Galois Theory Solutions

Saxon Supple

July 2024

Exercise 0.1. *Suppose That G is a group. Show that the identity element e is unique, and that for each $g \in G$ the inverse element g^{-1} is also unique.*

Proof. Let e_1 and e_2 be identity elements of G. Then $e_1 = e_1 e_2 = e_2$ so identity elements are unique. Let g_1^{-1} and g_2^{-1} be inverses of g. Then $e = g_1^{-1} g = g_2^{-1} g \implies g_1^{-1} = g_2^{-1}$ so inverses are unique. □

Exercise 0.2. *Show that if H is a subgroup of $\mathbb{Z}$, then H is cyclic.*

Proof. There exists a greatest common divisor of the elements of H. Call it d. $d \in H$ by Bezout's lemma. Furthermore, every element of H is a multiple of d. Thus d is a generator of H so H is cyclic. □

Exercise 0.3. *Show that a subgroup F of a cyclic group G is cyclic.*

Proof. Let g be a generator of G. Then every element $f \in F$ is of the form g^n for some $n \in \mathbb{Z}$. Let H be the set of all integers n such that $g^n \in F$. $e = g^0 \in F$ so $0 \in H$. $g^n \in F \implies g^{-n} \in F$ so H is closed under inverses. $g^n, g^m \in F \implies g^n g^m = g^{n+m} \in F$ so H is closed under composition. Thus H is a subgroup of $\mathbb{Z}$ so is cyclic. Let d be a generator of H. every element of F is then of the form $(g^d)^k$ for some integer k. Thus F is cyclic. □

Exercise 0.4. *Suppose that A, A_1 and A_2 are subsets of a group G, and that $A_1 \subseteq A_2$. Show that*

$$\begin{aligned}
&(i) Z(A) \textit{ is a subgroup of } G\\
&(ii) Z(A_2) \subseteq Z(A_1)\\
&(iii) A \subseteq Z(Z(A))\\
&(iv) Z(A) = Z(Z(Z(A)))\\
&(v) A \subseteq Z(A) \textit{ if and only if } A \textit{ is abelian.}
\end{aligned}$$

Proof. (i)
$e^{-1}g^{-1}eg = e \forall g \in G$ so $e \in Z(A)$.
Let $a \in Z(A)$. Let $g \in A$. Then

$$\begin{aligned}
a^{-1}g^{-1}ag &= e\\
\implies ag &= ga\\
\implies g^{-1}ag &= a\\
\implies g^{-1}a &= ag^{-1}\\
\implies ag^{-1}a^{-1} &= g^{-1}\\
\implies ag^{-1}a^{-1}g &= e
\end{aligned}$$

so $a^{-1} \in Z(A)$.

Let $a, b \in Z(A), g \in A$. $(ab)^{-1}g^{-1}(ab)g = b^{-1}a^{-1}g^{-1}abg = b^{-1}g^{-1}bg = e$ so $ab \in Z(A)$. Thus $Z(A)$ is a subgroup of G.

(ii)

Let $a \in Z(A_2)$. Let $g \in A_1$. Then $g \in A_2$ so $[a, g] = e$. Thus $a \in Z(A_1)$.

(iii)

Let $a \in A$. We want $[a, g] = e \forall g \in Z(A)$. If $g \in Z(A)$, then $[g, a] = e \implies [a, g] = e$.

(iv)

$A \subseteq Z(Z(A))$ so $Z(Z(Z(A))) \subseteq Z(A)$. Furthermore, $Z(A) \subseteq Z(Z(Z(A)))$ so $Z(A) = Z(Z(Z(A)))$.

(v)

Let $a, b \in A$. Then $a \in Z(A)$ so $[a, b] = 0$ so A is abelian.

Now let A be abelian. Then every element of A commutes with every element of A so $A \subseteq Z(A)$. □

Exercise 0.5. *Show that if ϕ is a homomorphism of a group G into a group H then its kernel is a normal subgroup of G.*

Proof. let $a \in \ker\,\phi$ so that $\phi(a) = e$. Let $g \in G$. Then $\phi(g^{-1}ag) = \phi(g^{-1})\phi(a)\phi(g) = \phi(g)^{-1}\phi(g) = e$ so $a^g \in \ker\,\phi$. Thus $\ker\,\phi$ is normal. □

Exercise 0.6. *Suppose that A is a non-empty subset of a group G and that $g \in G$. let $\psi_A(g) = A^g$. Show that ψ_A maps G onto conj(A), and $\psi_A(g') = \psi_A(g)$ if and only if $g' \in N(A)g$. Thus if G is a finite group then $|conj(A)| = |G/N(A)|$, so that $|conj(A)| \cdot |N(A)| = |G|$.*

Proof. $\psi_A(g) = A^g$ so $\psi_A(g)$ is conjugate to A. ψ_A is also clearly surjective so maps G onto conj(A).

$\psi_A(g') = \psi_A(g) \iff A^{g'} = A^g$.

Let $g' \in N(A)g$. Then $g' = hg$ for some $h \in G$ such that $a^h \in A \forall a \in A$. Thus given $a \in A$, $a^{g'} = (hg)^{-1}ahg = g^{-1}h^{-1}ahg = g^{-1}a^hg \in A^g$. Hence $A^{g'} \subseteq A^g$. Furthermore, $g = h^{-1}g'$ so $A^g \subseteq A^{g'}$. Thus $A^{g'} = A^g$.

Now let $A^{g'} = A^g$. We want $a^{g'g^{-1}} \in A \forall A$. Let $a \in A$. $a^{g'g^{-1}} = gg'^{-1}ag'g^{-1} = ga^{g'}g^{-1} = (b^g)^{g^{-1}}$ for some $b \in A$. Thus $a^{g'g^{-1}} \in A$.

Let G be finite. We have established a correspondence between elements of conj(A) and cosets of $N(A)$ so $|\text{conj}(A)| = |G/N(A)|$. $|\text{conj}(A)| \cdot |N(A)| = |G|$ since $|G/N(A)| = |G|/|N(A)|$. □

Exercise 0.7. *Show that if G is a finite group and G is a subgroup of G with index 2 in G, then H is a normal subgroup of G.*

Proof. Let H and gH be the cosets in G/H with $g \notin H$. Let $a \in G$. Then $aH = H$ or $aH = gH$. If $aH = H$, then $a \in H$ so $aH = H = Ha$. If $aH = gH$, then $a \notin H$ so $Ha \neq H$ so $Ha = gH = aH$. Thus the left and right cosets of H are the same so H is normal. □

Exercise 0.8. *Show that if G is a group, then $G/[G, G]$ is abelian, and if $H \trianglelefteq G$ then G/H is abelian if and only if $[G, G] \subseteq H$.*

Proof. Let $a, b \in G$. $(a[G, G])^{-1}(b[G, G])^{-1}a[G, G]b[G, G] = [a, b][G, G] = e[G, G]$ so $G/[G, G]$ is abelian.

$(\implies)$ Let $a, b \in G$. $[a, b]H = [aH, bH] = H$ so $[a, b] \in H$. Thus $[G, G] \subseteq H$.

$(\impliedby)$ Let $aH, bH \in G/H$. $[aH, bH] = [a, b]H = eH$. Thus G/H is abelian. □

Exercise 0.9. *Suppose that G has exactly one subgroup H of order k. Show that H is a normal subgroup of G.*

Proof. Let $g \in G$. $|H^g| = H$ so $H^g = H$. Thus H is normal. □

Exercise 0.10. *Suppose that H is a normal subgroup of G and that K is a normal subgroup of H. Is K necessarily a normal subgroup of G?*

Proof. No. Let $G = S_4$, $H =< (12)(34) >$, $K = \{(12)(34), (13)(42), (23)(41), e\}$. □

Exercise 0.11. *Show that a group G is generated by each of its elements (other than the identity element) if and only if G is a finite cyclic group of prime order.*

Proof. ($\Longleftarrow$) Let g be a generator of G and let G have order p for p a prime. Let g^n be any element of G that isn't the identity. Then n is not a multiple of p and so is coprime to p. Thus for any $a \in \mathbb{Z}$ there exists an $x \in \mathbb{Z}$ such that $nx \equiv a \mod p$ implying $(g^n)^x = g^a$. Thus g^n is a generator.

