynomial over $\mathbb{Q}$, namely $x^3 - 2$ which factors as $(x-b)(x-ab)(x-a^2b)$. Hence this $\mathbb{Q}(a, b)$ is a normal extension of $\mathbb{Q}$.

15. If K is the splitting field of $f(x)$ over F then $[K : F] \leq n!$ where n is the degree of $f(x)$.

    To see this, let $\alpha \in$ be a root of $f(x)$ and let $d = [F(\alpha) : F]$. Since $f(\alpha) = 0$ and $f(x) \in F[x]$ it follows the minpoly of α over F must divide $f(x)$. Hence, d, the degree of this minpoly, is at most n. Now let $g(x) = f(x)/(x - \alpha) \in F(\alpha)[x]$. It has degree $n - 1$ and so by induction, the splitting field of $g(x)$ over $F(\alpha)$ has degree at most $(n-1)!$ over $F(\alpha)$. But this splitting field is just K, so we get $[K : F(\alpha)] \leq (n-1)!$. Then $[K : F] = [K : F(\alpha)] \cdot [F(\alpha) : F] \leq (n-1)! \cdot d \leq n!$.

    Note that if the $\leq n!$ is an equality then d will have to be equal to n, in other words, $f(x)$ is irreducible over F. Furthermore, $g(x)$ will have to be irreducible over $F(\alpha)$ (otherwise the $\leq (n-1)!$ won't be an equality) etc.

16. A polynomial $f \in F[x] - F$ is called *square-free in* $F[x]$ if there does not exist a polynomial $g \in F[x] - F$ such that g^2 divides f. It is clear that:

    $$f \text{ irreducible in } F[x] \Longrightarrow f \text{ is square-free in } F[x]$$

17. Let K be a splitting field of f. A polynomial $f \in F[x] - F$ is called *separable* if the following equivalent conditions hold:

    (a) The number of distinct roots of f in the splitting K equals the degree.

    (b) f has no multiple roots (roots with multiplicity > 1) in the splitting field K.

(c) The gcd of f and the derivative f' is a constant (it does not matter if you compute this in $F[x]$ or in $K[x]$, the result of the gcd computation is the same).

(d) f is square-free in $K[x]$
(note: This condition is stronger than the condition that f is square-free in $F[x]$ because K is a bigger field).

18. **If** the characteristic of F is 0, **or if** F is a finite field, then the following is true for any $f \in F[x]$

$$f \text{ is square-free in } F[x] \Longleftrightarrow f \text{ is separable.}$$

Remarks: In general "separable" is stronger than "square-free in $F[x]$" because separable means not only square-free in $F[x]$ but also means "square-free in $K[x]$ for any field extension K of F". For example, if $F = \mathbb{F}_p(t)$ then you can find a polynomial $f = x^p - t \in F[x]$ that is square-free and even irreducible in $F[x]$ but not separable. The splitting field is $K = \mathbb{F}_p(\sqrt[p]{t})$ and in $K[x]$ we find $f = (x - \sqrt[p]{t})^p$. So f is square-free in $F[x]$ but is not separable because f is not square-free in $K[x]$.

19. **If** the characteristic of F is 0, **or if** F is a finite field, and if K is an extension of F then the following are equivalent

(a) K is a normal extension of F (this was defined in item 14a)

(b) K is the splitting field of some set of *separable* polynomials in $F[x]$.

Proof: Take the set S from item 14a. For each polynomial $f \in S \subseteq F[x]$, we can make it square-free as follows: as long as g^2 divides f for some $g \in F[x]$, replace f by f/g. Then f/g and f have the same roots, so the splitting fields do not change. We can repeat this until all the f's in S have become square-free. Then by item 18 these f's are also separable.
Note: The assumption made on F is relevant, without it we get counter examples such as $F = \mathbb{F}_p(t), \;\; S = \{x^p - t\}$.

20. Definition: $\mathrm{Aut}(K)$ is the group of all automorphisms of K.

21. Definition: An automorphism of K/F (automorphism of K over F) is an automorphism $\sigma : K \to K$ that acts trivially on F (i.e. $\sigma(a) = a$ for all $a \in F$).
Definition: $\mathrm{Aut}(K/F)$ is the group of all automorphisms of K over F.

