Introduction to the Galois Correspondence

Maureen Fenrick

A Primer on the Integers

1. Division algorithm: given n and $d \neq 0$ one can find q and r such that $0 \leq r < d$ and $n = qd + r$.

2. $d|n$ when $r = 0$.

3. Greatest common divisor of two integers: largest positive divisor.

4. Construction of greatest common divisor of a and b: form

$$S = \{ja + kb : j, k \in \mathbb{Z}\}.$$

Let the smallest positive integer be x. Claim: x divides a. To see this, write $a = qx + r$ where $0 \leq r < x$. To avoid $r \in S$ must have $r = 0$. Similarly x divides b. Therefore $x \leq d$. On the other hand, if we write $a = a_0 d$ and $b = b_0 d$ then we have $d|x$ therefore $d \leq x$. So $x = d$.

5. Relatively prime integers a and b: gcd is 1. Equivalent to having solution to $ja + kb = 1$.

6. a and b relatively prime and $a|bc$ implies $a|c$. Reason: $ja + kb = 1$, $jac + kbc = c$, $jac + kad = c$, $a|c$.

7. p prime and $p|ab$ implies $p|a$ or $p|b$. Reason: if p doesn't divide a then they are relatively prime so p divides b.

8. Every positive integer ≥ 2 can be factored into prime numbers. Reason: By induction on size. $n = 2$: true. $n > 2$: either prime or composite. If composite, each factor can be factored into primes.

9. Prime factorizations are unique up to order. Proof: We will prove $n = p_1 \cdots p_k$ and $n = q_1 \cdots q_j$ implies $k = j$ and same factors by induction on k. $k = 1$: $p_1 | q_1 \cdots q_j$ therefore p_1 divides some q_i so is equal to it. Forces $n = q_i = p_1$. Now consider $k > 1$. $p_1 = q_i$ for some i. Divide and use induction hypothesis.

Quotient Groups and Subgroups, pp. 16–34

Note: We can circumvent the isomorphism theorems on pp. 23–25 using the two technical points below.

Lemma: Let G be a group and let $g \in G$. If $g^n = e$ then $o(g)|n$.

Proof: Write $n = o(g)q + r$, $0 \leq r < o(g)$. Then $g^r = e$, therefore $r = 0$.

Lemma Let G be a group, let p be a prime number, and let $g \in G\backslash\{e\}$ with $g^p = e$. Then $o(g) = p$.

Proof: We have $o(g)|p$ and $o(g) > 1$, therefore $o(g) = p$.

Theorem [2.21] (Cauchy's Theorem for Finite Abelian Groups). Let G be a finite abelian group and let p be a prime divisor of $o(G)$. Then G has an element of order p.

Proof: First suppose that G is cyclic. Let $G = \langle x \rangle$ with $o(x) = n$. Let $k = \frac{n}{p}$. Then $x^k \neq e$ and $(x^k)^p = x^n = e$, therefore $o(x^k) = p$.

Now we will use induction on $o(G)$. If $o(G) = 2$ then G has an element of order 2. Now assume $2 \leq o(G) < n$ and G abelian and $p|n$ implies G has an element of order p. Consider $o(G) = n$. If G is cyclic then we are done. But if G is not cyclic, choose any $g \in G\backslash\{e\}$. Then $\langle g \rangle$ is a non-trivial normal subgroup of G. We have $|G| = |G/\langle g \rangle| \cdot o(g)$, therefore p divides one of the factors. If it divides $o(g)$ then, since $\langle g \rangle$ is a cyclic group whose order is divisible by p, it has an element of order p. But if it divides $|G/\langle g \rangle|$, then by the induction hypothesis the quotient group has an element of order p. Call it $\langle g \rangle x$. Then $(\langle g \rangle x)^{o(x)} = \langle g \rangle$, therefore $p|o(x)$, therefore $\langle x \rangle$ is a cyclic group with size divisible by p, hence contains an element of order p.

[2.26] The conjugacy relation is an equivalence relation. Reason: Symmetric from $x = e^{-1}xe$. Reflexive from $x = g^{-1}yg$ implies $y = gxg^{-1}$. Transitive: $x = g^{-1}y$ and $y = h^{-1}zh$ implies $x = (hg)^{-1}z(hg)$.

Grouping the elements of a finite group G into classes: Given $x \in G$ we have

$$c(x) = \{g^{-1}xg : g \in G\}.$$

Letting $c(x_1), \ldots, c(x_m)$ be the distinct conjugacy classes of G, we obtain the class equation

$$|G| = |c(x_1)| + \cdots + |c(x_m)|.$$

Given $x \in G$, set $G_y = \{g \in G : g^{-1}xg = y\}$. Then we have

$$|G| = \sum_{y \in c(x)} |G_y|.$$

We claim that G_x is a subgroup of G and that $G_x g = G_{g^{-1}xg}$. The latter statement implies $|G| = |c(x)||G_x|$, i.e.

$$|c(x)| = \frac{|G|}{|G_x|}.$$

If so, the class equation can be updated to

$$|G| = \frac{|G|}{|G_{x_1}|} + \cdots + \frac{|G|}{|G_{x_n}|}.$$

For each x_i with $G_{x_i} = G$ we have $x_i \in Z(G)$. Assuming $x_1, \ldots, x_k \in Z(G)$ and $x_{k+1}, \ldots, x_n \notin Z(G)$ we can write

$$|G| = |Z(G)| + \frac{|G|}{|G_{x_{k+1}}|} + \cdots + \frac{|G|}{|G_{x_n}|}.$$

$G_x = \{g \in G : g^{-1}xg = x\}$. Clearly $e \in G_x$ and $g \in G_x \implies g^{-1} \in G_x$. Suppose $g, h \in G_x$. Then $(gh)^{-1}x(gh) = g^{-1}(h^{-1}xh)g = g^{-1}xg = x$, hence $gh \in G$. The group G_x is written $C(x)$ for the centralizer of x in G.

If $g \in G_x y$ then $g = hy$ where $h^{-1}xh = x$, therefore $g^{-1}xg = y^{-1}h^{-1}xhy = y^{-1}xy$, hence $g \in G_{y^{-1}xy}$. Therefore $G_x y \subseteq G_{y^{-1}xy}$. Conversely, if $g^{-1}xg = y^{-1}xy$ then $yg^{-1}xgy^{-1} = x$, therefore $gy^{-1} \in G_x$, therefore $g \in G_x y$.

Some corollaries:

Proposition [2.30]. If G is a group of order p^n for some prime p then $p|o(Z(G))$.

Proof: In the class equation, every $|G|/|G_{x_i}|$ is divisible by p when $i > k$.

Theorem [2.31] (Cauchy's Theorem). If G is a finite group whose order is divisible by p then G has an element of order p.

Proof: By induction on $|G|$. Base case $|G| = 2$ is true. More generally, using the class equation, either the center has an element of order p or it doesn't. If it doesn't then it's size is not divisible by p, so there is some quotient group G/G_x which is not divisible by p, meaning that $|G_x|$ is divisible by p. Hence G_x has an element of order p.

p-group: a group of order p^k for some prime p.

p-Sylow subgroup: A subgroup of order p^k in a group of order $p^k q$ where $p \not| \ j$. Alternatively: a p-group H which is a subgroup of a group G with $[G : H]$ not divisible by p.

Theorem [2.34]: Let p be a prime and let G be a group with $p|o(G)$. Then G contains a Sylow p-subgroup.

Proof: By induction on m, where $|G| = p^m q$ and $p \not| \ q$.

$m = 1$: G has an element x of order p, hence $\langle x \rangle$ is a p-Sylow subgroup of G.

$m > 1$: Suppose, in the class equation, $p \not| \ [G : G_{x_i}]$. Then G_{x_i} is a p-Sylow subgroup of G. Now suppose that $p|[G : G_{x_i}]$ for each i in the class equation. Then $p|o(Z(G))$, therefore $Z(G)$ has an element x of order p and the subgroup $\langle x \rangle$ is normal in G. The quotient group $G/\langle x \rangle$ has order $p^{m-1}q$ where $p \not| \ q$, so by the induction hypothesis $G/\langle x \rangle$ has a subgroup of the form $H/\langle x \rangle$ of order p^{m-1}. This implies that $o(H) = p^m$, hence H is a p-Sylow subgroup of G.

Technical Point #1: Let K be a subgroup of G/N. Then $K = H/N$ for some subgroup H of G. Construction: let $H = \{g \in G : Ng \in K\}$. H is a subgroup of G: $h_1, h_2 \in H \Rightarrow Nh_1, Nh_2 \in K \Rightarrow (Nh_1)(Nh_2)^{-1} \in K \Rightarrow Nh_1h_2^{-1} \in K \Rightarrow h_1h_2^{-1} \in H$. $K \subseteq H/N$: $k \in K \Rightarrow k = Ng$ for some $g \in G \Rightarrow g \in H \Rightarrow k \in H/N$. $H/N \subseteq K$: $x \in H/N \Rightarrow x = Nh$ for some $h \in H \Rightarrow Nh \in K \Rightarrow x \in K$.

Corollary [2.35]: Let p be a prime and let G be a group of order $p^m q$ where $p \not| \ q$. Then G has a chain of subgroups

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_m$$

such that H_i is normal in H_{i+1} for each i and H_{i+1}/H_i is cyclic of order p.

Proof: We can take H_m to be a p-Sylow subgroup of G. This reduces the problem to showing that any p-group G has a normal subgroup H such that $[G : H] = p$. We will do this by induction on m, where $o(G) = p^m$.

$m = 1$: We can take $H = \{e\}$.

$m > 1$: By the class equation, $Z(G)$ has order divisible by p, hence has an element x of order p. The quotient group $G/\langle x \rangle$ has order p^{m-1}, so by the induction hypothesis it contains a normal subgroup K of order p^{m-2}. If we write $K = H/\langle x \rangle$ then H is a normal subgroup of G of order p^{m-1}.

Technical Point #2: If K is a normal subgroup of G/N and we write $K = H/N$ as before, then H is normal in G. Reason: form $H = \{g \in G : Ng \in K\}$ as before. We must show $ghg^{-1} \in H$ for each $g \in G$. Let $h \in H$ and $g \in G$ be given. Then $Nh \in K$, hence $(Ng)(Nh)(Ng)^{-1} \in K$, therefore $N(ghg^{-1}) \in K$, therefore $ghg^{-1} \in H$.

Exercise: Work out the details of finding the 2-Sylow and 3-Sylow subgroups of D_6.

Finite Abelian Groups and Solvable Groups, pp. 34 – 42.

The definition of internal direct product is not quite right – we'll give the one we found online.

G is the internal direct product of normal subgroups $N_1, \ldots, N_k$ if $G = N_1 \cdots N_k$ and $N_i \cap N_1 \cdots \widehat{N_i} \cdots N_k = \{e\}$ for each i.

Theorem: If G is the internal direct product of normal subgroups $N_1, \ldots, N_k$ then $G \simeq N_1 \times \cdots \times N_k$.

Proof: We first show that $x_{\sigma(1)} \cdots x_{\sigma(k)} = x_1 \cdots x_k$ when $x_i \in N_i$ for each i. If suffices to show that $x_i x_j = x_j x_i$ when $i \neq j$. This follows from N_i, N_j normal and $N_i \cap N_j = \{e\}$. So the mapping $(x_1, \ldots, x_n) \mapsto x_1 \cdots x_n$ is a surjective homomorphism from $N_1 \times \cdots \times N_k$ to G. The mapping is injective because $x_1 \cdots x_k = e$ implies $x_i \in N_1 \cdots \widehat{N_i} \cdots N_k$ implies $x_i = e$ for each i.

Lemma: Let G be a group and suppose $a \in G$ and $o(a) = n$. Then $o(a^s) = \frac{n}{\gcd(n,s)}$.

Proof: Let m be the least positive integer such that $a^{sm} = e$. Write $d = \gcd(n, s)$ and $n = n_0 d$ and $s = s_0 d$. We must show $m = n_0$. We have $a^{sn_0} = a^{s_0 n} = e$, therefore $m \leq n_0$. We also have $a^{sm} = e$, therefore $n | sm$, therefore $n_0 | s_0 m$, therefore $n_0 | m$, therefore $n_0 \leq m$. Therefore $m = n_0$.

Example motivating next Lemma: Let G be cyclic of order 4: $G = \langle a \rangle$. By the previous Lemma, $o(a^2) = \frac{4}{\gcd(4,2)} = 2$. Therefore $G/\langle a^2 \rangle$ is a group of order 2. We have $o(\langle a^2 \rangle a) = 2$. But we also have $\langle a^2 \rangle a = \{a, a^3\}$. Note $o(a) = 4$ and $o(a^3) = 4$. So no element in $\langle a^2 \rangle a$ has order equal to the order of $o(\langle a^2 \rangle a)$.

Lemma: Let G be a finite abelian group and let $a \in G$ have maximum order in G. Then for each $g \in G$ there exists $h \in \langle a \rangle g$ such that $o(h) = o(\langle a \rangle g)$.