($\Longrightarrow$) G is cyclic by definition. Suppose that G is infinite. Let $g \in G$ be a generator. Then g^2 is also a generator so there exists an $n \in \mathbb{Z}$ such that $g^{2n} = g \implies g^{2n-1} = e$. But then g has finite order; a contradiction. Thus G is finite. Now suppose that G is of composite order. Write $|G|$ as ab where a and b are positive integers greater than 1. Let g be a generator of G. Then g^a is also a generator of G. However, g^a has order $b < |G|$ so is not a generator; a contradiction. Thus $|G|$ is prime. □

Exercise 0.12. *Describe the elements of $\mathbb{Z}_n$ which generate $\mathbb{Z}_n$.*

Proof. The numbers coprime to n. □

Exercise 0.13. *Give an example of a non-abelian group of order 8 all of whose subgroups are normal.*

Proof. Q_8. □

0.1 Finite Abelian Groups

Exercise 0.14. *Suppose that G is a finite abelian group for which every element other than the identity has order k. Show that k is a prime number, and that G is isomorphic to the product of cyclic groups, each of order k.*

Proof. Suppose that k is composite. Let $k = ab$ where $a, b > 1$. Let $g \in G$ not be the identity so have order k. Then $g^a \neq 0$ has order b; a contradiction. Thus k is prime.

We have that $G \cong \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_n}$, where each d_i is a prime power. Let $\phi : \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_n} \to G$ be the isomorphism. Let $a_i = (0, ..., 0, 1, 0, ..., 0)$ ie, 1 in the ith place and 0 elsewhere. Then $d_i = o(a_i) = o(\phi(a_i)) = k$. Thus $G \cong \mathbb{Z}_k \oplus ... \oplus \mathbb{Z}_k$. □

Exercise 0.15. *Suppose that a and b are positive integers with highest common factor d. Show that $\mathbb{Z}_a \oplus \mathbb{Z}_b \cong \mathbb{Z}_d \oplus \mathbb{Z}_{ab/d}$.*

Proof. □

Exercise 0.16. *Suppose that G is an abelian group. Show that the set T of elements of finite order is a subgroup of G and that every element of G/T, except the identity, is of infinite order.*

Proof. $e \in T$. Let $a, b \in T$ with orders n and m respectively. Then $(ab)^{nm} = (a^n)^m (b^m)^n = e$ so $ab \in T$. If $a \in T$ has order n then a^{-1} has order n. Thus T is a subgroup of G. Let $gT \in G/T$ where $g \notin T$. Then g has infinite order. Suppose there exists an integer n such that $(gT)^n = T$. Then g^n has finite order so g has finite order; a contradiction. □

Exercise 0.17. *Suppose that G is a finitely generated abelian group every element of which, except the identity, has infinite order. Show that $G \cong \mathbb{Z}^s$, where s is defined by the property that G is generated by s elements, but is not generated by $s-1$ elements.*

Proof. Let $g_1, ..., g_s$ be a generating set of G. Define $\phi : \mathbb{Z}^s \to G : (a_1, ..., a_s) \mapsto a_1 g_1 + ... + a_s g_s$. ϕ is a homomorphism and surjective. Suppose that ϕ is not injective. Let m be the smallest positive integer such that there exists a set of generators $\{h_1, ..., h_s\}$ and a relation $mh_1 + a_2h_2 + ... + a_sh_s = 0$. $m > 1$ since otherwise G would be generated by $h_2, ..., h_s$. We can write $a_i = mq_i + r_i$ where $0 \leq r_i < m$ for $2 \leq i \leq s$. Then if $w = h_1 + q_2h_2 + ... + q_sh_s$, G is generated by $\{w, h_2, ..., h_s\}$ and $mw_1 + r_2h_2 + ... + r_sh_s = mh_1 + (a_2 - r_2)h_2 + ... + (a_s - r_s)h_s + r_2h_2 + ... + r_sh_s = mh_1 + a_2h_2 + ... + a_sh_s = 0$. The minimality of m implies that $r_2 = ... = r_s = 0$ and so $mw = 0$. But then w has finite order while not being the identity (since $m > 1$ so $h_1 + q_2h_2 + ... + q_sh_s \neq 0$); a contradiction. Thus ϕ is injective so an isomorphism. □

Exercise 0.18. *Suppose that G is a finitely generated abelian group. Show that $G \cong \mathbb{Z}^s \oplus T$, where T is a finite group.*

Proof. Let $\{g_1, ..., g_n\}$ be a generating set of G. Let F be generated by all g_i of infinite order and let T be generated by all g_i of finite order so that $G \cong F \oplus T$. The result then follows by the above exercise. □

Exercise 0.19. *By considering conjugacy classes, show directly that A_5 is simple.*

Proof. $|A_5| = 60$ so a subgroup of A_5 will have order $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30$ or 60. A normal subgroup is a union of conjugacy classes. The conjugacy classes of A_5 have $1, 12, 12, 15$ and 20 elements. The only possibility for unions of those conjugacy classes which include the trivial group are the trivial group and A_5 so A_5 is simple. □

Exercise 0.20. *Show that the group of rotations of the cube has 24 elements. By considering its four diagonals, show that it is isomorphic to S_4. By considering the three pairs of opposite faces, show that there is an epimorphism of S_4 onto S_3.*

Proof. A rotation of a cube is uniquely characterized by the final position and rotation of one of its faces. A face can be moved to 6 different places and can then be placed in 4 different rotations so the group of rotations of the cube has 24 elements.

Each permutation of the four diagonals of the cube can be attained by a rotation of the cube and the only rotation which yields the trivial permutation of the diagonals is the trivial rotation so by the first isomorphism theorem the two groups are isomorphic. The group of permutations of the diagonals is then isomorphic to S_4 so the group of rotations is isomorphic to S_4.

Similar argument for the existence of an epimorphism of S_4 onto S_3. □

Exercise 0.21. *Show that the group of rotations of the dodecahedron has 60 elements. Using the fact that five cubes can be inscribed in a dodecahedron, or otherwise, show that it is isomorphic to A_5.*

Proof. The dodecahedron has 12 pentagonal faces so the group of rotations has $12 \cdot 5 = 60$ elements.

The group of rotations is isomorphic to a subgroup of S_5 and the only subgroup of S_5 with 60 elements is A_5. □

Exercise 0.22. *A group series $(G_i)_{i=0}^r$ is an upper central series if $G_{i-1}/G_i = Z(G/G_i)$ for $1 \leq i \leq r$. Show that G possesses an upper central series if and only if G is nilpotent.*

Proof. ($\Longrightarrow$) Trivial.

($\Longleftarrow$) Let $(G_i)_{i=0}^r$ be a central series. Define a series $(H_i)_{i=0}^r$ by $H_0 = G$ and $H_i = [G_{i-1}, G_{i-1}]$ for $1 \leq i \leq r$.

We have $[g, h] \in G_i \forall g \in G, h \in G_{i-1}$ □

Exercise 0.23. *Let $z \in \mathbb{Q}$. Show that z is not conjugate to z' for any complex number $z' \neq z$.*

Proof. Define $p \in \mathbb{Q}[x]$ by $p(x) = x - z$. Then $p(z) = 0$ and $p(z') \neq 0$ so z and z' are not conjugate. □

Exercise 0.24. *Show that Gal(f) is a subgroup of S_k.*

Proof. $(\alpha_1, ..., \alpha_k)$ is conjugate to itself so $\text{Id} \in S_k$.

Let $\sigma, \tau \in \text{Gal}(f)$. Let $p \in \mathbb{Q}[x_1, ...x_k]$ such that $p(\alpha_1, ..., \alpha_k) = 0$ so that $p(\alpha_{\sigma(1)}, ..., \alpha_{\sigma(k)}) = 0$ and $p(\alpha_{\tau(1)}, ..., \alpha_{\tau(k)}) = 0$. Define $q \in \mathbb{Q}[x_1, ...x_k]$ by $q(x_1, ..., x_k) = p(\tau(x_1), ..., \tau(x_k))$. Then $q(\alpha_1, ..., \alpha_k) = p(\alpha_{\tau(1)}, ..., \alpha_{\tau(k)}) = 0 \implies q(\alpha_{\sigma(1)}, ..., \alpha_{\sigma(k)}) = p(\alpha_{\tau\circ\sigma(1)}, ..., \alpha_{\tau\circ\sigma(k)}) = 0$.