22. Some easy things to note: $\mathrm{Aut}(K/F) \leq \mathrm{Aut}(K)$, i.e. $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$. Also:

$$F_1 \subseteq F_2 \Longrightarrow \mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$$

Finally, if $\mathbb{Q} \subseteq K$ and $\sigma \in \mathrm{Aut}(K)$, then σ acts trivially on 1 (i.e. $\sigma(1) = 1$) and so σ must also act trivially on the subfield of K that is generated by 1, i.e. σ acts trivially on $\mathbb{Q}$. Hence, $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$. So we find

$$\mathrm{Aut}(K/\mathbb{Q}) = \mathrm{Aut}(K).$$

Another trivial remark is that

$$\mathrm{Aut}(K/K) = \{1\}.$$

23. Let K/F be a finite extension and let $|\mathrm{Aut}(K/F)|$ denote the order, the number of elements, of the group $\mathrm{Aut}(K/F)$. The following is always true:

$$|\mathrm{Aut}(K/F)| \leq [K : F] \tag{4}$$

Moreover, the following are equivalent

(a) $\mathrm{Aut}(K/F)$ has $[K : F]$ elements

(b) K is the splitting field of some separable polynomial in $F[x]$

24. Definition: Let K/F be a finite extension. Then K/F is called a Galois extension if item 23a (and hence item 23b) is true. In this case, we denote $\mathrm{Aut}(K/F)$ as $\mathrm{Gal}(K/F)$ and call this the Galois group.

25. In this item we assume that either $\mathrm{char}(F) = 0$, or F is a finite field. We also assume that $[K : F] < \infty$. Then using item 19 you see that you may ignore the word "separable" in item 23b, so then we get

$$K/F \text{ Galois} \Longleftrightarrow K/F \text{ normal.}$$

Recall from item 14b that this is equivalent to a rather intriguing property, namely that every irreducible $f(x) \in F[x]$ that has at least one root in K has *all* of its roots in K. The explanation for this property is the following: If $f(x) \in F[x]$ has a root $\alpha \in K$, and if σ is an automorphism of K over F, then $\sigma(\alpha)$ is again a root of $f(x)$ in K. Now a Galois extension is by definition an extension that has as many as possible (namely $[K : F]$) automorphisms. Applying all these automorphisms to that one root α, we find all the roots of the minpoly of α over F. If $f(x)$ is irreducible, then that means that we get all roots of $f(x)$.

26. We have to prove item 23. First, we have to prove formula (4) and then we have to show that we get an equality in formula (4) if and only if K is the splitting field of some separable polynomial over F.
Let $N := [K : F]$ and let $G = \mathrm{Aut}(K/F)$. By using induction, we may assume that everything in item 23 is true for any field extension of degree smaller than N. Now suppose that $K \neq F$ and take some element $\alpha \in K$, $\alpha \notin F$. Let $d = [F(\alpha) : F] > 1$ and so $[K : F(\alpha)] = N/d$. Since $N/d < N$ we may by induction assume that everything in item 23 is true for the field extension $F(\alpha) \subseteq K$.
Now G acts on K. Let G_α be the stabilizer of α, and let O_α be the orbit of α under G. Remember from group theory that the stabilizer G_α is the group $\{g \in G | g(\alpha) = \alpha\}$, that O_α is the set $\{g(\alpha) | g \in G\}$. Group theory tells us that

$$|G| = |G_\alpha| \cdot |O_\alpha|$$

Now $G_\alpha = \mathrm{Aut}(K/F(\alpha))$ so by induction we get that $|G_\alpha| \leq [K : F(\alpha)]$, with equality if and only if K is the splitting field over $F(\alpha)$ of some separable polynomial in $F(\alpha)[x]$.
Let $m(x)$ be the minpoly of α over F. If $g \in G$ then g acts trivially on F and so $g(m(x)) = m(x)$. Then $0 = g(0) = g(m(\alpha)) = m(g(\alpha))$ so we see that every element of O_α is a root of $m(x)$. Hence, $|O_\alpha| \leq \deg(m(x))$. Then we find

$$|G| = |G_\alpha| \cdot |O_\alpha| \leq [K : F(\alpha)] \cdot \deg(m(x)) = [K : F(\alpha)] \cdot [F(\alpha) : F] = N$$

so we have now proved formula (4).