Proof: We have $g^{o(\langle a\rangle g)} = a^n$ for some n. Therefore, for an arbitrary q,

$$(ga^q)^{o(\langle a\rangle g)} = a^{n+o(\langle a\rangle g)q},$$

hence computing orders we have

$$\frac{o(ga^q)}{\gcd(o(ga^q), o(\langle a\rangle g))} = \frac{o(a)}{\gcd(o(a), n + o(\langle a\rangle g)q)}.$$

Since

$$(\langle a\rangle g)^{o(ga^q)} = (\langle a\rangle ga^q)^{o(ga^q)} = \langle a\rangle e,$$
$$o(\langle a\rangle g) | o(ga^q).$$

This implies

$$\frac{o(ga^q)}{o(\langle a\rangle g)} = \frac{o(a)}{\gcd(o(a), n + o(\langle a\rangle g)q)},$$
$$o(ga^q) = \frac{o(a)o(\langle a\rangle g)}{\gcd(o(a), n + o(\langle a\rangle g)q)}.$$

Since a has maximum order in G, this implies

$$o(\langle a\rangle g) \leq \gcd(o(a), n + o(\langle a\rangle g)q).$$

If we write $n = do(\langle a\rangle g) + r$ with $0 \leq r < o(\langle a\rangle g)$, then choosing $q = -d$ we have $n + o(\langle a\rangle g)q = r < o(\langle a\rangle g)$. If r is positive we obtain the contradiction $o(\langle a\rangle g) \leq r < o(\langle a\rangle g)$, therefore $r = 0$ and

$$o(ga^q) = \frac{o(a)o(\langle a\rangle g)}{\gcd(o(a), n + o(\langle a\rangle g)q)} = \frac{o(a)o(\langle a\rangle g)}{\gcd(o(a), 0)} = o(\langle a\rangle g).$$

Theorem: Let G be a finite abelian group with $o(G) \geq 2$. Then G contains non-trivial elements $a_1, \ldots, a_k$ such that every element in G can be expressed in the form $a_1^{e_1} \cdots a_k^{e_k}$ where e_i is unique mod a_i for each i.

Proof: By induction on $o(G)$. When $o(G) = 2$ we can write $G = \langle g\rangle$ for some g. Now consider $o(G) = n$. If G is cyclic then the statement of the theorem is true. Now suppose that G is not cyclic. Let $a \in G$ have maximum order. Let $[a_1], \ldots, [a_k] \in G/\langle a\rangle$ be provided by the induction hypothesis. Then every element in G can be expressed in the form $a_1^{e_1} \cdots a_k^{e_k} a^n$ where the

choice of each e_i is unique mod $o([a_i])$. We can assume that we have chosen $a_1, \ldots, a_k$ so that $o([a_i]) = o(a_i)$ for each i. If

$$a_1^{e_1} \cdots a_k^{e_k} a^n = e$$

then by uniqueness we have $e_1 \equiv 0 \bmod o(a_1)$,..., $e_k \equiv 0 \bmod o(a_k)$, leaving $a^n = e$ and $n \equiv 0 \bmod o(a)$.

Note that this theorem implies that

$$G \simeq \langle a_1 \rangle \times \cdots \times \langle a_k \rangle \simeq \mathbb{Z}_{o(a_1)} \times \cdots \times \mathbb{Z}_{o(a_k)}.$$

The textbook proves that if $n = n_1 \cdots n_k$ is a factorization into pairwise relatively prime integers then

$$\mathbb{Z}_n \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

via the Chinese Remainder Theorem. Here is another proof:

Lemma: Let G be a finite abelian group and let $a_1, \ldots, a_k \in G$ with relatively prime orders. Then $o(a_1 \cdots a_k) = o(a_1) \cdots o(a_k)$.

Proof: It will suffice to prove this for two elements. Since $(a_1 a_2)^{o(a_1)o(a_2)} = e$, we have $o(a_1 a_2) | o(a_1)o(a_2)$. To show $o(a_1)o(a_2) | o(a_1 a_2)$ it suffices to show $o(a_1) | o(a_1 a_2)$ and $o(a_2) | o(a_1 a_2)$ since the two orders are relatively prime. We have

$$a_1^{o(a_1 a_2)} = a_2^{-o(a_1 a_2)},$$

$$\frac{o(a_1)}{\gcd(o(a_1), o(a_1 a_2))} = \frac{o(a_2)}{\gcd(o(a_2), o(a_1 a_2))},$$

$$o(a_1) \gcd(o(a_2), o(a_1 a_2)) = o(a_2) \gcd(o(a_1), o(a_1 a_2)),$$

$$o(a_1) | \gcd(o(a_1), o(a_1 a_2)) \text{ and } o(a_2) | \gcd(o(a_2), o(a_1 a_2)),$$

$$o(a_1) | o(a_1 a_2) \text{ and } o(a_2) | o(a_1 a_2).$$

Now let G_i be cyclic of order n_i with generator a_i for $1 \leq i \leq k$, where the orders are relatively prime. Then $G_1 \times \cdots \times G_k$ has order $n = n_1 \cdots n_k$. Since the element $(a_1, \ldots, a_k)$ has order $n_1 \cdots n_k$, we have

$$G_1 \times \cdots \times G_k = \langle (a_1, \ldots, a_k) \rangle.$$

If G is any cyclic group of order $n_1 \cdots n_k$ with cyclic generator a then an isomorphism from G to $G_1 \times \cdots \times G_k$ is given by $a^x \mapsto (a_1^x, \ldots, a_k^x)$.

Note that if $G_i = \mathbb{Z}_{n_i}$ then an isomorphism is $[x]_n \mapsto ([x]_{n_1}, \ldots, [x]_{n_k})$. Since $\gcd(x, n) = 1 \Leftrightarrow \gcd(x, n_i) = 1$ for all i, this implies

$$\mathbb{Z}_n^\times \simeq \mathbb{Z}_{n_1}^\times \times \cdots \times \mathbb{Z}_{n_k}^\times$$

since the map is multiplicative and injective and the two groups have the same number of elements. To verify the statement about gcd, suppose $\gcd(x, n_i) = 1$ for all i. Then we get $a_i x + b_i n_i = 1$ for each i, and the product of these equations yields $ax + bn = 1$.

Normal Subgroups Lemma:

(a) Let N be normal in G. Then H is normal in G/N if and only if $H = K/N$ for some normal subgroup of K containing N.

(b) If G is a group, H is a subgroup, and N is a normal subgroup, then $NH = HN$ and NH is a subgroup.

Proof: (a) Let $K = \{g \in G : Ng \in H\}$. This contains N. It is a subgroup since H is a subgroup. If is normal because H is normal.

(b)$Nh = hN \subseteq HN$, therefore $NH \subseteq HN$. $hN = Nh \subseteq NH$, therefore $HN \subseteq NH$. Hence $NH = HN$. NH is closed: $(NH)(NH) = N(HN)H = N(NH)H \subseteq NH$. NH is closed with respect to inverses: $(nh)^{-1} = h^{-1}n^{-1} \in HN = NH$.

Definition: a group G is solvable if and only if there is a chain of subgroups of G such that each is normal in the next and the quotient groups are abelian.

Theorem [3.9]: Subgroups of solvable groups are solvable.

Proof: Let G be solvable. Let $K < G$ be given. Given $H \lhd H' < G$ such that H'/H is abelian, we will show that $K \cap H \lhd K \cap H'$ and that $K \cap H'/K \cap H$ is abelian. Let $x \in K \cap H$ and $y \in K \cap H'$ be given. Then $yxy^{-1} \in K$ by closure of K in H' and $yxy^{-1} \in H$ by normality of H in H', therefore $yxy^{-1} \in K \cap H$. Let $x, y \in K \cap H'$. Then $xyx^{-1}y^{-1} \in K$ by closure of K and $xyx^{-1}y^{-1} \in H$ since H'/H is abelian, hence $xyx^{-1}y^{-1} \in K \cap H$, hence $K \cap H'/K \cap H$ is abelian. So we get a solvable series for K by intersecting the solvable series for G by K.

Theorem [3.10]: Quotients of solvable groups are solvable.

Proof: Let G be solvable and let N be a normal subgroup of G. Given $H \lhd H' < G$ such that H'/H is abelian, form $K = NH$ and $K' = NH'$. Since N is normal, these are subgroups of G. They both contain N. We must show that $NH/N \lhd NH'/N$ and that their quotient is abelian. If $L = \{g \in G : Ng \in NH/N\}$ then we can show that $L = NH$. If $L' = \{g \in G : Ng \in NH'/N\}$ then we can show that $L = NH'$. So it suffices to show $NH \lhd NH'$. This is clear by a calculation. The quotient is abelian because because $h_1h_2h_1^{-1}h_2^{-1} \in H$ for all $h_1, h_2 \in H'$. To find a solvable series for G/N, first find a solvable series for G, then multiply each subgroup by N, then form the quotient with N.

Theorem [3.11]: Let G be a group. If G has a normal subgroup N such that both N and G/N are solvable, then G is solvable.

Proof: First, find a solvable series for N. Second, find a solvable series for G/N. Lift the latter to a chain of subgroups containing N, each normal in the next with abelian quotients. Concatenate the two series.

Theorem [3.15]: S_n is not solvable for $n \geq 5$.

Proof: By contradiction. If H is normal in S_n and S_n/H is abelian, then

$$(123) = (342)(215)(324)(251) = (342)(215)(342)^{-1}(215)^{-1} \in H.$$

By the same logic, (123) is an element of every subgroup in a solvable series, which contradicts the fact that the first group in such a series is $\{e\}$. Hence there cannot be a solvable series.

Introduction to Rings – pp. 43 – 60

Example of a non-trivial non-unital ring homomorphism: Let R be a commutative ring with an element $x \neq 1_R$ such that $x^2 = x$. Define $f : R \to R$ by $f(a) = xa$. Then $f(a + b) = x(a + b) = xa + xb = f(a) + f(b)$, $f(ab) = xab = (xa)(xb) = f(a)f(b)$, $f(x) = x^2 = x$. For example, $R = \mathbb{Z} \times \mathbb{Z}$ with $x = (1, 0)$.

Motivation for definition of an ideal: Let $f : R \to S$ be a ring homomorphism. Set $I = \ker f = \{r \in R : f(r) = 0_S\}$. Then $\ker f$ is a normal subgroup of R under addition, and the quotient group R/I is defined. Note also that if $r \in R$ and $x \in I$ then $rx \in I$ and $xr \in I$. If we define $(I+x)(I+y) = I+xy$ and check that this is well-defined, we must verify that $x - x' \in I$ and $y - y' \in I$ implies $xy - x'y' \in I$. We have

$$xy - x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y') \in I.$$

Definition: Let R be a ring. An ideal of R is any subset I such that I is a subgroup under addition and $rI = Ir = I$ for all $r \in R$. The expression R/I denotes the quotient ring whose elements belong to the quotient group R/I under addition and with multiplication defined by $(I + x)(I + y) = I + xy$.

Quotient Field of an Integral Domain: Let R be an integral domain. Define an equivalence relation on $R \times R^*$ by $(a, b) \equiv (a', b')$ if and only if $ab' = a'b$. Clearly reflexive and symmetric. Transitive: $ab' = a'b$ and $a'b'' = a''b'$ implies $ab'b'' = a'bb'' = a''b'b$ implies $(ab'' - a''b)b' = 0$ implies $ab'' - a''b = 0$ implies $ab'' = a''b$.

Addition: $[(a_1, b_1)] + [(a_2, b_2])] = [(a_1b_2 + a_2b_1, b_1b_2)]$. Well defined: suppose $a_1b_1' = a_1'b_1$ and $a_2b_2' = a_2'b_2$. Then

$$(a_1b_2 + a_2b_1)b_1'b_2' = a_1b_1' \cdot b_2b_2' + a_2b_2' \cdot b_1b_1' = a_1'b_1 \cdot b_2b_2' + a_2'b_2 \cdot b_1b_1' =$$

$$(a_1'b_2' + a_2'b_1')b_1b_2.$$

Multiplication: $[(a_1, b_2)][(a_2, b_2)] = [(a_1a_2, b_1b_2)]$. Well defined: suppose $a_1b_1' = a_1'b_1$ and $a_2b_2' = a_2'b_2$. Then

$$a_1a_2b_1'b_2' = a_1'b_1a_2'b_2 = a_1'a_2'b_1b_2.$$

Additive identity: $[(0, 1_R)]$.

Additive inverse: $-[(a, b)] = [(-a, b)]$.

Multiplicative inverse: $[(b, b')]^{-1} = [(b', b)]$.

Isomorphic copy of R: $r \to [(r, 1_R)]$, $[(r + r', 1_R)] = [(r, 1_R)] + [(r', 1_R)]$, $[(rr', 1_R)] = [(r, 1_R)][(r', 1_R)]$, $[(r, 1_R)] = [(0_R, 1_R)]$ implies $r \cdot 1_R = 1_R\dot{0}_R$ implies $r = 0_R$.

Corollary [4.35]: Let R be an integral domain with fraction field K. If E is any field containing R then E contains an isomorphic copy of K.

Proof: Define $K_E = \{ab^{-1} : a, b \in R, b \neq 0_R\}$. One can check that this is closed with respect to addition, formation of additive inverses, and formation of multiplicative inverses. Now define $f : qf(R) \to K_E$ by $f([(a, b)]) = ab^{-1}$.

Well-defined: if $ab' = a'b$ then $ab^{-1} = a'(b')^{-1}$ in E, hence in K_E. One can also check additive and multiplicative and surjective. Injective: $ab^{-1} = a'(b')^{-1}$ implies $ab' = a'b$ implies $[(a,b)] = [(a',b')]$.

pp. 60–72: Factoring in $F[x]$

Begin with Section 23 Notes, A First Course in Abstract Algebra, John B. Raleigh, 2003, Addison-Wesley.