Now let $p \in \mathbb{Q}[x_1, ...x_k]$ such that $p(\alpha_{\tau\circ\sigma(1)}, ..., \alpha_{\tau\circ\sigma(k)}) = 0$. Define $q \in \mathbb{Q}[x_1, ...x_k]$ by $q(x_1, ..., x_k) = p(\tau(x_1), ..., \tau(x_k))$. Then $q(\alpha_{\sigma(1)}, ..., \alpha_{\sigma(k)}) = p(\alpha_{\tau\circ\sigma(1)}, ..., \alpha_{\tau\circ\sigma(k)}) = 0 \implies q(\alpha_1, ..., \alpha_k) = p(\alpha_{\tau(1)}, ..., \alpha_{\tau(k)}) = 0 \implies p(\alpha_1, ..., \alpha_k) = 0$. Thus $\tau \circ \sigma \in \text{Gal}(f)$.

Let $\sigma \in \text{Gal}(f)$. Let $p \in \mathbb{Q}[x_1, ...x_k]$. Define $q \in \mathbb{Q}[x_1, ...x_k]$ by $q(x_1, ..., x_k) = p(\sigma^{-1}(x_1), ..., \sigma^{-1}(x_k))$. Then $p(\alpha_{\sigma^{-1}(1)}, ..., \alpha_{\sigma^{-1}(k)}) = q(\alpha_1, ..., \alpha_k) = 0 \iff q(\alpha_{\sigma(1)}, ..., \alpha_{\sigma(k)}) = p(\alpha_1, ..., \alpha_k) = 0$ so $\sigma^{-1} \in \text{Gal}(f)$.

Thus $\text{Gal}(f) \leqslant S_k$. □

Exercise 0.25. *Prove that the only subring of a ring R that is also an ideal is R itself.*

Proof. Let S be a subring of R which is also an ideal. S contains 1 so $r \cdot 1 = r \in S \forall r \in R$ so $S = R$. □

Exercise 0.26. *Show that the only ring in which* $0 = 1$ *is the trivial ring.*

Proof. Let R be a non-trivial ring with $0 = 1$ and let $a \in R$ be non-zero. Then $a = 1 \cdot a = 0 \cdot a = 0$; a contradiction. □

Exercise 0.27. *Show that $\mathbb{Z}$ is a principal ideal domain.*

Proof. Let I be an ideal in $\mathbb{Z}$. If $I = \{0\}$ then $I = \langle 0 \rangle$. Otherwise, let n be the smallest positive integer in I. Let $a \in I$. Then $a = kn + r$ for some $k \in \mathbb{Z}$ and $0 \leq r < n$. $kn \in I$ so $r = a - kn \in I$. n is the smallest positive integer in I so $r = 0$ meaning that n divides a. Thus $I = \langle n \rangle$. □

Exercise 0.28. *let $\phi : K \to L$ be a homomorphism of fields. Show that char K = char L.*

Proof. Suppose that K has characteristic 0. Then $m \cdot 1_K \neq 0 \forall m > 0$. Thus $\phi(m \cdot 1_K) = m \cdot 1_L \neq 0 \forall m > 0$ by injectivity so L has characteristic 0.

Now suppose that K has characteristic $p > 0$. Then $p \cdot 1_L = \phi(p \cdot 1_K) = \phi(0) = 0$. Now suppose that there exists an m such that $0 < m < p$ and $m \cdot 1_L = 0$. ϕ is injective so $m \cdot 1_L = \phi(m \cdot 1_K) = 0 \implies m \cdot 1_K = 0$; a contradiction. Thus L has characteristic p. □

Exercise 0.29. *Let p be a prime and consider the field $\mathbb{F}_p(t)$ of rational expressions over $\mathbb{F}$. Show that t has no pth root in $\mathbb{F}_p(t)$.*

Proof. Suppose that t has a pth root $a \in \mathbb{F}_p(t)$. Write a as $\frac{r}{s}$ for $r, s \in \mathbb{F}_p[t]$. Then $t = (\frac{r}{s})^p \implies ts^p = r^p \implies 1 + p\deg(s) = p\deg(r) \implies 1 = p(\deg(r) - \deg(s))$. A contradiction. □

Exercise 0.30. *Let f be a quadratic polynomial over $\mathbb{Q}$. Prove that Gal(f) is S_2 if f has two distinct irrational roots, and trivial otherwise.*

Proof. Let f have distinct irrational roots α_1, α_2. Let d be the discriminant of f, which is irrational. Since d^2 is rational, we can express any $\omega \in \mathbb{Q}(d)$ uniquely as $a + bd$ where $a, b \in \mathbb{Q}$. Define $\overline{\omega}$ as $a - bd$. Given $\nu = f + gd$, we have $\overline{\nu} + \overline{\omega} = (a + f) - (b + g)d = \overline{\nu + \omega}$. Furthermore, $\overline{\nu} \cdot \overline{\omega} = (a - bd)(f - gd) = af - (ag + bf)d + bgd^2$ and $\overline{\nu \cdot \omega} = \overline{af + (bf + ag)d + bgd^2} = af - (bf + ag)d + bgd^2$ so $\overline{\nu} \cdot \overline{\omega} = \overline{\nu \cdot \omega}$. Now let $p \in \mathbb{Q}[x_1, x_2]$. By induction we have that $p(\overline{x_1}, \overline{x_2}) = \overline{p(x_1, x_2)}$ so $p(\alpha_1, \alpha_2) = 0 \iff p(\overline{\alpha_1}, \overline{\alpha_2}) = \overline{0} = 0 \iff p(\alpha_2, \alpha_1) = 0$. Thus (α_1, α_2) and (α_2, α_1) are conjugate so $\mathrm{Gal}(f) = S_2$.

The case where both roots are rational was covered in an exercise. It's not possible for only one root to be rational by the quadratic formula so all cases are covered. □

Exercise 0.31. *Let R be a ring and let $\phi\colon 1 \to R$ be a homomorphism, where 1 denotes the trivial ring. Prove that R is trivial too and that ϕ is an isomorphism.*

Proof. $1_R = \phi(1_1) = \phi(0_1) = 0_R$ so R is trivial. ϕ is injective and surjective so a ring isomorphism. □

Exercise 0.32. *Let $f(t) = a_0 + a_1 t + ... + a_n t^n \in \mathbb{Z}[t]$. Let c/d be a rational root of f, where c and d are coprime integers. Prove the rational roots theorem: $c | a_0$ and $d | a_n$.*

Proof. $f(c/d) = a_0 + a_1 c/d + ... + a_n (c/d)^n = 0 \implies a_0 d^n + a_1 c d^{n-1} + ... + a_n c^n = 0$. Thus $a_0 \equiv 0 \bmod c$ and $a_n \equiv 0 \bmod d$ as required. □

Exercise 0.33. *Can C_6 act faithfully on a 4-element set?*

Proof. No. Let S be the 4-element set and suppose that $\Phi\colon C_6 \to \mathrm{Sym}(S) : g \mapsto (x \mapsto g \cdot x)$ is injective, ie has trivial kernel. 1 has order 6 so $\Phi(1)$ also has order 6. However, $\mathrm{Sym}(S)$ has no element of order 6; a contradiction. □

Exercise 0.34. *Let G be a finite group acting transitively on a nonempty set X. Prove that $|X|$ divides $|G|$.*

Proof. Let $x \in X$. Then $|G| = |\mathrm{Orb}(x)| \cdot |\mathrm{Stab}(x)| = |X| \cdot |\mathrm{Stab}(x)|$ so $|X|$ divides $|G|$. □

Exercise 0.35. *Let R be a ring and let $I_0 \subseteq I_1 \subseteq ...$ be ideals of R. Prove that $\bigcup_{n=0}^{\infty} I_n$ is an ideal of R.*

Proof. Let $a, b \in \bigcup_{n=0}^{\infty} I_n$. We have that $a \in I_k$ for some k. Then given any $r \in R$, we have $ra \in I_k \subseteq \bigcup_{n=0}^{\infty} I_n$. We also have that $b \in I_l$ for some l. Let $m = \max(k, l)$ so that $a, b \in I_m$. Then $b - a \in I_m \subseteq \bigcup_{n=0}^{\infty} I_n$. Thus $\bigcup_{n=0}^{\infty} I_n$ is an ideal. □

Exercise 0.36. *Let R be a principle ideal domain and let $I_0 \subseteq I_1 \subseteq ...$ be ideals of R. Prove that there is some $n \geq 0$ such that $I_n = I_{n+1} = I_{n+2} = ...$*

Proof. There exists some $a \in R$ such that $\bigcup_{n=0}^{\infty} I_n = \langle a \rangle$. There exists some $k \in \mathbb{N}$ such that $a \in I_k$ implying that $\bigcup_{n=0}^{\infty} I_n = I_n \forall n \geq k$. □