We now have to show that if we get an equality, then K has to be a splitting field. But the only way we can get $|G| = N$ in the last formula is when $|O_\alpha| = \deg(m(x))$. But every element of O_α is a root of $m(x)$, so inside O_α (which is a subset of K) we can already find $\deg(m(x))$ roots. Therefore $m(x)$ splits in K. Moreover, $m(x)$ also has to be separable (otherwise we it is impossible to find $\deg(m(x))$ roots in any field, let alone K). If K is the splitting field of $m(x)$ then we are done; otherwise write $K = F(\alpha_1, \ldots, \alpha_r)$ for some $\alpha_i \in K$ (note: K/F is finite implies K/F is finitely generated). Let $m_{\alpha_i}(x)$ be the minpoly of α_i over F. Just like we saw that $m(x)$ is separable and splits over K, the same argument shows that $m_{\alpha_i}(x)$ splits over K as well (and is again separable). Then take $f(x)$ as the least common multiple of the polynomials $m_{\alpha_1}(x), \ldots, m_{\alpha_r}(x)$. Again, this polynomial is separable and splits over K because each of the m_{α_i} is separable and splits over K. But this time, the splitting field of $f(x)$ is K.

We have shown that $G = \mathrm{Aut}(K/F)$ has at most $[K : F]$ elements, and that if it has exactly $[K : F]$ elements then K has to be the splitting field of some separable polynomial $f(x) \in F[x]$. Remains to show that if K is the splitting field of some separable polynomial $f(x)$, that then G has precisely $[K : F]$ elements. Again, lets do this by induction. If $f(x)$ splits over F then we're done, otherwise, let $m(x)$ be an irreducible factor of $f(x)$ in $F[x]$ of degree $d > 1$. Let $\alpha_1, \ldots, \alpha_d$ be the roots of $m(x)$ in K. Then each of the fields $F(\alpha_i)$ is isomorphic to $F[x]/(m(x))$ and hence each of these fields is isomorphic to $F(\alpha_1)$. So we have an isomorphism $\sigma_i' : F(\alpha_1) \to F(\alpha_i)$ and, following the proof of Theorem 27 in section 13.4, we see that this σ_i' can be extended to an isomorphism $\sigma_i : K \to K$, so $\sigma_i \in \mathrm{Aut}(K/F)$ (what is denoted as $F, F', E, E', \sigma', \sigma, \alpha, \beta$ in the proof of Theorem 27 is in our setting denoted as $F, F, K, K, \sigma_i', \sigma_i, \alpha_1, \alpha_i$).
Since $\{\sigma_1, \ldots, \sigma_d\}$ is a subset (not necessarily a subgroup) of G, it follows that $\{\sigma_1(\alpha_1), \ldots, \sigma_d(\alpha_1)\} = \{\alpha_1, \ldots, \alpha_d\}$ is a subset of O_{α_1}, the orbit of α_1 under G. Hence, O_{α_1} has at least d elements. Then it has precisely d elements because every element of O_{α_1} has to be a root of $m(x)$, the minpoly of α_1. Now G_{α_1}, the stabilizer of α_1, is the same as $\mathrm{Aut}(K/F(\alpha_1))$ and by induction this group has precisely $[K : F(\alpha_1)]$ elements (to use induction, note that K is the splitting field of $f(x)$ over $F(\alpha_1)$ and note

that this extension $K/F(\alpha_1)$ is an extension of lower degree than the extension K/F). Then $|G| = |G_{\alpha_1}| \cdot |O_{\alpha_1}| = [K : F(\alpha_1)] \cdot d = [K : F]$.