1. Throughout this section, F is a field and $F[x]$ is the ring of polynomials with coefficients in F. We will show that $F[x]$ has many properties we associate with $\mathbb{Z}$: a division algorithm, prime (irreducible) polynomials, and unique factorization into irreducible polynomials. We will also write f instead of $f(x)$. The degree of f is $\deg(f) = k$ where $f = \sum_{i=0}^{k} a_k x^k$ and $a_k \neq 0$.

2. Division Algorithm: For each $f, g \in F[x]$ such that $f \neq 0$ and $g \neq 0$ there exists $r, q \in F[x]$ such that $f = gq + r$ and $\deg(r) < \deg(g)$.

Proof: we will first show that this is true when $\deg(f) < \deg(g)$. In this case we have $f = g \cdot 0 + f$, so can take $q = 0$ and $r = f$.

Now we'll show that q and r can be found when $\deg(f) \geq \deg(g)$ by induction on $n = \deg(f) - \deg(g)$. The base case is $n = 0$. In this case $f = f_0 + a_k x^k$ and $g = g_0 + b_k x^k$ where f_0 and g_0 are smaller degree polynomials and $a_k \neq 0, b_k \neq 0$. Note that $f - \frac{a_k}{b_k} g$ has degree $< k$. Therefore we have $f = g\frac{a_k}{b_k} + (f - \frac{a_k}{b_k} g)$, and we set $q = \frac{a_k}{b_k}$ and $r = f - \frac{a_k}{b_k} g$.

Now assume that we can find q and r when $\deg(f) - \deg(g) = n$. Consider now $\deg(f) - \deg(g) = n+1$. Then $\deg(f) - \deg(gx) = n$, and by the induction hypothesis we can find q_1, r_1 such that $f = (gx)q_1 + r_1$. If $\deg(r_1) < \deg(g)$ then we are done, setting $q = q_1 x$ and $r = r_1$. But if $\deg(r) = \deg(g)$ then by the base base we can find q_2 and r_2 with $r = gq_2 + r_2$ with $\deg(r_2) < \deg(g)$. Hence we have $f = (gx)q_1 + gq_2 + r_2 = g(xq_1 + q_2) + r_2$, and we can set $q = xq_1 + q_2$ and $r = r_2$.

2. The polynomials q and r in the Division Algorithm are unique.

Proof: Let f and g be given and assume $f = gq_1 + r_1$ and $f = gq_2 + r_2$ where $\deg(r_1) < \deg(g)$ and $\deg(r_2) < \deg(g)$. Then we have $gq_1 + r_1 = gq_2 + r_2$, $g(q_1 - q_2) = (r_2 - r_1)$. If neither expression is zero, then the lefthand side has degree $\geq \deg(g)$ and the righthand side has degree $< \deg(g)$. Contradiction. Therefore $r_2 - r_1 = 0$, which forces $g(q_1 - q_2) = 0$, which forces $q_1 - q_2 = 0$ since $F[x]$ is an integral domain. Hence $q_1 = q_2$ and $r_1 = r_2$.

3. A non-constant polynomial $f \in F[x]$ is irreducible if and only if $f = ab$ implies $\deg(a) = \deg(f)$ or $\deg(b) = \deg(f)$. A non-zero polynomial f divides a non-zero polynomial g if and only if $f = gh$ for some $h \in F[x]$. Two polynomials f and g are said to be relatively prime if and only if $d|f$ and $f|g$ implies $\deg(d) = 0$.

4. f and g are relatively prime polynomials if and only if there exist $r, s \in F[x]$ such that $rf + sg = 1$.

Proof: Assume f and g are relatively prime in $F[x]$. Let $S = \{hf+kg : h, k \in F[x]\}$. Then there is at least one non-zero polynomial in S. Let d be the smallest degree non-zero polynomial in S. We claim that $d|f$ and $d|g$, hence $\deg(d) = 0$. To see this, write $f = dq + r$ where $\deg(r) < \deg(d)$. Note that we can write $d = hf+kg$ for some $h, k \in F[x]$. So we have $f = (hf+kg)q+r$, $r = (1-h)f + (-kq)g \in S$. To avoid a contradiction, we must have $r = 0$. Hence $f = dq$ and $d|f$. Similarly, $d|g$. Therefore $\deg(d) = 0$.

Conversely, suppose that f and g are relatively prime. Then $rf + sg = 1$ is possible. If $d|f$ and $d|g$ then we can write $f = df_0$ and $g = dg_0$, hence $1 = rdf_0 + sdg_0 = d(rf_0 + sg_0)$, which can only be possible if both d and $rf_0 + sg_0$ both have degree 0.

5. Theorem: Let f and g be relatively prime polynomials in $F[x]$. If $f|gh$ in $F[x]$ then $f|h$.

Proof: We can write $rf + sg = 1$. Now suppose $f|gh$. Then $gh = fk$ for some polynomial k. Therefore $h = h(rf + sg) = hrf + hsg = hrf + sfk = f(hr + sk)$, therefore $f|h$.

6. Corollary: if p is irreducible and $p|rs$ in $F[x]$ then $p|r$ or $p|s$.

Proof: Suppose p does not divide r. Then p and r are relatively prime: Let $d|p$ and $d|r$. We will show that d must have degree 0. If not, then it must have degree equal to the degree of p, therefore $p = d\alpha$ where $\alpha \in F^*$. Since $d|r$, we have $r = dr_0 = \alpha^{-1}pr_0 = p(\alpha^{-1}r_0)$, which contradicts our hypothesis that p does not divide r. Hence p and r are relatively prime. By the previous theorem, we must have $p|s$.

7. Every non-constant polynomial f can be factored into a product of irreducible polynomials.

Proof: by induction on $\deg(f) = n$. If $n = 1$, then $f = ab$ implies $\deg(a) = 1 = \deg(f)$ or $\deg(b) = 1 = \deg(f)$, so f is irreducible, and f is its own product of irreducible polynomials.

Now assume that all polynomials of degree $1, 2, \ldots, n$ can be factored into a product of irreducible polynomials. Consider f with degree $n+1$. If f is irreducible, we are done. But if f is not, then $f = ab$ where $\deg(a) < \deg(f)$ and $\deg(b) < \deg(f)$. This implies that neither a nor b is a constant polynomial. By the induction hypothesis, both a and b can be factored into products of irreducible polynomials. Multiplying them together, so can f.

8. If $f = p_1 p_2 \cdots p_k$ and $f = q_1 q_2 \cdots q_j$ are two factorizations of f into irreducible polynomials then $k = j$ and the irreducible factors can be paired into associates (two polynomials are associates if one is a non-zero constant multiple of the other).

Proof: By induction on $k \geq 1$. For the base case, suppose $p_1 = f = q_1 q_2 \cdots q_j$. Since p_1 is irreducible, $j = 1$ and we have $p_1 = q_1$. Now assume the theorem is true for $k \leq n$. Consider $k = n+1$. Write $p_1 \cdots p_{n+1} = f = q_1 \cdots q_j$. Then $p_{n+1} | q_1 \cdots q_j$, so we must have $p_{n+1} | q_i$ for some i. Since q_i is irreducible, we must have $\deg(p_{n+1}) = \deg(q_i)$. This implies $q_i = \alpha_i p_{n+1}$ for some $\alpha_i \in F^*$. Hence p_{n+1} and q_i are associates. So now we have $p_1 \cdots p_n = (\alpha_i q_1) \cdots \widehat{q_i} \cdots q_j$. The polynomial $\alpha_i q_1$ is irreducible. Using the induction hypothesis, we must have $j - 1 = n$ and we can pair off the remaining irreducible factors into associates. Note that if $\alpha_i q_1$ is an associate of p_j then so is q_1. So we have $j = n+1$ and all irreducibles paired off into associates.

9. We have proved the main theorems. We are ready for some applications. The first application is the Factor Theorem: if $f \in F[x]$, $a \in F$, then $f(a) = 0$ if and only if $x - a$ divides f.

Proof: Assume $f(a) = 0$. Using the division algorithm, write $f(x) = (x - a)q + r$ where $\deg r < 1$. Then r is a constant polynomial. Applying the homomorphism ϕ_a to both sides, we get $f(a) = (a-a)q(a) + r(a)$, i.e. $0 = r$. Therefore $f(x) = (x - a)q$ and $x - a$ divides f. Conversely, suppose $x - a$ divides f. Then $f = (x - a)q$. Applying ϕ_a, we get $f(a) = (a - a)q(a) = 0$.

10. Corollary: If f has n distinct roots then $\deg(f) \geq n$.

Proof: by induction on n. For $n = 1$ we have $f = (x - a)q$ where $f(a) = 0$, therefore $\deg(f) \geq 1$. Now assume if f has n distinct roots then $\deg(f)$ has degree $\geq n$. Consider $f \in F[x]$ with roots $a_1, \ldots a_{n+1}$. We can write $f = (x - a_{n+1})g$ for some polynomial g. Since g has roots $a_1, \ldots, a_n$, the induction hypothesis implies that g has degree $\geq n$, hence f has degree $\geq n + 1$.

11. Corollary: if F is a field and $G \leq F^*$ is a finite group under multiplication then G is cyclic.

Proof: Write $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$. Then G has an element of order $m = \text{lcm}(n_1, \ldots, n_k)$, hence $o(G) \geq m$. Now every element $g \in G$ satisfies $g^m = 1_F$, therefore the elements of G are roots of $x^m - 1_F$, and since there are at most m distinct roots, we must have $o(G) \leq m$. Therefore $o(G) = m$ and G is cyclic.

12. The next few results are methods of proving that a polynomial is irreducible.

13. If $f \in F[x]$ has degree 2 or 3 then f is reducible if and only if f has a root in F.

Proof: If f is reducible then $f = hk$ for some $h, k \in F[x]$, and one of these factors has the form $ax + b$ where $a \neq 0$. Therefore $f(-\frac{b}{a}) = 0$. Conversely, if $f(r) = 0$ then $f = (x - r)k$ for some $k \in F[x]$.

14. Example: $f(x) = x^2 - 6$ is irreducible in $\mathbb{Q}[x]$. Otherwise, it would have a root in $\mathbb{Q}$, which clearly it does not. See also Example 23.8, page 214.

15. Theorem: if $f \in \mathbb{Z}[x]$ and $f = bc$ with $b, c \in \mathbb{Q}[x]$ then $f = BC$ with $B, C \in \mathbb{Z}[x]$ and $\deg(B) = \deg(b)$ and $\deg(C) = \deg(c)$. (See Proposition [5.25] below.)

16. Corollary: if $f = x^n + \text{lower terms} \in \mathbb{Z}[x]$ has a root $r \in \mathbb{Z}$ then it has a root $m \in \mathbb{Z}$ and $m | f(0)$.

Proof: Write $f = (x - r)c$. Then $f = (jx + k)C$ for some $j, k \in \mathbb{Z}$ and $C \in \mathbb{Z}[x]$. Since the leading term of f has coefficient 1, this forces $j = \pm 1$. Without loss of generality $f = (x + k)C$. Therefore $f(-k) = 0$.

17. Eisenstein's Criterion: Let $f = a_0 + a_1 x + \cdots + a_n x^n$ be a non-constant polynomial with integer coefficients. If there is prime number p such that p divides a_0 through a_{n-1}, $p \not| \, a_n$, and $p^2 \not| \, a_0$, then f is irreducible in $\mathbb{Q}[x]$.

Proof. Suppose not. Then we can write $f = bc$ for some pair of polynomials b and c with integer coefficients, each of degree between 1 and $n - 1$. Write $b = b_0 + b_1 x + \cdots + b_r x^r$ and $c = c_0 + c_1 x + \cdots + c_{n-r} x^{n-r}$. Then $a_0 = b_0 c_0$, therefore $p | b_0 c_0$, therefore p divides b_0 or c_0 but not both of them. Without loss of generality we will say that $p | b_0$ and $p \not| \, c_0$.

We will now prove that $p|b_k$ for all k by induction on k, $0 \leq k \leq r$. This will yield a contradiction because $a_n = b_r c_{n-r}$ and $p|b_r$ implies $p|a_n$, contrary to hypothesis.

Base Case: $p|b_0$. We already know this.

Induction Hypothesis: p divides b_0 through b_k for some $k < r$.

We will now show that $p|b_{k+1}$. We have $a_{k+1} = b_{k+1}c_0 + b_k c_1 + b_{k-1}c_2 + \cdots + b_0 c_{k+1}$. Since $k < r$ and $r < n$, we must have $k + 1 < n$. By hypothesis we know that $p|a_{k+1}$. On the other hand, by the induction hypothesis we know that p divides b_0 through b_k. Therefore p divides $a_{k+1} - (b_k c_1 + \cdots + b_0 c_{k+1}) = b_{k+1}c_0$. Since $p|b_{k+1}c_0$ and $p \not| c_0$, $p|b_{k+1}$. This completes the induction proof. Hence $p|b_r$, which contradicts $p \not| a_n$. Therefore f must be irreducible.

18. Example: $f = 11 + 121x^5 + 5x^{27}$ is irreducible in $\mathbb{Q}[x]$ using $p = 5$.

Let $f(x) \in \mathbb{Z}[x]$. The content of $f(x)$ is the greatest common divisor of its coefficients. A polynomial is primitive if its content is 1.

Proposition [5.24] If f and g are primitive then so is fg.