Exercise 0.37. *Let R be an integral domain. Let $r, s \in R$ with $r \neq 0$ and s not a unit. Prove that $\langle rs \rangle$ is a proper subset of $\langle r \rangle$.*

Proof. Clearly $\langle rs \rangle \subseteq \langle r \rangle$. Now suppose that $\langle rs \rangle = \langle r \rangle$. We then have some $a \in R$ such that $ars = r \implies r(as - 1) = 0$. $r \neq 0$ so $as = 1$. But s is not a unit; a contradiction. □

Exercise 0.38. *Let R be a principle ideal domain. Let $r \in R$ be neither 0 not a unit. Prove that some irreducible divides r.*

Proof. Suppose that no irreducible divides r. Then writing $r_0 = r$, we have $r_0 = r_1 s_1$ for some non-units r_1 and s_1. Similarly, no irreducible divides r_1 so we can express r_1 as $r_1 = r_2 s_2$ for some non-units r_2 and s_2. Continue this ad infinitum such that $r_i = r_{i+1} s_{i+1}$ for non-units $r_{i+1} s_{i+1}$ with r_i not divisible by an irreducible. We then have $\langle r_0 \rangle \subset \langle r_1 \rangle \subset \langle r_2 \rangle \subset ....$ However, there exists some i such that $\langle r_i \rangle = \langle r_{i+1} \rangle = \langle r_{i+2} \rangle = ...$; a contradiction. □

Exercise 0.39. *For $f \in K[t]$, there is a unique homomorphism $\theta_f \colon K[t] \to K[t]$ such that $\theta_f(t) = f$ and $\theta_f(a) = a$ for all $a \in K$. Which result guarantees this?*

Proof. Universal property of the polynomial ring. The homomorphism is given by $\theta_f(\sum_i a_i t^i) = \sum_i a_i f^i$ □

Exercise 0.40. *For $f, g \in K[t]$, what is $\theta_f(g)$ in explicit terms?*

Proof. $g(f)$ and it has degree $\deg(f)\deg(g)$. □

Exercise 0.41. *For $f_1, f_2 \in \mathbb{K}[t]$, what can you say about the composite homomorphism*

$$\mathbb{K}[t] \overset{\theta_{f_1}}{\to} \mathbb{K}[t] \overset{\theta_{f_2}}{\to} \mathbb{K}[t]?$$

Proof. $\deg(\theta_{f_2} \circ \theta_{f_1}(g)) = \deg(f_1)\deg(f_2)\deg(g)$. □

Exercise 0.42. *Using the previous parts, find all the isomorphisms $\mathbb{K}[t] \to \mathbb{K}[t]$ over $\mathbb{K}$.*

Proof. Any isomorphism over $\mathbb{K}$ is of the form θ_f for some $f \in \mathbb{K}[t]$, with f necessarily having degree 1 and hence linear. Let f be given as $at+b$ for some $a, b \in \mathbb{K}$ with $a \neq 0$. Then $\theta_f(g) = g(at+b) \forall g \in \mathbb{K}[t]$. $\theta_{\frac{t-b}{a}} \circ \theta_f(g) = \theta_{\frac{t-b}{a}}(g(at+b)) = g(a\frac{t-b}{a} + b) = g \forall g \in \mathbb{K}[t]$ and $\theta_f \circ \theta_{\frac{t-b}{a}}(g) = \theta_f(g(\frac{t-b}{a})) = g(\frac{at+b-b}{a}) = g \forall g \in \mathbb{K}[t]$ and so θ_f is an isomorphism. Hence all isomorphisms $\mathbb{K}[t] \to \mathbb{K}[t]$ over $\mathbb{K}$ are of the form θ_{at+b} for non-zero a. □

Exercise 0.43. *Let $f(t) = t^4 + t^3 + t^2 + t + 1$, which has roots $\omega, \omega^2, \omega^3, \omega^4$ where $\omega = e^{2\pi i/5}$. One of the elements of Gal(f) is σ given by $\omega \mapsto \omega^2 \mapsto \omega^4 \mapsto \omega^3 \mapsto \omega$. Prove that Gal($f$) is generated by σ, and deduce that Gal(f) $\cong C_4$.*

Proof. □

Exercise 0.44. *prove that cos($\pi/9$) is algebraic over $\mathbb{Q}$, and find its minimal polynomial.*

Proof. We have $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ and so $1/2 = \cos(\pi/3) = 4\cos^3(\pi/9) - 3\cos(\pi/9)$. Thus $\cos(\pi/9)$ is algebraic over $\mathbb{Q}$ and a solution of $f = 8t^3 - 6t - 1$. 5 is a prime which does not divide 8 and $\overline{f} = 3t^3 - t - 1 \in \mathbb{F}_5[t]$ is irreducible so f is irreducible over $\mathbb{Q}$ by the Mod p method and thus the minimal polynomial. □

Exercise 0.45. *Show that for every $n \geq 1$, there exists an extension of $\mathbb{Q}$ of degree n.*

Proof. Consider the polynomial $t^n - 2$. The prime 2 does not divide the leading coefficient and does divide all other coefficients; furthermore 2^2 does not divide the constant term so $t^n - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. $\sqrt[n]{2}$ then has minimal polynomial $t^n - 2$ so $\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}$ has degree n. □

Exercise 0.46. *Which of the following polynomials are irreducible over $\mathbb{Q}$?*

(i) $1 + 2t - 5t^3 + 2t^6$

(ii) $4 - 3t - 2t^2$

(iii) $4 - 13t - 2t^3$

(iv) $1 + t + t^2 + t^3 + t^4 + t^5$

(v) $1 + t + t^2 + t^3 + t^4 + t^5 + t^6$

(vi) $2.2 + 3.3t - 1.1t^3 + t^7$

(vii) $1 + t^4$

Proof. (i) Reducible since 1 is a root

(ii) The discriminant is $9 + 4 * 4 * 2 = 41$ which is not a square so the polynomial is irreducible.

(iii) Taken modulo 3, the polynomial becomes $1 - t - 2t^3$ which has no solutions modulo 3 so the polynomial is irreducible by the Mod p method.

(iv) The polynomial is $\frac{t^6-1}{t-1} = \frac{(t^3-1)(t^3+1)}{t-1} = \frac{(t-1)(t^2+t+1)(t^3+1)}{t-1} = (t^2 + t + 1)(t^3 + 1)$ so not irreducible

(v) Yes, since it's Φ_7 and cyclotomic polynomials are irreducible.

(vi) 10 is a unit so the polynomial is irreducible if and only if $f = 22+33t-11t^3+10t^7$ is irreducible. The prime 11 divides each coefficient other than the leading one and 100 does not divide the constant term so f is irreducible by Eisenstein's criterion.

(vii) The polynomial is irreducible modulo 3 so is irreducible by the Mod p method.

□

Exercise 0.47. *Let $\mathbb{M} : \mathbb{K}$ be a field extension. Show that $\mathbb{K}(Y \cup Z) = (\mathbb{K}(Y))(Z)$ whenever $Y, Z \subseteq \mathbb{M}$*

Proof. $\mathbb{K}(Y \cup Z) = \bigcap$Subfields of $\mathbb{M}$ containing $\mathbb{K} \cup (Y \cup Z) = \bigcap$Subfields of $\mathbb{M}$ containing $(\mathbb{K} \cup Y) \cup Z = (\mathbb{K}(Y))(Z)$ □

Exercise 0.48. *Let $\mathbb{M} : \mathbb{K}$ be a field extension and $\alpha, \beta \in \mathbb{M}$. Call α and β conjugate over $\mathbb{K}$ if for all $p \in \mathbb{K}[t]$, we have $p(\alpha) = 0 \iff p(\beta) = 0$.*

(i) Prove that α and β are conjugate over $\mathbb{K}$ if and only if either both are transcendental or both are algebraic and they have the same minimal polynomial.

(ii) Show that if there exists an irreducible polynomial $p \in \mathbb{K}[t]$ such that $p(\alpha) = 0 = p(\beta)$, then α and β are conjugate over $\mathbb{K}$.

(iii) Show that if α and β are conjugate over $\mathbb{K}$ then $\mathbb{K}(\alpha) \cong \mathbb{K}(\beta)$ over $\mathbb{K}$.

(iv) Let p be a prime number and put $\omega = e^{2\pi i/p}$. Prove that $\omega, ..., \omega^{p-1}$ are conjugate over $\mathbb{Q}$.