27. Let H be a subgroup of $\mathrm{Aut}(K)$. We define the *fixed field of* H as

$$K^H := \{a \in K \mid \sigma(a) = a \text{ for all } \sigma \in H\}.$$

Note that "the smaller the group H is, the bigger the field K^H will be", specifically, if you take the smallest group $H = \{1\}$ then the fixed field of H is just K itself.

28. Let K be any field, and let H be any finite subgroup of $\mathrm{Aut}(K)$. Since H acts trivially on K^H, it is clear that $H \leq \mathrm{Aut}(K/K^H)$, but in fact we can say much more, namely:

$$H = \mathrm{Aut}(K/K^H) \tag{5}$$

and

$$|H| = [K : K^H] \tag{6}$$

Note: combining the above two equations with the definition in item 24 shows that K/K^H is Galois.

Proof: Let $n = |H|$ and $N = [K : K^H]$. Now

$$n = |H| \leq |\mathrm{Aut}(K/K^H)| \leq N \tag{7}$$

where the first $\leq$ is because $H \leq \mathrm{Aut}(K/K^H)$ and the second $\leq$ comes from formula (4). Remains to show: $N \leq n$. Once we've shown this, then both $\leq$ in (7) become an equality, and then both equations (5),(6) follow.

Assume that $N > n$ (remains to prove: a contradiction). Denote $F := K^H$ and with $[K : F] = N > n$ we can then find at least $n + 1$ F-linearly independent elements $\alpha_1, \ldots, \alpha_{n+1}$ in K. Let $H = \{\sigma_1, \ldots, \sigma_n\}$, where σ_1 is the identity, and make an n by $n + 1$ matrix A in which the i'th row is equal to $\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_{n+1})$. Notice that if $\sigma \in H$ then $\sigma(A)$ is just A with some rows interchanged. Therefore, A and $\sigma(A)$ will have the same reduced row echelon form, lets call this matrix $\mathrm{rref}(A) = R$. Then $\sigma(R) = \mathrm{rref}(\sigma(A)) = R$ and so R is invariant under H, and hence R is an n by $n+1$ matrix with entries in $F = K^H$. Now let $(c_1, \ldots, c_{n+1}) \in F^{n+1}$ be a non-zero vector in the Nullspace of R. Then this is also in the Nullspace of A (a matrix A has the same Nullspace as its reduced row echelon form). Now multiply the first row of A by this vector $(c_1, \ldots, c_{n+1})$ and we get a linear relation $c_1\alpha_1 + \cdots + c_{n+1}\alpha_{n+1} = 0$ which contradicts that $\alpha_1, \ldots, \alpha_{n+1}$ are linearly independent over F.

29. The book gives a different proof of formula (4), I will sketch it here. First, there is a useful fact that is true in general: "automorphisms of K are linearly independent over K" (Cor. 8 in section 14.2). Now let $\sigma_1, \ldots, \sigma_n$ be elements of $\mathrm{Aut}(K/F)$. Then they are also F-linear maps from K to

K, so they are elements of $V := \mathrm{Hom}_F(K,K)$. Now V is an F-vector space of dimension N^2 where $N := [K : F]$. If you have an F-linear map $\phi : K \to K$ and if $a \in K$ then $a\phi$ is also an F-linear map from K to K. In other words, $a\phi \in V$ for every $a \in K$ and $\phi \in V$, or, as mathematicians would say: V is a K-vector space. Its dimension as K-vector space must then be the dimension as F-vector space divided by $[K : F]$, so as a K-vector space, V will have dimension $N^2/N = N$. Now $\sigma_1, \ldots, \sigma_n \in V$ are linearly independent (over K) and hence $n \leq N$.

30. Subgroups give you subfields, and subfields give you subgroups, as follows:

    Let $G = \mathrm{Aut}(K/F)$. Let H be a subgroup of G. Then K^H, defined in item 27, is a subfield of K/F.

    Now, lets say that E is some subfield of K/F (i.e. E is a subfield of K for which $F \subseteq E$). Then $\mathrm{Aut}(K/E)$ is a subgroup of $\mathrm{Aut}(K/F)$ because any automorphism of K that acts trivially on E is also an automorphism of K that acts trivially on F.