Proof: For any n and any p, q such that $p + q = n$, the coefficient of x^n in fg is

$$\sum_{i<p} f_i g_{n-i} + f_p g_q + \sum_{j<q} f_{n-j} g_j.$$

If fg is not primitive then there is a prime number P which divides all its coefficients. Choose $p \geq 0$ such that $P \not| f_p$ but $p|f_0, \ldots, f_{p-1}$. Choose $q \geq 0$ such that $q \not| g_q$ but $q|g_0, \ldots, g_{q-1}$. Then $P|f_p g_q$, which implies $P|f_g$ or $P|g_q$: contradiction. Therefore fg is primitive.

Proposition [5.25] If $f(x)$ be primitive in $\mathbb{Z}[x]$. If $f(x)$ is reducible in $\mathbb{Q}[x]$ then $f(x)$ is reducible in $\mathbb{Z}[x]$.

Proof: Write $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$. Then $nf(x) = G(x)H(x)$ in $\mathbb{Z}[x]$ for some $n \in \mathbb{Z}^+$, where $G(x)$ and $H(x)$ are primitive in $\mathbb{Z}[x]$. Since $G(x)H(x)$ is primitive and n divides all of its coefficients, $n = 1$.

Finite Dimensional Field Extensions, pp. 73–97.

We begin with a review of dimension theory.

Definition: Let $K \subseteq F$ be fields. A linear combination of $f_1, \ldots, f_n \in F$ over K is an expression of the form $k_1 f_1 + \cdots + k_n f_n$ where each $k_i \in K$. The

span of $f_1, \ldots, f_n \in F$ over K is the set of all linear combinations over K, denoted by $\text{span}_K(f_1, \ldots, f_n)$. We say that F is finitely generated over K if $F = \text{span}_K(f_1, \ldots, f_n)$ for some finite collection $\{f_1, \ldots, f_n\} \subseteq F$. When F is finitely generated over K we define the dimension $[F : K]$ to be the smallest n such that F is generated by n elements over K. A basis for F over K is defined to be any set $\{f_1, \ldots, f_n\} \subseteq F$ such that $F = \text{span}_K(f_1, \ldots, f_n)$ and $n = [F : K]$.

Example: $\mathbb{C} = \text{span}_{\mathbb{R}}(1, i)$ and $[\mathbb{C} : \mathbb{R}] = 2$ because $\mathbb{C}$ cannot be generated by one element, otherwise it contains all reals or no reals other than 0.

Definition: Let $K \subseteq F$ be fields. The elements $f_1, \ldots, f_n \in F$ are said to be linearly independent over K if $k_1 f_1 + \cdots k_n f_n = 0_F$ implies $k_1 = \cdots = k_n = 0_K$. A linearly dependent collection $f_1, \ldots, f_n \in F$ is one in which $k_1 f_1 + \cdots + k_n f_n = 0_F$ where at least one $k_i \neq 0_K$.

Example: 1 and i in $\mathbb{C}$ are linearly independent over $\mathbb{R}$.

Lemma: Let $K \subseteq F$ be a field extension. For all integers $n \geq 1$ and $f_1, \ldots, f_n \in F$, every $u_1, \ldots, u_{n+1} \in \text{span}_K(f_1, \ldots, f_n)$ are linearly dependent over K.

Proof: By induction on n. For $n = 1$ consider $k_1 f_1$ and $k_2 f_1$ in $\text{span}_K(f_1)$. If $k_1 = k_2$ then $1_K(k_1 f) - 1_K(k_2 f_2) = 0_F$. Otherwise, $k_2(k_1 f_1) - k_1(k_2 f_1) = 0_F$, and either $k_1 \neq 0_K$ or $k_2 \neq 0_K$. Assume the lemma is true for $f_1, \ldots, f_n$. Consider $f_1, \ldots, f_{n+1}$ and linear combinations $u_1, \ldots, u_{n+2} \in \text{span}_k(f_1, \ldots, f_{n+1})$. If these are all linear combinations of $f_1, \ldots, f_n$ then we can find a non-trivial linear combination of u_1 through u_{n+1} to be 0_F and we can set the coefficient of u_{n+2} to be 0_K. Otherwise, without loss of generality u_{n+2} has a non-zero coefficient of f_{n+1}. Then for each i we can find k_i such that $u_i - k_i u_{n+2}$ is a linear combination of $f_1, \ldots, f_n$. Using the induction hypothesis we can combine these into 0_F using a non-trivial linear combination via

$$k'_1(u_1 - k_1 u_{n+2}) + \cdots + k'_{n+1}(u_{n+1} - k_{n+1} u_{n+2}) = 0_F.$$

This yields

$$k'_1 u_1 + \cdots + k'_{n+1} u_{n+1} - (k'_1 k_1 + \cdots + k'_{n+1} k_{n+1}) u_{n+2} = 0_F,$$

which is a non-trivial linear combination.

Theorem: Let $K \subseteq F$ be a field extension, let $\{f_1, \ldots, f_n\} \subseteq F$ be linearly independent, and suppose $F = \text{span}_K(f_1, \ldots, f_n)$. Then $[F : K] = n$.

Proof: We have $[F : K] \leq n$. We cannot have $[F : K] < n$, otherwise $\{f_1, \ldots, f_n\}$ are linearly dependent.

Theorem: Let $K \subseteq F$ be a field extension with $[F : K] = n$. Let $\{f_1, \ldots, f_n\} \subseteq F$. The following statements are equivalent:

(1) $F = \text{span}_K(f_1, \ldots, f_n)$.

(2) $f_1, \ldots, f_n$ are linearly independent over K.

Proof: Suppose $F = \text{span}_K(f_1, \ldots, f_n)$. If they are not linearly independent, then one of them can be expressed in terms of the other and the remaining $n - 1$ of them span F over K. This contradicts $[F : K] = n$. Hence they must be linearly independent.

Conversely, suppose $\{f_1, \ldots, f_n\}$ are linearly independent over K. Given that $[F : K] = n$, there is a set $\{g_1, \ldots, g_n\} \subseteq F$ such that $F = \text{span}_K(g_1, \ldots, g_n)$. For each g_i, the set $\{f_1, \ldots, f_n, g_i\}$ is linearly dependent over K, hence there is a non-trivial linear combination

$$\alpha_1 f_1 + \cdots + \alpha_n f_n + \beta g_i = 0$$

with coefficients in K. We cannot have $\beta = 0$, otherwise $\alpha_1 = \cdots = \alpha_n = 0$ by linear independence. Therefore $g_i \in \text{span}_K(f_1, \ldots, f_n)$. This implies

$$F = \text{span}_K(g_1, \ldots, g_n) \subseteq \text{span}_K(f_1, \ldots, f_n) \subseteq F,$$

hence $F = \text{span}_K(f_1, \ldots, f_n)$.

The two theorems taken together say that to compute $[F : K]$, find any basis. Knowing $[F : K] = n$, any n linearly independent elements in F form another basis, and any n elements that generate F over K form a basis.

Example: $1 + i$ and $1 - i$ are linearly independent over $\mathbb{R}$, hence form a basis for $\mathbb{C}$. $\mathbb{C} = \text{span}_{\mathbb{R}}(1 + i, 2 + i)$, therefore $1 + i$ and $2 + i$ form a basis for $\mathbb{C}$.

One interesting consequence of $[F : K] = n$: every $u \in F$ is the root of some polynomial $f(x) \in K[x]$ of degree $\leq n$. Reason: the elements $1, u, \ldots, u^n$ must be linearly dependent.

Example: $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. So every $a + b\sqrt{2}$ satisfies a polynomial of degree ≤ 2. In fact, we have

$$(a + b\sqrt{2})^2 = a^2 + 2ab\sqrt{2} + 2b^2 = 2a(a + b\sqrt{2}) - a^2 + 2b^2,$$

hence $a + b\sqrt{2}$ is a root of $f(x) = x^2 - 2ax + (a^2 - 2b^2) \in \mathbb{Q}[x]$.

Theorem: Let F be a field. Let $f(x) = \sum_{i=0}^{n} f_k x^k \in F[x]$ be a non-zero polynomial. Then there exists a field E and an injective ring homomorphism $\phi : F \to E$ such that $\phi(F)$ is isomorphic to F and the polynomial $f'(x) = \sum_{i=0}^{n} \phi(f_k) x^k$ has a root in $\phi(F)$.

Proof: Let $p(x)$ be an irreducible divisor of $f(x)$. Form the field $E = F[x]/(p(x))$. Define $\phi : F \to E$ by $\phi(\alpha) = \alpha + (p(x))$. Then ϕ is an injective ring homomorphism and $\phi(F) = \{\alpha + (p(x)) : \alpha \in F\}$ is isomorphic to F. Let $\beta = x + (p(x)) \in E$. Then

$$f'(\beta) = \sum_{i=0}^{n} \phi(f_k)\beta^k = \sum_{i=0}^{n} (f_k + (p(x)))(x^k + (p(x))) =$$

$$f(x) + (p(x)) = 0 + p(x).$$

Remark: In the theorem just proved, $\phi(F)$ is an isomorphic copy of F in E and $\phi(F)[x]$ is an isomorphic copy of $F[x]$ in $E[x]$. These relationships are represented symbolically by $F \prec E$ and $F[x] \prec E[x]$. Our point of view is that two isomorphic structures represent the same object expressed in two languages; the isomorphism supplies the translation. To give one example, real numbers can be represented by equivalence classes of Cauchy sequences of rational numbers and also by Dedekind cuts of rational numbers, and the two structures are isomorphic. In keeping with this point of view, and in order to simplify notation, we will write $F \subseteq E$ instead of $F \prec E$ and $F[x] \subseteq E[x]$ instead of $F[x] \prec E[x]$.

Definition: Let F and E be fields with $F \subseteq E$. An element $a \in E$ is said to be algebraic over F if there is a nonzero polynomial $p(x) \in F[x]$ such that $p(a) = 0$. We will say that a is algebraic of degree d over F when d is the smallest degree of all such polynomials. If $a \in E$ is not algebraic over F we say that a is transcendental over F.

Example: Let $p(x) = x^2 - 2 \in \mathbb{Q}[x]$. Then $p(\sqrt{2}) = 0$, therefore $\sqrt{2}$ is algebraic of degree $d \leq 2$ over $\mathbb{Q}$. To show that $d = 2$, consider any $q(x) = ax + b \in \mathbb{Q}[x]$ where $a \neq 0$. Then $q(\sqrt{2}) \neq 0$, otherwise $\sqrt{2} = -\frac{b}{a} \in \mathbb{Q}$. Hence $d = 2$.

Example: Let F be a field and let $f(x)$ be a non-zero polynomial in $F[x]$ with irreducible factor $p(x)$. Set $E = F[x]/(p(x))$ and $\beta = x + (p(x))$. Since

$p(\beta) = 0$, β is algebraic of degree $d \leq \deg p(x)$ over F. We will see below that $d = \deg p(x)$.

Example: Let E be the quotient field of $\mathbb{Q}[x]$. Then $\mathbb{Q} \subseteq E$. The element $x \in E$ is not algebraic over $\mathbb{Q}$: $p_0 + p_1 x + \cdots + p_k x^k = 0$ is not possible for a non-zero polynomial in $\mathbb{Q}[x]$. Hence x is transcendental over $\mathbb{Q}$.

Example: It can be shown that the real number e is transcendental over $\mathbb{Q}$ (Herstein, Topics in Algebra, Second Edition, 1975, Wiley, pp. 216 – 219).

Theorem: Let $F \subseteq E$ be fields, let $a \in E$ be algebraic over F, and let $p(x) \in F[x]$ be a monic polynomial of least degree such that $p(a) = 0$. Then:

(i) For each $f(x) \in F[x]$, $f(a) = 0$ if and only if $p(x)|f(x)$.

(ii) $p(x)$ is unique.

(iii) $p(x)$ is irreducible.

(iv) If $f(x) \in F[x]$ is monic and irreducible and $f(a) = 0$ then $f(x) = p(x)$.

Proof: (i) Suppose $f(a) = 0$. Write $f(x) = p(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg p(x)$. Then $r(a) = 0$, therefore $r(x) = 0$.

(ii) If $q(x)$ is a monic polynomial of least degree such that $q(a) = 0$, then $p(x)|q(x)$, and since they have the same degree we must have $q(x) = \alpha p(x)$ for some $\alpha \in F$. Since both polynomials are monic, $\alpha = 1_F$ and $q(x) = p(x)$.

(iii) Suppose $p(x) = f(x)g(x)$. Then $f(a) = 0$ or $g(a) = 0$, which implies that $p(x)|f(x)$ or $p(x)|g(x)$, which implies that $f(x)$ or $g(x)$ is an associate of $p(x)$. Hence $p(x)$ is irreducible.

(iv) Write $f(x) = p(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg p(x)$. Then $r(a) = 0$, therefore $f(x) = p(x)q(x)$. Since $f(x)$ is irreducible, $f(x)$ and $p(x)$ are associates. Since $f(x)$ is monic, $f(x) = p(x)$.

Definition: Let $F \subseteq E$ and let $a \in E$ be algebraic over F. The minimal polynomial of a is the unique monic polynomial $p(x)$ of least degree such that $p(a) = 0$.

Example: Let $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. Since $p(x)$ is monic and irreducible in $\mathbb{Q}[x]$ and $p(\sqrt[3]{2}) = 0$, $p(x)$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ and $\sqrt[3]{2}$ is algebraic of degree 3 over $\mathbb{Q}$.

Example: Let F be a field and let $f(x)$ be a non-zero polynomial in $F[x]$ with monic irreducible factor $p(x)$. Set $E = F[x]/(p(x))$ and $\beta = x + (p(x))$.