(v) Prove that $\mathbb{Q}(\pi) \cong \mathbb{Q}(e)$ over $\mathbb{Q}$.

Proof. (i) ($\Longleftarrow$)If both are transcendental then they're vacuously conjugate. Suppose both are algebraic with the same minimal polynomial m. $\ker(\mathrm{ev}_\alpha) = \langle m\rangle = \ker(\mathrm{ev}_\beta)$ so $p(\alpha) = 0 \iff p \in \ker(\mathrm{ev}_\alpha) \iff p \in \ker(\mathrm{ev}_\beta) \iff p(\beta) = 0$.

($\Longrightarrow$) Suppose α and β are conjugate over $\mathbb{K}$. Then $\ker(\mathrm{ev}_\alpha) = \ker(\mathrm{ev}_\beta)$. If the ideals are not trivial then α and β are algebraic with the same minimal polynomials (the unique monic polynomial which generates the ideal). If the ideals are trivial, then α and β are transcendental.

(ii) They would then be algebraic with the same minimal polynomial so conjugate.

(iii) First consider the case where α and β are algebraic with minimal polynomial m. Then $\mathbb{K}(\alpha) \cong \mathbb{K}[t]/\langle m\rangle \cong \mathbb{K}(\beta)$, with each isomorphism fixing $\mathbb{K}$ pointwise. Now consider the case when they're both transendental. Then $\mathbb{K}(\alpha) \cong \mathbb{K}(x) \cong \mathbb{K}(\beta)$, with the isomorphisms again fixing $\mathbb{K}$ pointwise.

(iv) They're all roots of the irreducible (over $\mathbb{Q}$) polynomial Φ_p so are conjugate over $\mathbb{Q}$.

(v) Both π and e are transcendental over $\mathbb{Q}$ so apply part *(iii)*.

□

Exercise 0.49. *Let $\mathbb{M} : \mathbb{L} : \mathbb{K}$ be field extensions, which you may not assume to be finite.*

(i) Let $\alpha \in \mathbb{M}$. Prove that if α is algebraic over $\mathbb{L}$ and $\mathbb{L}$ is algebraic over $\mathbb{K}$ then α is algebraic over $\mathbb{K}$.

(ii) Deduce that if $\mathbb{M} : \mathbb{L}$ and $\mathbb{L} : \mathbb{K}$ are algebraic then so is $\mathbb{M} : \mathbb{K}$.

Proof. (i) Let $p = a_0 + a_1x + ... + a_nx^n \in \mathbb{L}[x]$ be a non-zero polynomial such that $p(\alpha) = 0$. Note that $p \in \mathbb{K}(a_0, ..., a_n)[x]$. $\mathbb{K}(a_0, ..., a_n) : \mathbb{K}$ is finite and $\mathbb{K}(a_0, ..., a_n, \alpha) : \mathbb{K}(a_0, ..., a_n)$ is simple algebraic, so finite, hence $\mathbb{K}(a_0, ..., a_n, \alpha) : \mathbb{K}$ is finite so algebraic. Thus α is algebraic over $\mathbb{K}$.

(ii) Every $\alpha \in \mathbb{M}$ is algebraic over $\mathbb{K}$ so $\mathbb{M} : \mathbb{K}$ is algebraic.

□

Exercise 0.50. *Prove that $\overline{\mathbb{Q}}$, the subfield of $\mathbb{C}$ consisting of the complex numbers algebraic over $\mathbb{Q}$, is algebraically closed.*

Proof. Let $f \in \overline{\mathbb{Q}}[x]$ be a non-zero polynomial and let $\mathbb{F}$ be a splitting field of f. $\mathbb{F} : \overline{\mathbb{Q}}$ is algebraic and $\overline{\mathbb{Q}} : \mathbb{Q}$ is algebraic so $\mathbb{F} : \mathbb{Q}$ is algebraic, so every root of f is in $\overline{\mathbb{Q}}$. □

Exercise 0.51. *(i) Here I will write $\langle X\rangle$ for the subfield generated by a subset X of a field $\mathbb{K}$. Show that for all $X \subseteq \mathbb{K}$ and homomorphisms of fields $\phi : \mathbb{K} \to \mathbb{L}$,*

$$\phi\langle X\rangle = \langle \phi X\rangle.$$

(ii) Let $\mathbb{M} : \mathbb{K}$ and $\mathbb{M}' : \mathbb{K}$ be field extensions, and let $\phi : \mathbb{M} \to \mathbb{M}'$ be a homomorphism over $\mathbb{K}$. Show that $\phi(\mathbb{K}(Y)) = \mathbb{K}(\phi Y)$ for all subsets Y of $\mathbb{M}$

Proof. (i) $\phi X \subseteq \phi\langle X\rangle \implies \langle \phi X\rangle \subseteq \langle \phi\langle X\rangle\rangle = \phi\langle X\rangle$ since $\phi\langle X\rangle$ is already a field. Suppose that Y is a subfield of $\mathbb{L}$ containing ϕX. Then $X = \phi^{-1}\phi X \subseteq \phi^{-1}Y$. $\phi^{-1}Y$ is a field so $\langle X\rangle \subseteq \phi^{-1}Y \implies \phi\langle X\rangle \subseteq Y$. Thus $\langle \phi X\rangle = \phi\langle X\rangle$.

(ii) $\phi(\mathbb{K}(Y)) = \phi(\langle \mathbb{K} \cup Y\rangle) = \langle \phi(\mathbb{K} \cup Y)\rangle = \langle \phi(\mathbb{K}) \cup \phi(Y)\rangle = \langle \mathbb{K} \cup \phi(Y)\rangle = \mathbb{K}(\phi Y)$.

□

Exercise 0.52. *Let f be a nonconstant polynomial over $\mathbb{Z}$. Prove that f is primitive and irreducible over $\mathbb{Q}$ $\iff$ f is irreducible over $\mathbb{Z}$.*

Proof. ($\Longleftarrow$) Gauss' lemma.

($\Longrightarrow$) Suppose that f is primitive and irreducible over $\mathbb{Q}$ but is reducible over $\mathbb{Z}$. Then $f = gh$ for some $g, h \in \mathbb{Z}[x]$, neither of which are 0 or 1 (the only unit). If both have degree at least 1 then f is reducible over $\mathbb{Q}$. Thus one is a constant other than 0 or 1. But then f is an integer multiple other than 0 or 1 of a polynomial over $\mathbb{Z}$ and so isn't primitive; a contradiction. □

Exercise 0.53. *(i) Let $\mathbb{K}$ be a field and $a \in \mathbb{K}$. Show that*

$$[\mathbb{K}(\sqrt{a}) : \mathbb{K}] = \begin{cases} 1 & \textit{if } a \textit{ has a root in } \mathbb{K} \\ 2 & \textit{otherwise} \end{cases}$$

(ii) Let $\mathbb{L}$ be a field with char $\mathbb{L} \neq 2$, and let $a, b, c, \alpha \in \mathbb{L}$ with $a \neq 0$. Suppose that $a\alpha^2 + b\alpha + c = 0$, Prove that $b^2 - 4ac$ has a square root σ in $\mathbb{L}$, and that

$$\alpha \in \{\frac{-b+\sigma}{2a}, \frac{-b-\sigma}{2a}\}.$$

(iii) Let $\mathbb{L} : \mathbb{K}$ be a field extension of degree 2, with char $\mathbb{K} \neq 2$. Prove that $\mathbb{L} \cong \mathbb{K}(\sqrt{d})$ for some $d \in \mathbb{K}$.

Proof. (i) Let $m \in \mathbb{K}[x]$ be the minimal polynomial of $\sqrt{a}$. If $\sqrt{a} \in \mathbb{K}$ obvious. Otherwise $m = x^2 - a$ so has degree 2.

(ii) $\alpha^2 + \frac{b}{a}\alpha + \frac{c}{a} = 0 \implies (\alpha + \frac{b}{2a})^2 - \frac{b^2}{4a^2} + \frac{c}{a} = 0 \implies (\alpha + \frac{b}{2a})^2 = \frac{b^2-4ac}{4a^2} \implies b^2 - 4ac = ((2a)(\alpha + \frac{b}{2a}))^2$ so $b^2 - 4ac$ has a square root of $\sigma = (2a)(\alpha + \frac{b}{2a})$ in $\mathbb{L}$. The rest is just computation.