31. Let S_1 be the set of all subgroups of $G := \mathrm{Aut}(K/F)$. Let S_2 be the set of all subfields of K/F. In item 30 we gave a map, lets call it Φ_1, from S_1 to S_2. We also gave a map, lets call it Φ_2, from S_2 to S_1. Do these two maps give us a 1-1 correspondence here between subgroups and subfields? Are these maps each others inverses?

    (a) If $|G| < [K : F]$ then the answer is NO. To see that, start with the two elements F and K^G in S_2. Now $\Phi_2(F) = G$ and $\Phi_2(K^G)$ is also G. However, if $|G| < [K : F]$ then $F \neq K^G$ by item 28, so then we see that Φ_2 is not one-to-one.

    (b) **Galois correspondence:** If K/F is a Galois extension, i.e. if $|G| = [K : F]$ then the answer is YES. We will prove this in the next two items.

32. First some observations that are true whether K/F is Galois or not:

    (a) If $E \subseteq E'$ are subfields of K/F, and $H = \mathrm{Aut}(K/E)$ and $H' = \mathrm{Aut}(K/E')$ are the corresponding subgroups, then $H' \subseteq H$.
    Proof: if $g \in H'$ then g leaves acts trivially on E', so it acts trivially on $E \subseteq E'$, and so $g \in H$.

    (b) If $H \subseteq H'$ are subgroups of G, and $E = K^H$ and $E' = K^{H'}$ are the corresponding subfields, then $E' \subseteq E$.
    Proof: If $a \in E'$ then a is invariant under H' so then it is definitely invariant under $H \subseteq H'$ and so it is in E.

    (c) If E is a subfield of K/F, if $H = \mathrm{Aut}(K/E)$, and if $E' = K^H$ then

    $$E \subseteq E' \quad \text{and} \quad \mathrm{Aut}(K/E) = \mathrm{Aut}(K/E').$$

    Proof: If $a \in E$ then it is invariant under H, and hence also an element of K^H, and so $a \in E'$. So $E \subseteq E'$ and then $H' := \mathrm{Aut}(K/E') \subseteq$

H by item 32a. Now take $g \in H$, so then g acts trivially on $E' = K^H$, and hence $g \in H'$, so $H \subseteq H'$, and so $H = H'$.

(d) If E is a subfield of K/F and if K/F is Galois, then K/E is Galois as well.
Proof: K/F Galois is equivalent (see item 23, I gave a complete proof of this in item 26) to saying that K is the splitting field of some separable polynomial $f(x) \in F[x]$. But then $f(x)$ is also an element of $E[x]$ so K is also the splitting field of $f(x)$ over E. Then, using item 23 again, we see that K/E is also Galois.

33. Proof of Galois Correspondence. Assume that K/F is Galois, then we get

(a) The map $\Phi_1\Phi_2$ is the identity on S_2.
Proof: Let $E \in S_2$, so E is a subfield of K/F. Then K/E is Galois by item 32d, so the group $H := \mathrm{Aut}(K/E)$ has $[K : E]$ elements. Now let $E' = K^H$ and let $H' = \mathrm{Aut}(K/E')$. Now K/E' is also Galois by item 32d, so the group H' has $[K : E']$ elements. But $H = H'$ by item 32c and so $[K : E'] = [K : E]$. But since $E \subseteq E'$, see item 32c, we get $[K : E] = [K : E'] \cdot [E' : E]$ and hence $[E' : E] = 1$ so $E' = E$. But E was an arbitrary element of S_2, and $H = \Phi_2(E)$, while $E' = \Phi_1(H) = \Phi_1\Phi_2(E)$. So the fact that $E' = E$ means that $\Phi_1\Phi_2$ sends E to E.

(b) The map $\Phi_2\Phi_1$ is the identity on S_1.
Proof: Let $H \in S_1$. Then formula (5) in item 28 says that $H = \mathrm{Aut}(K/K^H) = \Phi_2(K^H) = \Phi_2\Phi_1(H)$.