Since $p(\beta) = 0 + (p(x))$, β has minimal polynomial $p(x)$ and β is algebraic of degree $\deg p(x)$ over F.

Definition: Let $K \subseteq F$. Then $[F : K]$ denotes the dimension of F as a vector space over K.

Example: $\mathbb{C}$ is a field extension of $\mathbb{R}$ with basis $\{1, i\}$, hence $[\mathbb{C} : \mathbb{R}] = 2$.

Definition: Let $F \subseteq E$ be fields and let $a \in E$ be algebraic over F. We define $F[a]$ to be the set of all polynomials in a with coefficients in F. This is a field isomorphic to $F[x]/(p(x))$, where $p(x)$ is the minimal polynomial of a over F. $F[a]$ is called a simple extension of F.

Theorem: If a is algebraic of degree d over F then a basis for $F[a]$ over F is $\{1, a, \cdots, a^{d-1}\}$ and $[F[a] : F] = d$.

Proof: We have $F[x]/(p(x)) \cong F[a]$, where $p(x)$ is the minimal polynomial for a over F. The isomorphism maps $x^n + (p(x))$ to a^n for each non-negative integer n. Since $F[x]/(p(x))$ has basis

$$\{1 + (p(x)), x + (p(x)), \ldots, x^{d-1} + (p(x))\}$$

over F, where $d = \deg p(x)$, a basis for $F[a]$ is

$$\{1, a, \ldots, a^{d-1}\}.$$

Example: Since the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$, the field $\mathbb{Q}[\sqrt{2}]$ has basis $\{1, \sqrt{2}\}$ and $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. Every element in $\mathbb{Q}[\sqrt{2}]$ can be expressed uniquely in the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$.

Example: Since the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$, the field $\mathbb{Q}[\sqrt[3]{2}]$ has basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ and $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$. Every element in $\mathbb{Q}[\sqrt[3]{2}]$ can be expressed uniquely in the form $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ with $a, b, c \in \mathbb{Q}$.

Theorem: Assume $F \subseteq E \subseteq L$ is a tower of fields. Assume further that $[E : F] = m$ and $[L : E] = n$. Then $[L : F] = mn$.

Proof: Assume that E is generated by $X = \{e_1, \ldots, e_m\}$ over F and that L is generated by $Y = \{l_1, \ldots, l_n\}$ over E. This means that every element $e \in E$ can be expressed in the form

$$e = f_1 e_1 + \cdots + f_m e_m$$

for some choice of $f_1, \ldots, f_m \in F$ and every element $l \in L$ can be expressed in the form

$$l = e_1 l_1 + \cdots + e_n l_n$$

for some choice of $e_1, \ldots, e_n \in E$. Now let us take this expression for l but write

$$e_1 = f_{11} e_1 + f_{12} e_2 + \cdots + f_{1m} e_m$$

$$e_2 = f_{21} e_1 + f_{22} e_2 + \cdots + f_{2m} e_m$$

$$\cdots$$

$$e_n = f_{n1} e_1 + f_{n2} e_2 + \cdots + f_{nm} e_m.$$

Then we have

$$l = \sum_{i=1}^{n} e_i l_i = \sum_{i=1}^{n} \sum_{j=1}^{m} f_{ij} l_i e_j.$$

Therefore L is spanned by $Z = \{l_i e_j : i \leq n, j \leq m\}$ over F. Note that $|Z| = mn$. To finish the proof we must show that the elements in Z are linearly independent over F.

Suppose that

$$\sum_{i=1}^{n} \sum_{j=1}^{m} f_{ij} e_j l_i = 0.$$

Since the elements in Y are linearly independent over E, this forces

$$\sum_{j=1}^{m} f_{ij} e_j = 0$$

for each $i \leq n$. Since the elements in X are linearly independent over F, this forces

$$f_{i1} = f_{i2} = \cdots = f_{im} = 0$$

for each $i \leq n$. Hence each $f_{ij} = 0$, and Z is a basis for L over F.

Example: we have

$$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2.$$

We will show that

$$[\mathbb{Q}[\sqrt{2}][\sqrt[3]{5}] : \mathbb{Q}[\sqrt{2}]] = 3.$$

By Theorem 4.1, this will imply

$$[\mathbb{Q}[\sqrt{2}][\sqrt[3]{5}] : \mathbb{Q}] = 6.$$

Note that $\sqrt[3]{5}$ is a root of $x^3 - 5$ in $\mathbb{Q}[\sqrt{2}][x]$. To show that $x^3 - 5$ is irreducible in $\mathbb{Q}[\sqrt{2}][x]$, we will demonstrate that $x^3 - 5$ does not have a root in $\mathbb{Q}[\sqrt{2}]$. The only root is $\sqrt[3]{5}$. Suppose that

$$\sqrt[3]{5} = p + q\sqrt{2}$$

where $p, q \in \mathbb{Q}$. Cubing both sides and simplifying, this implies

$$5 = (p^3 + 6pq^2) + (3p^2q + 2q^3)\sqrt{2}.$$

To avoid the conclusion that $\sqrt{2} \in \mathbb{Q}$, we must have

$$3p^2q + 2q^3 = 0$$

$$p^3 + 6pq^2 = 5.$$

The first equation factors as

$$q(3p^2 + 2q^2) = 0.$$

Therefore $q = 0$ or $3p^2 + 2q^2 = 0$. We will show that either condition leads to a contradiction.

Suppose $q = 0$. Then $p^3 = 5$. Writing $p = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ are relatively prime integers, we have $\frac{a^3}{b^3} = 5$ or $a^3 = 5b^3$. This implies $5|a^3$, and since 5 is a prime number, $5|a$. Substituting, we have $125 = 5b^3$ or $25 = b^3$. This implies $5|b^3$, which implies $5|b$. Contradiction, since a and b are relatively prime. For another proof that $p^3 \neq 5$ for any rational number p, note that $x^3 - 5$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion. Hence it has no roots in $\mathbb{Q}$.

Suppose $3p^2 + 2q^2 = 0$. This implies $p = q = 0$, which contradicts $p^3 + 6pq^2 = 5$.

Therefore $x^3 - 5$ is irreducible in $\mathbb{Q}[\sqrt{2}][x]$ and

$$[\mathbb{Q}[\sqrt{2}][\sqrt[3]{5}] : \mathbb{Q}] = 6.$$

Another proof that $[\mathbb{Q}[\sqrt{2}][\sqrt[3]{5}] : \mathbb{Q}] = 6$: Since $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$ and $[\mathbb{Q}[\sqrt[3]{5}] : \mathbb{Q}] = 3$ and these are both subfields of $\mathbb{Q}[\sqrt{2}][\sqrt[3]{5}]$,

$$6|[\mathbb{Q}[\sqrt{2}][\sqrt[3]{5}] : \mathbb{Q}].$$

But $[\mathbb{Q}[\sqrt{2}][\sqrt[3]{5}] = \text{span}(1, \sqrt{2}, \sqrt[3]{5}, \sqrt{2}\sqrt[3]{5}, \sqrt[3]{25}, \sqrt{2}\sqrt[3]{25})$, therefore

$$[\mathbb{Q}[\sqrt{2}][\sqrt[3]{5}] : \mathbb{Q}] \leq 6.$$

Note also that this field contains $\sqrt{2}\sqrt[3]{5}$, and the minimal polynomial for this is $x^6 - 200$, therefore

$$\mathbb{Q}[\sqrt{2}][\sqrt[3]{5}] = \mathbb{Q}[\sqrt{2}\sqrt[3]{5}].$$

Theorem: If $F \subseteq E$ and $[E : F] = n$ then every $a \in E$ satisfies a polynomial of degree $\leq n$ in $F[x]$.

Proof: Let $a \in E$ be given. Since $[E : F] = n$, any $n + 1$ elements in E are linearly dependent over F. In particular, the elements $1, a, \ldots, a^n$ are linearly dependent, so there are coefficients $f_0, f_1, \ldots, f_n$, not all zero, such that $f_0 + f_1 a + \cdots + f_n a^n = 0$. Hence a is a root of $f_0 + f_1 x + \cdots + f_n x^n$.

Theorem: Let $F \subseteq E$ be a field extension. If $e_1, e_2 \in E$ are both algebraic over F then so are $e_1 e_2$ and $e_1 + e_2$.

Proof: Suppose that e_1 is algebraic of degree d_1 over F and e_2 is algebraic of degree d_2 over F. Then e_2 is algebraic of degree $d_2' \leq d_2$ over $F[e_1]$. Hence $[F[e_1][e_2] : F] = d_1 d_2'$. Write $d_1 d_2' = n$. Since $F[e_1][e_2]$ has a basis of size n over F, any $n + 1$ elements in $F[e_1][e_2]$ are linearly dependent over F. So if $a \in F[e_1][e_2]$ then the elements $1, a, a^2, \ldots, a^n$ are linearly dependent over F, i.e. there exist $f_0, f_1, \ldots, f_{n'}$, not all zero, such that

$$f_0 1 + f_1 a + \cdots + f_n a^n = 0.$$

Therefore a is a root of the nonzero polynomial $f(x) = f_0 + f_1 x + \cdots + f_n x^n \in F[x]$ and is algebraic over F. Both of the elements $e_1 e_1$ and $e_1 + e_2$ belong to $F[e_1][e_2]$, hence they are both algebraic over F.

The previous theorem implies that the set of elements in E which are algebraic over F form a field: If e is algebraic then so is $-e$. If $e \neq 0$ is a root of $\sum_{k=0}^{n} p_k x^k$ then e^{-1} is a root of $\sum_{k=0}^{n} p_{n-k} x^k$.

Example: Since $\sqrt{2}$ and $\sqrt[3]{5}$ are algebraic of degree 2 and 3, respectively, over $\mathbb{Q}$, in principle $\sqrt{2}\sqrt[3]{5}$ and $\sqrt{2}+\sqrt[3]{5}$ should be algebraic of degree ≤ 6 over $\mathbb{Q}$. The method for finding polynomials whose roots they are is to write out the zeroth through the sixth powers of each element and find a rational linear dependence among them. We do that as follows:

Using Mathematica, the successive powers of $a = \sqrt{2}\sqrt[3]{5}$ are

$$a^0 = 1$$

$$a^1 = 2^{1/2} \cdot 5^{1/3}$$

$$a^2 = 2 \cdot 5^{2/3}$$

$$a^3 = 10 \cdot 2^{1/2}$$

$$a^4 = 20 \cdot 5^{1/3}$$

$$a^5 = 20 \cdot 2^{1/2} \cdot 5^{2/3}$$

$$a^6 = 200$$

A polynomial in $\mathbb{Q}[x]$ satisfied by $2^{1/2}\sqrt[3]{5}$ is $x^6 - 200$.

Using Mathematica, the successive powers of $a = \sqrt{2} + \sqrt[3]{5}$ are

$$a^0 = 1$$

$$a^1 = 2^{1/2} + 5^{1/3}$$

$$a^2 = 2 + 2 \cdot 2^{1/2} \cdot 5^{1/3} + 5^{2/3}$$

$$a^3 = 5 + 2 \cdot 2^{1/2} + 6 \cdot 5^{1/3} + 3 \cdot 2^{1/2} \cdot 5^{2/3}$$

$$a^4 = 4 + 20 \cdot 2^{1/2} + 5 \cdot 5^{1/3} + 8 \cdot 2^{1/2} \cdot 5^{1/3} + 12 \cdot 5^{2/3}$$

$$a^5 = 100 + 4 \cdot 2^{1/2} + 20 \cdot 5^{1/3} + 25 \cdot 2^{1/2} \cdot 5^{1/3} + 5 \cdot 5^{2/3} + 20 \cdot 2^{1/2} \cdot 5^{2/3}$$

$$a^6 = 33 + 200 \cdot 2^{1/2} + 150 \cdot 5^{1/3} + 24 \cdot 2^{1/2} \cdot 5^{1/3} + 60 \cdot 5^{2/3} + 30 \cdot 2^{1/2} \cdot 5^{2/3}$$

Writing these elements as row vectors and putting them all into a matrix A, we obtain

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 & 1 & 0 \\ 5 & 2 & 6 & 0 & 0 & 3 \\ 4 & 20 & 5 & 8 & 12 & 0 \\ 100 & 4 & 20 & 25 & 5 & 20 \\ 33 & 200 & 150 & 24 & 60 & 30 \end{pmatrix}.$$

We wish to find a rational linear dependence relation among the rows. This is equivalent to finding a non-zero solution to the equation

$$\begin{bmatrix} f_0 & f_1 & f_2 & f_3 & f_4 & f_5 & f_6 \end{bmatrix} A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Mathematica yields the solution

$$\begin{bmatrix} f_0 & f_1 & f_2 & f_3 & f_4 & f_5 & f_6 \end{bmatrix} = \begin{bmatrix} 17 & -60 & 12 & -10 & -6 & 0 & 1 \end{bmatrix}.$$

Therefore a polynomial in $\mathbb{Q}[x]$ satisfied by $\sqrt{2} + \sqrt[3]{5}$ is

$$f(x) = 17 - 60x + 12x^2 - 10x^3 - 6x^4 + x^6.$$

I checked this in Mathematica and it works!!!

Definition: Let $K \subseteq F$ be a field extension. The Galois group of F over K is $Gal_K(F)$, the set of field automorphisms $f : F \to F$ that fix K.