(iii) We have that $\mathbb{L} = \mathbb{K} \oplus \alpha\mathbb{K}$ with α having a minimal polynomial $m \in \mathbb{K}$ of degree 2. Let $m = ax^2 + bx + c$. Then $\alpha = \frac{-b+\sqrt{b^2-4ac}}{2a}$ where $\sqrt{b^2 - 4ac}$ is the correctly chosen square root. Thus $\mathbb{L} = \mathbb{K}(\alpha) = \mathbb{K}(\sqrt{b^2 - 4ac})$.

□

Exercise 0.54. *Prove that the field extension $\overline{\mathbb{Q}} : \mathbb{Q}$ is not finite. Deduce that $\overline{\mathbb{Q}} : \mathbb{Q}$ is not even finitely generated.*

Proof. Suppose $\overline{\mathbb{Q}} : \mathbb{Q}$ is finite with degree n. There is an irreducible polynomial $f \in \mathbb{Q}[x]$ of degree $n + 1$. Let $\alpha \in \overline{\mathbb{Q}}$ be a root of f. Then $n = [\overline{\mathbb{Q}} : \mathbb{Q}] = [\overline{\mathbb{Q}} : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \geq [\mathbb{Q}(\alpha) : \mathbb{Q}] = n + 1$; a contradiction. Hence $\overline{\mathbb{Q}} : \mathbb{Q}$ cannot be both finitely generated and algebraic. $\overline{\mathbb{Q}} : \mathbb{Q}$ is clearly algebraic so it isn't finitely generated. □

Exercise 0.55. *A field extension $\mathbb{M} : \mathbb{K}$ is simple algebraic if there exists $\alpha \in \mathbb{M}$ such that $\mathbb{M} = \mathbb{K}(\alpha)$ and α is algebraic over $\mathbb{K}$. Prove that $\mathbb{M} : \mathbb{K}$ is simple algebraic if and only if it is simple and algebraic.*

Proof. ($\Longrightarrow$) By definition.

($\Longleftarrow$) $\mathbb{M} = \mathbb{K}(\alpha)$ for some $\alpha \in \mathbb{M}$. But $\mathbb{M} : \mathbb{K}$ is algebraic so α is as well. □

Exercise 0.56. *Let $\mathbb{Q}(t_1, t_2, ...)$ be the field of rational expressions in countably infinitely many symbols $t_1, t_2, ...$ (an element is a ratio of polynomials in these symbols, and can involve only finitely many of them). it has a subfield $\mathbb{Q}(t_2, t_3, ...)$. So we have extensions*

$$\mathbb{Q}(t_1, t_2, ...) : \mathbb{Q}(t_2, t_3, ...), \mathbb{Q}(t_2, t_3, ...) : \mathbb{Q}(t_2, t_3, ...).$$

Prove that the fields $\mathbb{Q}(t_1, t_2, ...)$ and $\mathbb{Q}(t_2, t_3, ...)$ are isomorphic, but not isomorphic over $\mathbb{Q}(t_2, t_3, ...)$.

Proof. Consider $\phi : \mathbb{Q}(t_1, t_2, ...) \to \mathbb{Q}(t_2, t_3, ...)$ given by $\phi(t_i) = t_{i+1}$ which is clearly an injective homomorphism between fields with inverse given by $\phi^{-1}(t_i) = t_{i-1}$ so is an isomorphism.

$[\mathbb{Q}(t_1, t_2, ...) : \mathbb{Q}(t_2, t_3, ...)] = \infty$ whereas $[\mathbb{Q}(t_2, t_3, ...) : \mathbb{Q}(t_2, t_3, ...)] = 1$ so they can't be isomorphic (since isomorphic vector spaces have the same dimension). □

Exercise 0.57. *Let $\mathbb{M} : \mathbb{K}$ be a finite extension. Prove that every homomorphism $\mathbb{M} \to \mathbb{M}$ over $\mathbb{K}$ is an automorphism of $\mathbb{M}$ over $\mathbb{K}$.*

Proof. Let $\phi : \mathbb{M} \to \mathbb{M}$ be a homomorphism over $\mathbb{K}$. By the rank-nullity theorem, $[\mathbb{M} : \mathbb{K}] = \text{rank}(\phi) + \text{nullity}(\phi) = \text{rank}(\phi)$ since homomorphisms between fields are injective. Thus $\text{Im}(\phi) \leqslant \mathbb{M}$ and $\dim(\text{Im}(\phi)) = \dim(\mathbb{M})$ so ϕ is surjective so an isomorphism. □

Exercise 0.58. *Let $\mathbb{K}, \mathbb{L}$ and $\mathbb{M}$ be subfields of a field $\mathbb{N}$, with $\mathbb{K} \subseteq \mathbb{L}$ and $\mathbb{K} \subseteq \mathbb{M}$. Here you will prove the 'diamond inequality', $[\mathbb{L}\mathbb{M} : \mathbb{L}] \leq [\mathbb{M} : \mathbb{K}]$.*

(i) First suppose that $\mathbb{M} = \mathbb{K}(\beta)$ for some β algebraic over $\mathbb{K}$. Show that $\mathbb{L}\mathbb{M} = \mathbb{L}(\beta)$, then deduce that $[\mathbb{L}\mathbb{M} : \mathbb{L}] \leq [\mathbb{M} : \mathbb{K}]$.

(ii) Now prove the diamond inequality when $\mathbb{M} = \mathbb{K}(\beta_1, ..., \beta_n)$ for some $\beta_1, ..., \beta_n$ algebraic over $\mathbb{K}$,

(iii) Finally, prove the diamond inequality in full generality.

Proof. (i) $\mathbb{L} \subseteq \mathbb{L}(\beta)$ and $\mathbb{M} = \mathbb{K}(\beta) \subseteq \mathbb{L}(\beta)$ since $\mathbb{K} \subseteq \mathbb{L}$ so $\mathbb{L} \cup \mathbb{M} \subseteq \mathbb{L}(\beta)$. Now let $\mathbb{I}$ be a subfield of $\mathbb{N}$ containing $\mathbb{L} \cup \mathbb{M}$. $\mathbb{I}$ then contains $\mathbb{L}$ and β so $\mathbb{L}(\beta) \subseteq \mathbb{I}$. Thus $\mathbb{L}\mathbb{M} = \mathbb{L}(\beta)$. Then $[\mathbb{L}\mathbb{M} : \mathbb{L}] = [\mathbb{L}(\beta) : \mathbb{L}] \leq \deg(m) = [\mathbb{M} : \mathbb{K}]$ where m is the minimal polynomial of β over $\mathbb{K}$.

(ii) We proceed by induction on n. The base case was covered above. Assume true for $n = k$. For $n = k + 1$, we have $\mathbb{M} = \mathbb{K}(\beta_1, ...\beta_k)(\beta_{k+1})$, $\mathbb{L}\mathbb{K}(\beta_1, ..., \beta_k) = \mathbb{L}(\beta_1, ..., \beta_k)$ and $[\mathbb{L}\mathbb{K}(\beta_1, ..., \beta_k) : \mathbb{L}] \leq [\mathbb{K}(\beta_1, ..., \beta_k) : \mathbb{K}]$. $\mathbb{L}\mathbb{M} = \mathbb{L}(\mathbb{K}(\beta_1, ..., \beta_k) \cup \{\beta_{k+1}\}) = (\mathbb{L}\mathbb{K}(\beta_1, ..., \beta_k))(\beta_{k+1}) = \mathbb{L}(\beta_1, ..., \beta_k)(\beta_{k+1}) = \mathbb{L}(\beta_1, ..., \beta_{k+1})$. Thus $[\mathbb{L}\mathbb{M} : \mathbb{L}] = [\mathbb{L}(\beta_1, ..., \beta_{k+1}) : \mathbb{L}] = [\mathbb{L}(\beta_1, ..., \beta_{k+1}) : \mathbb{L}(\beta_1, ..., \beta_k)][\mathbb{L}(\beta_1, ..., \beta_k) : \mathbb{L}] \leq [\mathbb{L}(\beta_1, ..., \beta_{k+1}) : \mathbb{L}(\beta_1, ..., \beta_k)][\mathbb{K}(\beta_1, ..., \beta_k) : \mathbb{K}] \leq [\mathbb{K}(\beta_1, ..., \beta_{k+1}) : \mathbb{K}(\beta_1, ..., \beta_k)][\mathbb{K}(\beta_1, ..., \beta_k) : \mathbb{K}] = [\mathbb{K}(\beta_1, ..., \beta_{k+1}) : \mathbb{K}] = [\mathbb{M} : \mathbb{K}]$ as required.