Theorem: Let $f \in Gal_K(F)$. Let $u \in F$ be algebraic over K. Then $p(x)$ is the minimal polynomial of u over K if and only if $p(x)$ is the minimal polynomial of $f(u)$ over K.

Proof: Let $p(x)$ be the minimal polynomial of $f(u)$ over K. Then $0 = f(p(u)) = p(f(u)$, hence $p(x)$ is the minimal polynomial of $f(u)$ over K. Conversely, let $q(x)$ be the minimal polynomial of $f(u)$ over K. Then $f(q(u)) = q(f(u)) = 0$, therefore $q(u) = 0$, therefore $q(x)$ is the minimal polynomial of u over K.

Corollary: Let $K \subseteq F$ be fields and let $u \in F$ be algebraic over K with minimal polynomial $p(x)$. If $p(x)$ has k distinct roots in F then $|Gal_K(K(u))| \leq k$.

Proof: Let $p(x)$ be the minimal polynomial of u. Let $u_1, \ldots, u_k$ be the distinct roots of $p(x)$ in F. Since $f(u) \in \{u_1, \ldots, u_k\}$ for each $f \in Gal_K(K(u))$, and since each such f is determined by $f(u)$, $Gal_K(K(u)) \leq k$.

Example: Let $f \in Gal_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}])$. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$, which has two distinct roots in $\mathbb{Q}[\sqrt{2}]$: $\sqrt{2}$ and $-\sqrt{2}$. Hence $|Gal_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}])| \leq 2$. The mappings $a + b\sqrt{2} \mapsto a + b\sqrt{2}$ and $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ are both elements of $Gal_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}])$. Hence $|Gal_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}])| = 2$ and $Gal_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}]) \cong \mathbb{Z}_2$.

Definition: Let $K \subseteq F$ be a field extension. Then $u, v \in F$ are conjugates if they have the same minimal polynomial.

Of theoretical interest:

Definition: Let $K \subseteq F$ be fields. F is said to be algebraic over K if every $f \in F$ is algebraic over K.

Theorem: If $K \subseteq F$ is an algebraic extension and $F \subseteq E$ is an algebraic extension then $K \subseteq E$ is an algebraic extension.

Proof: Let $e \in E$ be given. Let $f(x)$ be minimal polynomial of e over F. Then $f(x)$ is a polynomial satisfied by e over $K[f_0, \ldots, f_n]$, where $f_0, f_1, \ldots, f_n$ are the coefficients of $f(x)$. Since each of the f_i are algebraic over K, $[K[f_0, \ldots, f_n] : K] = m$ for some m. We also have $[K[f_0, \ldots, f_n][e] : K[f_0, \ldots, f_n]] \leq n$, therefore $[K[f_1, \ldots, f_n][e] : K] \leq mn$. This implies that e satisfies a polynomial of degree $\leq mn$ over K.

Splitting Fields and Normal Extensions

We know how to construct roots of polynomials. Once a polynomial $f(x) \in K[x]$ factors as $f(x) = (x - u)g(x)$ in $F[x]$, where $K \subseteq F$, we can continue to find extension fields for the other roots of $f(x)$ until we have an extension field $K \subseteq E$ that contains all the roots of $f(x)$. This gives rise the the following definition:

Definition: Let K be a field and let $f(x) \in K[x]$ be given. A splitting field for $f(x)$ over K is a field of the form $K[S]$, where S is the set of roots of $f(x)$ in some field F over which $f(x)$ factors into linear factors.

Theorem: If F is a splitting field of $f(x)$ over K and $K \subseteq L \subseteq F$ then F is a splitting field of $f(x)$ over L.

Proof: Write $F = K[S]$ where S contains the roots of $f(x) \in K[x]$. Then $F = K[S]$, hence $F = L[S]$. Since $f(x) \in L[x]$, F is the splitting field of $f(x)$ over L.

Theorem: Let F be a splitting field of $f(x) \in K[x]$ and let F' be a splitting field of $f'(x) \in K'[x]$, and assume $K \cong K'$ by an isomorphism that sends $f(x)$ to $f'(x)$. Then $F \cong F'$ by an isomorphism that sends K to K' and $[F : K] = [F' : K']$.

Proof: By induction on $[F : K]$. If $[F : K] = 1$ then $F = K$. Hence $f(x)$ splits in $K[x]$, hence $f'(x)$ splits in $K'[x]$, hence $F' = K'$, hence $[F' : K'] = 1$. Now consider $[F : K] > 1$. Let $p(x)$ be an irreducible factor of $f(x)$ of degree > 1. Then it has a root $u \in F$. We have $K[u] \cong K[x]/(p(x))$. We also

have $K[x] \cong K'[x]$, under which $p(x)$ gets mapped to $p'(x)$, which must be irreducible in $K'[x]$. Let u' be a root of $p'(x)$ in F', which must exist because $f'(x)$ splits in $F'[x]$ and $p'(x)$ is a divisor of $f'(x)$. Then $K'[u'] \cong K'[x]/(p'(x))$ and so $K[u] \cong K'[u']$ by an isomorphism that extends the isomorphism from K to K' and sends u to u'. In particular, $f(x)$ is sent to $f'(x)$, regarded as elements of $K[u][x]$ and $K'[u'][x]$. F is a splitting field of $f(x)$ over $K[u]$ and F' is a splitting field of $f'(x)$ over $K'[u']$. Since $[F : K[u]] < [F : K]$, by induction we can say that $F \cong F'$ by an isomorphism that sends K to K' and u to u' and $[F : K[u]] = [F' : K'[u']]$. Since $[K[u] : K] = [K'[u'] : K']$, we have $[F : K] = [F' : K']$.

Definition: A normal extension $K \subseteq F$ is one in which, for all irreducible $f(x) \in K[x]$, if $f(x)$ has a root in F then $f(x)$ splits in $F[x]$.

Note that all finite-dimensional normal field extensions are splitting fields. To see this, let $K \subseteq F$ be finite and normal. We can write $F = K[u_1, \cdots, u_n]$ since the extension is finite-dimensional. For each i let $f_i(x) \in F[x]$ be the irreducible polynomial of u_i. By normality, all the roots of $f_i(x)$ belong to F for each i. It is certainly true that $F = K[S]$ where S is the set of roots of $f_1(x) \cdots f_n(x)$, therefore F is splitting field of $f_1(x) \cdots f_n(x)$.

Theorem: All splitting fields are normal extension fields.

Proof: Let K be a field, let $f(x) \in K[x]$, and let $K[S]$ be a splitting field of $f(x)$ over K, where S is the set of roots of $f(x)$. Let $p(x)$ be an irreducible polynomial with a root $u \in K[S]$. We wish to show that $p(x)$ splits completely in $K[S][x]$, where S is the set of roots of $f(x)$ in F. Let E be a splitting field over $K[S]$ of $p(x)$. Let $v \neq u$ be a root of $p(x)$ in E. Then $K[S][u] = K[u][S]$ is a splitting field of $f(x)$ over $K[u]$ and $K[S][v] = K[v][S]$ is a splitting field of $f(x)$ over $K[v]$. Since $K[u] \cong K[v]$ by an isomorphism that fixes K and sends $f(x)$ to $f(x)$, $[K[S][u] : K[u]] = [K[S][v] : K[v]]$. This implies $[K[S][u] : K] = [K[S][v] : K]$. Dividing both sides by $[K[S] : K]$ yields $[K[S][u] : K[S]] = [K[S][v] : K[S]]$, and since $[K[S][u] : K[S]] = 1$, $[K[S][v] : K[S]] = 1$. This implies $v \in K[S]$.

Corollary [3.15]: If F is a finite field of characteristic p then $F = F_p[u]$ for some $u \in F$.

Proof: F is a vector space over the subfield $F_p = \{0, 1, \ldots, p-1\}$. Since $F^\times = \langle u \rangle$ for some $u \in F$, every element in F_p is a polynomial in u with coefficients in F_p.

Theorem [3.17]: Every finite field F with p^n elements is the splitting field of $x^{p^n} - x$.

Proof: Every element in F satisfies the polynomial, and since the degree of the polynomial is equal to the size of F, F is the complete set of roots of this polynomial. Since $F = F_p[F]$, F is the splitting field.

This implies that there is a unique finite field with p^n elements for each prime p and positive integer n (up to isomorphism).

Definition: A separable polynomial $f(x) \in K[x]$ is one that is irreducible and does not have a multiple root in any splitting field.

Theorem: In a field K of characteristic 0, all irreducible polynomials are separable.

Proof: Let $p(x)$ be irreducible in $K[x]$. We can assume without loss of generality that it is monic. If $K \subseteq F$ and $p(x) = (x-a)^2 q(x)$ in F then $p'(x) = 2(x-a)q(x) + (x-a)q'(x)$, therefore $p'(a) = 0$. Since $p(x)$ is the minimal polynomial of a in $K[x]$, $p(x)|p'(x)$. This implies $p'(x) = 0$, which is impossible in characteristic 0. Hence $p(x)$ is separable.

Note: We know that if F if a finite field with p^n elements then it is the splitting field of $x^{p^n} - x$. If we write $F = F_p[u]$ then the irreducible polynomial of u, $q(x)$, is a divisor of $x^{p^n} - x$. Since the latter has distinct roots, so does $q(x)$. Hence F is the splitting field of a separable polynomial.

Definition: Let $K \subseteq L$ be a finite-dimensional field extension. Write $L = K[u_1 \ldots, u_n]$. For each i let $f_i(x)$ be the minimal polynomial of u_i over K. Let F be a splitting field of $f(x) = f_1(x) \cdots f_n(x)$. F is called a normal closure of L over K.

Theorem: Let $K \cong K'$ be fields, let F be a normal closure of L over K, let F' be a normal closure of L' over K', and assume that $L \cong L'$ by an isomorphism that maps K onto K'. Then $F \cong F'$ by an isomorphism that maps K onto K'.

Proof: Assume that F is the splitting field of $f(x) = f_1(x) \cdots f_m(x)$ over K and F' is the splitting field of $f'(x) = f'_1(x) \cdots f'_n(x)$ over K'. The isomorphism that sends L to L' sends $f(x)$ to $\widetilde{f}(x) \in K'[x]$, and since each $f_i(x)$ has a root in L, each $\widetilde{f}_i(x)$ has a root in L'. Since F' is a normal extension, each $\widetilde{f}_i(x)$ splits in F', hence $\widetilde{f}(x)$ splits in F'. Therefore F' contains a splitting field F'_1 of $\widetilde{f}(x)$ over K'. Therefore $F \cong F'_1$ by an isomorphism that sends

K to K' and $[F : K] = [F'_1 : K']$. Hence $[F : K] \leq [F' : K']$. Similarly, we have $[F' : K'] \leq [F : K]$. Therefore $[F : K] = [F' : K']$, which implies $F' = F'_1 \cong F$ by an isomorphism that sends K to K'.

Corollary: If F and F' are normal closures of L over K then $F \cong F'$ by a K-automorphism.

The Fundamental Correspondence, pp, 110–149.

Definition [1.1]: Let $K \subseteq F$ be a field extension. Then $\mathrm{Gal}_K(F)$ is the set of K-automorphisms of F.

Lemma: Let $f \in \mathrm{Gal}_K(F)$. For each $u \in F$, u and $f(u)$ have the same minimal polynomial.

Proof: If $\sum_{i=0}^{n} k_i u^i = 0_F$ then $\sum_{i=0}^{n} k_i f(u)^i = f(\sum_{i=0}^{n} k_i u^i) = f(0_F) = 0_F$.

Lemma: Let $\alpha : K \cong K'$ be a field isomorphism. Let $K[u]$ be a finite-dimensional field extension of K with minimal polynomial $p(x) \in K[x]$. Let $p'(x) = \alpha(p(x))$ be the image of $p(x)$ in $K'[x]$ and let v be any root of $p'(x)$ in a splitting field of K'. The mapping $f : K[u] \to K'[v]$ via $f(g(u)) = g'(v)$ is an isomorphism which extends the one between K and K', where $g'(x) = \alpha(g(x))$.

Proof: $K[u] \cong K[x]/(p(x)) \cong K'[x]/(p'(x)) \cong K'[v]$.

Theorem: Let $F = K[u]$ be a finite-dimensional field extension of K. Let $p(x)$ be the minimal polynomial of u over K and let S be the set of roots of $p(x)$ in F. Then $\mathrm{Gal}_K(F) = \{f_v : v \in S\}$, where for each $v \in S$ we define $f_v : K[u] \to K[u]$ by $f_v(g(u)) = g(v)$.

Proof: Each f_v is a K-automorphism of F, and every K-automorphism of F must be of this form.

Example: Consider $K = \mathbb{Q}$ and $F = \mathbb{Q}[\sqrt[3]{2}]$. The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$ and the set of its roots is $S = \{\sqrt[3]{2}\}$. Hence $\mathrm{Gal}_K(F) = \{f_{\sqrt[3]{2}}\} = \langle e \rangle$.

Example: $K = \mathbb{Q}$, $F = \mathbb{Q}[\sqrt[3]{2}][i]$. Any $f \in \mathrm{Gal}_K(F)$ has to fix $K[\sqrt[3]{2}]$ and so is determined by where it maps i. Hence $\mathrm{Gal}_K(F) = \{f_i, f_{-i}\} = \langle f_{-i} \rangle \cong \mathbb{Z}_2$.