(iii) If $[\mathbb{M} : \mathbb{K}] = \infty$ then clearly the inequality holds. Otherwise, there are finitely many $\beta_1, ..., \beta_n$ algebraic over $\mathbb{K}$ such that $\mathbb{M} = \mathbb{K}(\beta_1, ..., \beta_n)$ and so part (ii) applies.

□

Exercise 0.59. *Let $\mathbb{M} : \mathbb{L} : \mathbb{K}$ be field extensions, with $\mathbb{M} : \mathbb{K}$ finite and normal. Prove that there is a smallest subfield $\mathbb{L}'$ of $\mathbb{M}$ such that $\mathbb{L} \subseteq \mathbb{L}'$ and $\mathbb{L}' : \mathbb{K}$ is normal. Here 'smallest' means that $\mathbb{L}' \subseteq \mathbb{L}''$ for any other subfield $\mathbb{L}''$ with the same properties.*

Proof. We have that $\mathbb{L} = \mathbb{K}(a_1, ..., a_n)$ for $a_1, ..., a_n$ algebraic over $\mathbb{K}$. Let $m_1, ..., m_n \in \mathbb{K}[x]$ be their minimal polynomials. Then define $\mathbb{L}'$ to be the splitting field of $m_1...m_n$. Clearly $\mathbb{L} \subseteq \mathbb{L}'$, and $\mathbb{L}' \subseteq \mathbb{M}$ since $\mathbb{M}$ is normal and so contains all the roots of all irreducible polynomials over $\mathbb{K}$ with a root in $\mathbb{M}$. $\mathbb{L}'$ is also normal since all splitting fields are normal. Now suppose $\mathbb{L}''$ is another subfield with the same properties. Then $\mathbb{L}''$ will contain $a_1, ..., a_n$ and so contain all the roots of $m_1, ..., m_n$ and so contain $\mathbb{L}'$. □

I was wondering if an irreducible polynomial having a non-solvable Galois group implies that every root is non-radical. The answer is yes. To prove this, it suffices to prove that if an irreducible polynomial has a radical root, then every root is radical.

Lemma 0.60. *Let $\mathbb{L}/\mathbb{K}$ be an algebraic extension, where $\mathbb{L} = \mathbb{K}(\alpha)$ for $\alpha \in \mathbb{L}$ with minimal polynomial $m \in \mathbb{K}[x]$. Let $\mathbb{F}$ be a splitting field of m. Then $\mathbb{F}/\mathbb{K}$ is the normal closure of $\mathbb{L}/\mathbb{K}$.*

Proof. $\mathbb{F}/\mathbb{K}$ is normal since $\mathbb{F}$ is the splitting field of a polynomial over $\mathbb{K}$. We now show that $\mathbb{F}/\mathbb{K}$ is minimal. Let $\mathbb{M}$ be a subfield of $\mathbb{F}$ containing $\mathbb{L}$ with $\mathbb{M}/\mathbb{K}$ normal. m must then split into linear factors over $\mathbb{M}$, since $\alpha \in \mathbb{M}$, and so $\mathbb{M}$ contains every root of m and hence contains $\mathbb{F}$. Thus $\mathbb{M} = \mathbb{F}$. □

Lemma 0.61. *The normal closure of a finite radical extension is a radical extension.*

Theorem 0.62. *If a root of an irreducible polynomial is radical, then every root is radical.*

Proof. Let $\mathbb{L}/\mathbb{K}$ be an extension contained in a finite radical extension $\mathbb{M}/\mathbb{K}$. Then the normal closure of $\mathbb{L}/\mathbb{K}$ is contained in the normal closure of $\mathbb{M}/\mathbb{K}$ which is radical by the above lemma. Now suppose that $\mathbb{L} = \mathbb{K}(\alpha)$ for $\alpha \in \mathbb{L}$ algebraic over $\mathbb{K}$ with minimal polynomial $m \in \mathbb{K}[x]$ and $\mathbb{M}/\mathbb{K}$ is a finite radical extension containing $\mathbb{L}/\mathbb{K}$; ie, m has a radical root. Then the spitting field of m, which is the normal closure of $\mathbb{L}/\mathbb{K}$, is contained in a radical extension (the normal closure of $\mathbb{M}/\mathbb{K}$) and hence every root of m is radical. □

Exercise 0.63. *Let $\mathbb{M} : \mathbb{K}$ be a field extension. Let $0 \neq f \in \mathbb{K}[t]$, and let $\alpha \in \mathbb{M}$ be a root of f; then $f(t) = (t - \alpha)g(t)$ for some $g(t) \in \mathbb{K}(\alpha)[t]$. Prove that $\mathbb{M}$ is a splitting field of g over $\mathbb{K}(\alpha)$ $\iff$ $\mathbb{M}$ is a splitting field of f over $\mathbb{K}$.*

Proof. ($\implies$) We have that $\mathbb{M} = \mathbb{K}(\alpha)(a_1, ..., a_n)$ where $a_1, ..., a_n$ are the roots of g. But then $\mathbb{M} = \mathbb{K}(\alpha, a_1, ..., a_n)$ where $alpha, a_1, ..., a_n$ are the roots of f and so $\mathbb{M}$ is a splitting field of f over $\mathbb{K}$.

($\impliedby$) We have that $\mathbb{M} = \mathbb{K}(\alpha, a_1, ..., a_n)$ where $a_1, ..., a_n$ are the other roots of f and so $\mathbb{M} = \mathbb{K}(\alpha)(a_1, ..., a_n)$ where $a_1, ..., a_n$ are the roots of g. □

Exercise 0.64. *Let $\mathbb{K}$ be a field and let $f \in \mathbb{K}[t]$ be an irreducible polynomial.*

(i) Prove that the order of $Gal_{\mathbb{K}}(f)$ is divisible by the number of distinct roots of f in its splitting field.

(ii) Deduce that if $Char(\mathbb{K}) = 0$ then $deg(f)$ divides $|Gal_{\mathbb{K}}(f)|$.

Proof. (i) let $a_1, ..., a_n$ be the distinct roots of f. $\mathrm{Gal}_{\mathbb{K}}(f)$ acts transitively on the roots so n divides the order of $\mathrm{Gal}_{\mathbb{K}}(f)$ by the orbit-stabilizer theorem.

(ii) f is separable so $\deg(f) = n$.

□

Exercise 0.65. *Let $\mathbb{M} : \mathbb{K}$ be a finite normal separable field extension. let H be a subgroup of $G = Gal(\mathbb{M} : \mathbb{K})$. Prove that H is a normal subgroup of G if and only if $Fix(H)$ is a normal extension of $\mathbb{K}$, and that if these conditions hold them $G/H \cong Gal(Fix(H) : \mathbb{K})$.*

Proof. Since $\mathbb{M} : \mathbb{K}$ is a Galois extension, we have that $H = \mathrm{Aut}_{\mathbb{L}}\mathbb{M}$ for some unique field $\mathbb{L}$ such that $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$. Then by the fundamental theorem of Galois theory, $H = \mathrm{Aut}_{\mathbb{L}}\mathbb{M}$ is a normal subgroup of G if and only if $\mathbb{L} = \mathrm{Fix}(H)$ is a normal extension, and furthermore $\mathrm{Gal}(\mathrm{Fix}(H) : \mathbb{K}) = \mathrm{Gal}(\mathbb{L} : \mathbb{K}) \cong G/\mathrm{Aut}_{\mathbb{L}}\mathbb{M} = G/H$. □

Exercise 0.66. *Prove that every field extension of degree 2 is normal.*

Proof. Let $\mathbb{M} : \mathbb{K}$ be a field extension of degree 2 and let $a \in \mathbb{M}$ have minimal polynomial $m \in \mathbb{K}[x]$. If $a \in \mathbb{K}$ then everything's fine. Suppose then that $a \notin \mathbb{K}$. $\mathbb{K} \subseteq \mathbb{K}(a) \subseteq \mathbb{M}$ so m has degree 2. Write m as $(x - a)(x - b)$ for b in a splitting field of m and suppose that $b \notin \mathbb{M}$. Then the constant coefficient of m is not in $\mathbb{M}$ and so $m \notin \mathbb{K}[x]$; a contradiction. □

Exercise 0.67. *Show that any automorphism of a field $\mathbb{M}$ is an automorphism over the prime subfield of $\mathbb{M}$.*