Example: Consider $K = \mathbb{Q}$ and $F = \mathbb{Q}[\sqrt{2}]$. The minimal polynomial of $\sqrt{2}$ is $x^2 - 2$ and $S = \{\sqrt{2}, -\sqrt{2}\}$. Hence $\mathrm{Gal}_K(F) = \{f_{\sqrt{2}}, f_{-\sqrt{2}}\} \cong \mathbb{Z}_2$.

Example: Consider $K = \mathbb{Q}[\sqrt{2}, \sqrt[3]{5}] = \mathbb{Q}[\sqrt{2}\sqrt[3]{5}]$. The minimal polynomial of $\sqrt{2}\sqrt[3]{5}$ is $x^6 - 200$ and $S = \{\sqrt{2}\sqrt[3]{5}, -\sqrt{2}\sqrt[3]{5}\}$, hence $\mathrm{Gal}_K(F) = \{f_{\sqrt{2}\sqrt[3]{5}}, f_{-\sqrt{2}\sqrt[3]{5}}\} \cong \mathbb{Z}_2$.

Another way to look at this: The minimal polynomial of $\sqrt[3]{5}$ is x^3-5 and its roots in K are $\{\sqrt[3]{5}\}$, hence $f(\sqrt[3]{5}) = \sqrt[3]{5}$. Writing $F = \mathbb{Q}[\sqrt[3]{5}][\sqrt{2}]$, any $f \in \mathrm{Gal}_K(F)$ is a member of $\mathrm{Gal}_{K[\sqrt[3]{5}]}(F)$, and since the minimal polynomial of $\sqrt{2}$ over $K[\sqrt[3]{5}]$ is x^2-2 with roots $\{\sqrt{2}, -\sqrt{2}\}$, $\mathrm{Gal}_K(F) = \mathrm{Gal}_{K[\sqrt{2}]}(F) = \{f_{\sqrt{2}}, f_{-\sqrt{2}}\} \cong \mathbb{Z}_2$.

Example: $K = \mathbb{Q}$, $F = \mathbb{Q}[\xi]$ where ξ is a primitive 5^{th} root of unity. It's minimal polynomial is $1 + x + x^2 + x^3$ and its roots are $\{\xi, \xi^2, \xi^3, \xi^4\}$, hence $\mathrm{Gal}_K(F) = \{f_\xi, f_{\xi^2}, f_{\xi^3}, f_{\xi^4}\} = \langle f_{\xi^3} \rangle \cong \mathbb{Z}_4$.

Example: Let $K = \mathbb{Q}$ and $F = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Since the minimal polynomial of $\sqrt{2}$ is $x^2 - 2$ and its roots in K are $\{\sqrt{2}, -\sqrt{2}\}$, any $f \in \mathrm{Gal}_K(F)$ satisfies $f(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$. Similarly, any $f \in \mathrm{Gal}_K(F)$ satisfies $f(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\}$. Since $f \in \mathrm{Gal}_K(F)$ is determined by $f(\sqrt{2})$ and $f(\sqrt{3})$,

$$o(\mathrm{Gal}_K(F)) \leq 4.$$

We will construct 4 distinct K-automorphisms of F.

We have $\mathrm{Gal}_K(K[\sqrt{2}]) = \{f_{\sqrt{2}}, f_{-\sqrt{2}}\}$. Since F is the splitting field of $K[\sqrt{2}]$, each $f \in \mathrm{Gal}_K(K[\sqrt{2}])$ extends to an isomorphism $\widehat{f}$ of F, which by construction is a K-automorphism. The choices for f are $\{f_{\sqrt{2}}, f_{-\sqrt{2}}\}$ and the choices for $\widehat{f}$ are $\{\widehat{f}_{\sqrt{3}}, \widehat{f}_{-\sqrt{3}}\}$ since the minimal polynomial of $\sqrt{3}$ over $K[\sqrt{2}]$ is $x^2 - 3$. So the four automorphisms are $f_{\sqrt{2},\sqrt{3}}, f_{-\sqrt{2},\sqrt{3}}, f_{\sqrt{2},-\sqrt{3}}, f_{-\sqrt{2},-\sqrt{3}}$. Since these commute and each has order 2, $\mathrm{Gal}_K(F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Another solution: $F = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ and $\sqrt{2}+\sqrt{3}$ has minimal polynomial x^4-10x^2+1, the roots of which are $\{\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}+\sqrt{3}, -\sqrt{2}-\sqrt{3}\}$. Therefore $\mathrm{Gal}_K(F) = \{f_{\sqrt{2}+\sqrt{3}}, f_{\sqrt{2}-\sqrt{3}}, f_{-\sqrt{2}+\sqrt{3}}, f_{-\sqrt{2}-\sqrt{3}}\}$. These commute and have order 2 each, therefore $\mathrm{Gal}_K(F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example: $K = \mathbb{Q}$, $F = \mathbb{Q}[\sqrt[4]{2}, i]$. Minimal polynomials: x^4-2, x^2+1. Roots in F: $\{w, -w, wi, -wi\}$ and $\{i, -i\}$. The minimal polynomial of i over $\mathbb{Q}[\sqrt[4]{2}]$ is $x^2 + 1$. So there are at most 8 K-automorphisms of F. We construct 8 as follows: There are two K-automorphisms from $K[w]$ to $K[w]$: $f(w) \mapsto f(w)$ and $f(w) \mapsto f(-w)$. F is a splitting field of $x^2 + 1$ over $K[w]$ and $x^2 + 1$ is the minimal polynomial of i over $K[w]$, hence the K-automorphisms of $K[w]$ lift to $\{\widehat{f}_i, \widehat{f}_{-i}\}$. Hence we obtain 4 K-automorphisms of F: $(w, i) \mapsto (w, i), (w, i) \mapsto (w, -i), (w, i) \mapsto (-w, i), (w, i) \mapsto (-w, -i)$. There are two isomorphisms between $K[w]$ and $K[wi]$: $f(w) \mapsto f(wi)$ and $f(w) \mapsto f(-wi)$. Since F is a splitting field of $x^2 + 1$ over $K[w]$ and F is a splitting field of

x^2+1 over $K[wi]$ and x^2+1 is the minimal polynomial of i over both $K[w]$ and $K[wi]$, these two isomorphisms lift to K-automorphisms of F whereby $i \mapsto i$ and $i \mapsto -i$. Hence we obtain 4 more K-automorphisms of F: $(w,i) \mapsto (wi,i), (w,i) \mapsto (wi,-i), (w,i) \mapsto (-wi,i), (w,i) \mapsto (-wi,-i)$.

One can check that $(w,i) \mapsto (wi,i)$ has order 4 and that $(w,i) \mapsto (w,-i)$ has order 2. Call these S and T, respectively. We have $TS : (w,i) \mapsto (wi,i) \mapsto (-wi,-i)$ and $S^3T : (w,i) \mapsto (w,-i) \mapsto (-wi,-i)$, therefore $TS = S^3T$. Hence $\mathrm{Gal}_K(F) \cong D_4$.

There is a theme developing here: To construct elements in $\mathrm{Gal}_K(F)$, find two isomorphic subfields L_1 and L_2 such that every $f \in \mathrm{Gal}_K(F)$ maps L_1 into L_2. Assuming F is a splitting field of L_1 and a splitting field of L_2 and $F = L_1[u]$ and $F = L_2[v]$ where u has minimal polynomial $p(x)$ over L_1 and v has minimal polynomial $p'(x)$ over L_2 and the isomorphism between L_1 and L_2 sends $p(x)$ to $p'(x)$. Then we can extend every K-fixing isomorphism between L_1 and L_2 to a K-automorphism of F, and we know exactly what the latter are.

Example: $K = \mathbb{Q}$, $F = K[w,\xi]$ where $w = \sqrt[5]{2}$ and $\xi = e^{\frac{2\pi i}{5}}$. Minimal polynomials over K: x^5-2 and $1+x+x^2+x^3+x^4$. Since these degrees are relatively prime, x^5-2 is the minimal polynomial of w over $K[\xi]$ and $1+x+x^2+x^3+x^4$ is the minimal polynomial of ξ over $K[w]$ (see Exercise [2.6], p. 98). The roots of x^5-2 are $w, w\xi, w\xi^2, w\xi^3, x\xi^4$, and for each u on this list, $K[w] \cong K[u]$ by an isomorphism that fixes K. F is a splitting field of $1+x^2+x^3+x^4$ over each of these fields, and each of these isomorphisms extends to a K-automorphism of F in which ξ gets mapped to one of the roots $\{\xi, \xi^2, \xi^3, \xi^4\}$ of $1+x^2+x^3+x^4$. Hence we can construct 20 elements in $\mathrm{Gal}_F(K)$. There can't be any more than these since any $f \in \mathrm{Gal}_K(F)$ is determined by the images of w and ξ, and the automorphisms we have constructed account for all the possibilities.

Let $K \subseteq F$ be fields. For every subgroup H of $\mathrm{Gal}_K(H)$ we can identify a field H' such that $K \subseteq H' \subseteq F$:

$$H' = \{u \in F : h(u) = u \text{ for all } h \in H\}.$$

To see this is a field, let $u, v \in H'$ and $h \in H$ be given. Then $h(u+v) = h(u)+h(v) = u+v$, $h(-u) = -h(u) = -u$, $h(uv) = h(u)h(v) = uv$, and, if $u \neq 0$, $h(u^{-1}) = h(u)^{-1} = u^{-1}$. Hence $u+v, -u, uv, u^{-1} \in H'$.

For every field L such that $K \subseteq L \subseteq F$ we can identify a subgroup L' of $\mathrm{Gal}_K(F)$: $L' = \mathrm{Gal}_L(F)$.

Example: Let $K = \mathbb{Q}, F = \mathbb{Q}[\sqrt[3]{2}, i]$. We have

$$K' = \mathrm{Gal}_K(F)$$

$$K[\sqrt[3]{2}]' = \mathrm{Gal}_K(F)$$

$$(\mathrm{Gal}_K(F))' = K[\sqrt[3]{2}].$$

$$K'' = K[\sqrt[3]{2}].$$

Hence the mapping $L \mapsto L'$ is not necessarily injective and $L \neq L''$ is possible.

The statements in the following theorem follow from elementary set theory:

Theorem: Let $K \subseteq F$.

(a) If $K \subseteq L_1 \subseteq L_2 \subseteq F$ then $L_2' \subseteq L_1'$.

(b) If $\langle e \rangle \subseteq H_1 \subseteq H_2 \subseteq \mathrm{Gal}_K(F)$ then $H_2' \subseteq H_1'$.

(c) If $\langle H \subseteq \mathrm{Gal}_K(F)$ then $H'' \subseteq H$.

(d) If $K \subseteq L \subseteq F$ then $L \subseteq L''$.

(e) $L''' = L'$ and $H''' = H'$.

Definition: Let $K \subseteq F$ be given. A subgroup H of $\mathrm{Gal}_K(F)$ is closed if $H = H''$. An intermediate field L is closed in F over K if $L = L''$.

Example: $\{e, T\}$ is a closed subgroup of $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\sqrt[4]{2}, i])$ and $K[\sqrt[4]{2}]$ is closed in $\mathbb{Q}[\sqrt[4]{2}, i]$ over $\mathbb{Q}$.

Given a field extension $F \subseteq L \subseteq K$, L'' consists of the field elements fixed by all $f \in \mathrm{Gal}_L(F)$. Given a subgroup H of $\mathrm{Gal}_K(F)$, H'' consists of all K-automorphisms of F that fix field elements that are fixed by every $h \in H$.

Theorem: Let $K \subseteq F$ be a finite-dimensional field extension. Then

$$o(\mathrm{Gal}_K(F)) \leq [F : K]$$

and

(a) If $K \subset L \subseteq M \subseteq F$ then $(L' : M') \leq [M : L]$.

(b) If $\langle e\rangle < H < J < \mathrm{Gal}_K(F)$ then $[H' : J'] \leq (J : H)$.

(c) If K is closed in F then $o(\mathrm{Gal}_K(F)) = [F : K]$, all subgroups of $\mathrm{Gal}_K(F)$ are closed in $\mathrm{Gal}_K(F)$, the inequalities in (a) and (b) are equalities, and the priming operation produces a one-to-one correspondence between subfields L such that $K \subseteq L \subseteq F$ and subgroups of $\mathrm{Gal}_K(F)$.

(d) K is closed in F if and only if $o(\mathrm{Gal}_K(F)) = [F : K]$.

Proof: (a) Consider any subfield $K \subseteq L \subseteq F$ where $L \neq F$. Choose any $u \in F \backslash L$. We claim that $(L' : L[u]') \leq [L[u] : L]$. To see this, let $L[u]'f$ and $L[u]'g$ be distinct cosets of $L[u]'$ in L', where $f, g \in L'$. Then $fg^{-1} \notin L[u]'$, hence $f(u) \neq g(u)$. Since $f(u)$ and $g(u)$ are distinct roots of the minimal polynomial $p(x)$ of u over $L[x]$,

$$(L' : L[u]') \leq \deg p(x) = [L[u] : L].$$

To prove (a) in general, observe that since $[M : L]$ is finite there is a chain of simple extensions

$$L = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n = M.$$

This yields

$$M' = L'_n \subseteq \cdots \subseteq L'_0 = L.$$

We have

$$(L'_i : L'_{i+1}) \leq [L_{i+1} : L]$$

for $0 \leq i < n$, hence

$$(L' : M') = (L'_0 : L'_1) \cdots (L'_{n-1} : L'_n) \leq [L_1 : L_0] \cdots [L_n : L_{n-1}] = [M : L].$$

In particular, since $K' = \mathrm{Gal}_K(F)$ and $F' = \langle e\rangle$, we have $o(\mathrm{Gal}_K(F)) = (\mathrm{Gal}_K(F) : \langle e\rangle) \leq [F : K]$.

(b) Now consider $\langle e\rangle < H < J < \mathrm{Gal}_K(F)$. We have $K \subseteq J' \subseteq H' \subseteq \mathrm{Gal}_K(F)$. Let $\{u_1, \ldots, u_n\}$ be a basis for H' over J'. Let $j_1H, \ldots, j_mH$ be the distinct cosets of H in J. We wish to show $n \leq m$. Form the m vectors

$$v_1 = \begin{bmatrix} j_1(u_1) \\ \vdots \\ j_m(u_1) \end{bmatrix}, \cdots, v_n = \begin{bmatrix} j_1(u_n) \\ \vdots \\ j_m(u_n) \end{bmatrix}.$$

It will suffice to show that $v_1, \ldots, v_n$ are linearly independent over F.

Every element in $j_i H$ sends u_i to the same element. Since $j \in J$ produces a permutation $jj_1H, \ldots, jj_mH$ of the cosets $j_1H, \ldots, jj_mH$, j permutes the entries of each v_i. Suppose $v_1, \ldots, v_n$ are linearly dependent. Then there is a non-trivial annihilating linear combination

$$a_1v_1 + \cdots + a_nv_n = 0$$

with maximum number of zero coefficients. We can assume without loss of generality that $a_1 = 1$ and $j_1 = e$. By linear independence of $\{u_1, \ldots, u_n\}$ over J' we must have $a_i \notin J'$ for some $i \geq 2$. Without loss of generality $a_2 \notin J'$. This implies that there is some $j \in J$ such that $j(a_2) \neq a_2$. Applying j to our annihilating linear combination yields

$$a_1v_1 + j(a_2)v_2 + \cdots + j(a_n)v_n = 0.$$

Subtracting the two equations we obtain an annihilating linear combination with more zero coefficents. Contradiction. Hence the v_i are linearly independent, $n \leq m$, and $[H' : J'] \leq (J : H)$.

(c) Assume that $K'' = K$. Let $K \subseteq L \subseteq F$ be given. Then we have

$$[L'' : K] = [L'' : K''] \leq (K' : L') \leq [L : K] \leq [L'' : K],$$

therefore $[L'' : K] = [L : K]$, therefore $L = L''$. Now let H be a subgroup of $\mathrm{Gal}_K(F)$. Since $\langle e \rangle'' = F$, we have

$$(H'' : \langle e \rangle) = (H'' : \langle e \rangle'') \leq [\langle e \rangle' : H'] \leq (H : \langle e \rangle) \leq (H'' : \langle e \rangle),$$

therefore $(H'' : \langle e \rangle) = (H : \langle e \rangle)$, hence $H'' = H$.

(d) If K is closed in F then by (c) we have $[F : K] = o(\mathrm{Gal}_K(F))$. Conversely, if $[F : K] = o(\mathrm{Gal}_K(F))$ then, since K'' is closed in F,

$$[F : K''] = o(\mathrm{Gal}_{K''}(F)) = o(\mathrm{Gal}_K(F)) = [F : K],$$

therefore $K = K''$, therefore K is closed in F.

Theorem: Let $K \subseteq F$ be a finite-dimensional normal extension.

(1) If H is a normal subgroup of $\mathrm{Gal}_K(F)$ then H' is a normal extension of K.

(2) If L is a normal intermediate field then $f(L) \subseteq L$ for all $f \in \mathrm{Gal}_K(F)$, hence $\mathrm{Gal}_K(F)/\mathrm{Gal}_L(F)$ is isomorphic to a subgroup of $\mathrm{Gal}_K(L)$ via the mapping $f \mapsto f|L$ and $o(\mathrm{Gal}_K(F)) \leq o(\mathrm{Gal}_K(L))o(\mathrm{Gal}_L(F))$.

Proof: (1) Let H be a normal subgroup of $\mathrm{Gal}_K(F)$. Let $p(x)$ be irreducible in $K[x]$ and let u be a root of $p(x)$ in H'. We wish to show that $p(x)$ splits in $H'[x]$. By normality of F over K, $p(x)$ splits in $F[x]$. Let v be any of its roots. Since F is a splitting field of K, we can lift the an isomorphism from $K[u]$ to $K[v]$ to a K-automorphism f of F which satisfies $f(u) = v$. Since H' is normal we have $f^{-1}hf \in H'$, hence $f^{-1}hf(u) = u$, hence $h(v) = v$. This places v in H'.

(2) Assume that L is normal over K. Let $f \in \mathrm{Gal}_K(L)$. Then $f(L) \subseteq L$: let $u \in L$ be given. Let $p(x)$ be the minimal polynomial of u over K. Then $f(u)$ is a root of $p(x)$ hence belongs to L. Therefore $f|L \in \mathrm{Gal}_K(L)$.

Theorem: Let $K \subseteq F$ be a finite-dimensional field extension. If K is closed in F then F is a normal extension of K.

Proof: Assume that K is closed in F. Let $p(x) \in K[x]$ be irreducible, and assume that $p(x)$ has a root $u \in F$. For each $f \in \mathrm{Gal}_K(F)$, $f(p(x)) = p(x)$, hence $f(u)$ is a root of $p(x)$ in F. Let $u_1, \ldots, u_n$ be the distinct images of u under $f \in \mathrm{Gal}_K(F)$. Set $g(x) = (x - u_1) \cdots (x - u_n)$. Then $f(g(x)) = g(x)$ for every $f \in \mathrm{Gal}_K(F)$, hence the coefficients of $g(x)$ are fixed by every f that fixes K, hence the coefficients of $g(x)$ reside in K'', hence in K. In other words, $g(x) \in K[x]$. Since $p(x)|g(x)$ and $g(x)$ is monic and has degree $\leq \deg p(x)$, $g(x) = p(x)$. Therefore $p(x)$ splits in F.

We have now proved all the pieces of Theorem [1.22], The Fundamental Theorem of Galois Theory: When $[F : K] = o(\mathrm{Gal}_K(F)) < \infty$ then there is a one-one correspondence between intermediate fields $K \subseteq L \subseteq F$ and subgroups of $\mathrm{Gal}_K(F)$: $L \leftrightarrow H$ where $H = L'$ and $L = H'$. Under this correspondence, $(L' : M') = [M : L]$ and $[H' : J'] = (J : H)$ for subfields $K \subseteq L \subseteq M \subseteq F$ and subgroups $\langle e \rangle \subseteq H \subseteq J \subseteq \mathrm{Gal}_K(F)$. Since K closed in F implies F normal over K, normal field extensions of K pair off with normal subgroups of $\mathrm{Gal}_K(F)$ under the priming correspondence and, since we can verify that $o(\mathrm{Gal}_K(F)/\mathrm{Gal}_L(F)) = o(\mathrm{Gal}_K(L))$, we have $\mathrm{Gal}_K(F)/\mathrm{Gal}_L(F) \cong \mathrm{Gal}_K(L)$.

The next two theorem describe conditions under which K is closed in F.

Theorem: Let $K \subseteq F$ be a finite-dimensional field extension. If F is the splitting field of a separable polynomial then K is closed in F.

Proof: By induction on $[F : K]$. The result is trivial if $[F : K] = 1$. Now consider $[F : K] > 1$. Assume that F splits $f(x)$ and that $f(x)$ has distinct roots in F. Let $p(x)$ be a monic irreducible factor of $f(x)$ in $K[x]$ and let u be a root of $p(x)$ in F. Then F splits $f(x)$ over $K[u]$. Since $[F : K[u]] < [F : K]$, $K[u]$ is closed in F. This implies $o(\mathrm{Gal}_{K[u]}(F)) = [F : K[u]]$. In other words, $(K[u]' : F') = [F : K[u]]$. If we can show that $(K' : K[u]') = [K[u] : K]$ then we will have $o(\mathrm{Gal}_K(F)) = (K' : F') = [F : K]$, hence K is closed in F.

By a previous theorem, we have $(K' : K[u]') \leq [K[u] : K]$. The method was to show that for each coset $K[u]'f$ of K', $f(u)$ is a root of $p(x)$. Since the roots of $p(x)$ are distinct in F, we simply need to show that for each root v of $p(x)$ in F there exists an element of K' such that $f(u) = v$. But this is clear: $K[u] \cong K[v]$ by an isomorphism that fixes K and sends u to v, and since F is a splitting field of f over both $K[u]$ and $K[v]$, the isomorphism extends to a K-automorphism f of K. We have $f \in K'$ and $f(u) = v$. Hence $(K' : K[u]') = [K[u] : K]$ and we are done.

Remark: If F is a finite field with p^n elements then F is the splitting field of the separable polynomial $x^{p_n} - x$ over F_p, hence F_p is closed in F.

Theorem: Let K be a field of characteristic 0. Let F be any splitting field of K. Then K is closed in F.

Proof: By induction on $[F : K]$. This is trivial if $[F : K] = 1$. Now consider $[F : K] > 1$. Let $u \in F \backslash K$ be given. Let $p(x)$ be the minimal polynomial of u in $K[x]$. Since K has characteristic 0, $p(x)$ is separable. All the roots of $p(x)$ belong to F. Let E be the splitting field of $p(x)$ in F. Then by the previous theorem, K is closed in E and $[E : K] = o(\mathrm{Gal}_K(E))$. Since F is a splitting field of $f(x)$ over E and E has characteristic 0, by the induction hypothesis we can say that E is closed in F. Hence $[F : E] = o(\mathrm{Gal}_E(F))$. We also know that $o(\mathrm{Gal}_K(F)) \leq o(\mathrm{Gal}_K(E))o(\mathrm{Gal}_E(F))$. Hence we have

$$o(\mathrm{Gal}_K(F)) \leq o(\mathrm{Gal}_K(E))o(\mathrm{Gal}_E(F)) = [F : K] \leq o(\mathrm{Gal}_K(F)).$$

This implies $[F : K] = o(\mathrm{Gal}_K(F))$, which implies that K is closed in F.

Method for finding a polynomial satisfied by an element u of a splitting field F over a field K: Compute $[F : K] = o(\mathrm{Gal}_K(F)) = n$, find $f_1, \ldots, f_n \in o(\mathrm{Gal}_K(F))$, then set $g(x) = (x - f_1(u)) \cdots (x - f_n(u))$. Then $g(x) \in K[x]$ and $g(u) = 0$. For example, $F = \mathbb{Q}[\sqrt[4]{2}, [i]]$ is the splitting field of the separable polynomial $(x^4 - 2)(x^2 + 1)$, hence is closed. Let $u = w + i$

where $w = \sqrt[4]{2}$. We computed $\mathrm{Gal}_K(F)$ in an example above. The 8 images of u under these elements are

$$w+i, -w+i, wi+i, -wi+i, w-i, -w-i, wi-i, -wi-i.$$

This yields

$$g(x) = 1 + 28x^2 + 2x^4 + 4x^6 + x^8.$$

Theorem: Every finite-dimensional field extension of $\mathbb{R}$ has dimension 2^n over $\mathbb{R}$ for some n.

Proof: Let $\mathbb{R} \subseteq G$ be the extension. We can extend G to a splitting field F over $\mathbb{R}$. Let $u \in F \notin \mathbb{R}$. Then u has a minimal polynomial over $\mathbb{R}$ which must be of even degree. Since $[F:\mathbb{R}] = [F:\mathbb{R}[u]][\mathbb{R}[u]:\mathbb{R}]$, $2|[F:\mathbb{R}]$. Therefore $2|o(\mathrm{Gal}_{\mathbb{R}}(F))$. Write $[F:\mathbb{R}] = 2^n q$ where $2 \not| q$. Let H be a 2-Sylow subgroup of $\mathrm{Gal}_{\mathbb{R}}(F)$. Then $[H':\mathbb{R}] = q$. If $q > 1$ then let $v \in H' \backslash \mathbb{R}$. It satisfies a minimal polynomial over $\mathbb{R}$ which must be of even degree, which implies q is even. Contradiction. Therefore $q = 1$ and $[F:\mathbb{R}] = 2^n$ for some n. This implies $[G:\mathbb{R}] = 2^m$ for some m.

Theorem: Every $f(x) \in \mathbb{C}[x]$ factors completely in $\mathbb{C}[x]$.

Proof: Let $f(x) \in \mathbb{C}[x]$ be given. Let F be its splitting field over $\mathbb{C}$. Then F is a finite-dimensional extension of $\mathbb{R}$, hence $[F:\mathbb{R}] = 2^n$ for some n, which implies $[F:\mathbb{C}] = 2^{n-1}$. Hence $o(\mathrm{Gal}_{\mathbb{C}}(F)) = 2^{n-1}$. If $n > 1$ there is a solvable series of the form

$$\langle e \rangle = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = \mathrm{Gal}_{\mathbb{C}}(F)$$

where $o(H_i/H_{i+1}) = 2$. Hence $[H_{n-1}:\mathbb{C}] = 2$. Choosing $u \in H_{n-1} \backslash \mathbb{C}$ we find that u has minimal polynomial of degree 2 over $\mathbb{C}$. Contradiction: every degree 2 polynomial over $\mathbb{C}$ has a root in $\mathbb{C}$ using the quadratic formula and the fact that every complex number has a square root in $\mathbb{C}$. To avoid this contradiction we must have $n = 1$, $[F:\mathbb{C}] = 1$, $F = \mathbb{C}$.