Proof. Let Φ be an automorphism over $\mathbb{M}$ and let $\mathbb{F}$ be the prime subfield. We have $\Phi(1_{\mathbb{M}}) = 1_{\mathbb{M}}$ and so $\Phi(m1_{\mathbb{M}}) = m\Phi(1_{\mathbb{M}}) = m1_{\mathbb{M}} \forall m \in \mathbb{Z}$. Thus $\Phi(\frac{m1_{\mathbb{M}}}{n1_{\mathbb{M}}}) = \frac{\Phi(m1_{\mathbb{M}})}{\Phi(n1_{\mathbb{M}})} = \frac{m1_{\mathbb{M}}}{n1_{\mathbb{M}}} \forall m, n \in \mathbb{Z}, n \notin \langle \mathrm{char}(\mathbb{M}) \rangle$ so Φ fixes $\mathbb{F}$. □

Exercise 0.68. *Show by example that for field extensions $\mathbb{M} : \mathbb{L} : \mathbb{K}$, $\mathbb{M} : \mathbb{L}$ and $\mathbb{L} : \mathbb{K}$ normal $\not\Rightarrow$ $\mathbb{M} : \mathbb{K}$ normal.*

Proof. Let $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{K}(\sqrt{2})$ and $\mathbb{M} = \mathbb{L}(i\sqrt[4]{2})$. $\mathbb{L} : \mathbb{K}$ is normal since $\mathbb{L}$ is a splitting field of $x^2 - 2$ over $\mathbb{K}$. $\mathbb{M} : \mathbb{L}$ is normal since $\mathbb{M}$ is a splitting field of $x^2 + \sqrt{2}$ over $\mathbb{L}$. $i\sqrt[4]{2}$ is a root of $x^4 - 2$ which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. For $\mathbb{M} : \mathbb{K}$ to be normal, we must then have $\sqrt[4]{2} \in \mathbb{M}$. Suppose this is the case. Then $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt{2}, i\sqrt[4]{2}) = \mathbb{Q}(i\sqrt[4]{2})$. Then by the tower law, $4 = [\mathbb{Q}(\sqrt{2}, i\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i\sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2^3 = 8$; a contradiction. Thus $\mathbb{M} : \mathbb{K}$ is not normal. □

Exercise 0.69. *(i) Let $\mathbb{K}$ be a field and let f and g be nonzero polynomials over $\mathbb{K}$. Put $\mathbb{L} = SF_{\mathbb{K}}(g)$. Show that $SF_{\mathbb{L}}(f)$ and $SF_{\mathbb{K}}(fg)$ are isomorphic over $\mathbb{K}$.*

(ii) Let f and g be nonzero polynomials over $\mathbb{Q}$. Prove that $SF_{\mathbb{Q}}(fg)$ is the compositum of $SF_{\mathbb{Q}}(f)$ and $SF_{\mathbb{Q}}(g)$, where all three splitting fields are viewed as subfields of $\mathbb{C}$.

Exercise 0.70. *(i) $SF_{\mathbb{L}}(f)$ is the smallest field containing the roots of f and $\mathbb{L}$ - the smallest field containing $\mathbb{K}$ and the roots of g - so $SF_{\mathbb{L}}(f)$ is the smallest field containing the roots of f and g and $\mathbb{K}$ so is the smallest field containing the roots of fg and $\mathbb{K}$ so is a splitting field of fg over $\mathbb{K}$. Splitting fields are isomorphic so $SF_{\mathbb{L}}(f)$ and $SF_{\mathbb{K}}(fg)$ are isomorphic over $\mathbb{K}$.*

(ii) Let $a_1, ..., a_m$ and $b_1, ..., b_n$ be the roots of f and g respectively. Then $SF_{\mathbb{Q}}(fg) = \mathbb{Q}(a_1, ..., a_m, b_1, ..., b_n) = \mathbb{Q}(a_1, ..., a_m)\mathbb{Q}(b_1, ..., b_n) = SF_{\mathbb{Q}}(f)SF_{\mathbb{Q}}(g)$.

Exercise 0.71. *Let $0 \neq f \in \mathbb{Q}[t]$ with distinct complex roots $\alpha_1, ..., \alpha_k$. Prove that $\sum_{i=1}^{k} \alpha_i^{10}$ is rational.*

Proof. Let $\phi \in \mathrm{Gal}(SF_{\mathbb{Q}}(f)/\mathbb{Q})$. ϕ permutes the roots so $\phi(\sum_{i=1}^{k} \alpha_i^{10}) = \sum_{i=1}^{k} \phi(\alpha_i)^{10} = \sum_{i=1}^{k} \alpha_i^{10}$. Every $\alpha \in SF_{\mathbb{Q}}(f) \backslash \mathbb{Q}$ has an automorphism in $\mathrm{Gal}(SF_{\mathbb{Q}}(f)/\mathbb{Q})$ which doesn't fix it so $\sum_{i=1}^{k} \alpha_i^{10}$ must be rational. □

Exercise 0.72. *Let $\mathbb{L} : \mathbb{K}$ be an algebraic extension. Prove that $\mathbb{L} : \mathbb{K}$ is normal if and only if it has the following property: for every extension $\mathbb{M} : \mathbb{L}$, the field $\mathbb{L}$ is a union of conjugacy classes in $\mathbb{M}$ over $\mathbb{K}$.*

(Conjugacy over $\mathbb{K}$ defined an equivalence relation of $\mathbb{M}$, and a 'conjugacy class in $\mathbb{M}$ over $\mathbb{K}$' means an equivalence class of this equivalence relation.)

Proof. ($\Longrightarrow$) Let $\mathbb{M} : \mathbb{L}$ be an extension. Let $a \in \mathbb{L}$ and let $b \in \mathbb{M}$ be conjugate to a over $\mathbb{K}$. Then $p(a) = 0 \iff p(b) = 0 \forall p \in \mathbb{K}[x]$. Let $f \in \mathbb{K}[x]$ be an irreducible polynomial which has a as a root. Then b is also a root of f and so $b \in \mathbb{L}$ since $\mathbb{L} : \mathbb{K}$ is normal. Thus if $\mathbb{L}$ contains a, it contains the whole conjugacy class of a in $\mathbb{M}$ and so $\mathbb{L}$ is a union of conjugacy classes in $\mathbb{M}$ over $\mathbb{K}$.

($\Longleftarrow$) Let $a \in \mathbb{L}$ and let $f \in \mathbb{K}[x]$ be an irreducible polynomial with a as a root. Let $b \in \mathbb{M}$ be another root of f. Then $\mathrm{Ker}(\mathrm{ev}_a) = \langle f \rangle = \mathrm{Ker}(\mathrm{ev}_b)$ and so a and b are conjugate so are in the same conjugacy class. $\mathbb{L}$ is a union of conjugacy classes in $\mathbb{M}$ so $b \in \mathbb{L}$. Thus $\mathbb{L} : \mathbb{K}$ is normal. □

Exercise 0.73. *Let f be an irreducible cubic over $\mathbb{Q}$. Write $\alpha_1, \alpha_2, \alpha_3$ for the complex roots of f, and put*

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$

(i) Show that $Gal_{\mathbb{Q}}(f)$ is isomorphic to A_3 or S_3.

(ii) Show that $\delta \neq 0$.

(iii) Show that $\theta(\delta) = \pm\delta$ for all $\theta \in Gal_{\mathbb{Q}}(f)$.

(iv) Show that

$$G \cong \begin{cases} A_3 & \text{if } \delta \in \mathbb{Q}, \\ S_3 & \text{otherwise.} \end{cases}$$

(v) Define

$$\Delta = \delta^2 = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

It is tedious but straightforward to check that if we write

$$B = -(\alpha_1 + \alpha_2 + \alpha_3), C = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, D = -\alpha_1\alpha_2\alpha_3$$

then

$$\Delta = -27D^2 + 18BCD - 4C^3 - 4B^3D + B^2C^2.$$

Which result from Chapter 8 implies that $\Delta \in \mathbb{Q}$, with zero calculation?

(vi) Deduce that if we write $f(t)$ as $t^3 + bt^2 + ct + d$ then

$$Gal_{\mathbb{Q}}(f) \cong \begin{cases} A_3 & \text{if } \sqrt{-27d^2 + 18bcd - 4c^3 - 4b^3d + b^2c^2} \in \mathbb{Q}, \\ S_3 & \text{otherwise.} \end{cases}$$

(vii) Find the Galois group of $t^3 - 3t - 1$.

Proof. (i) f is irreducible so $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = 3\forall i$. Thus 3 divides $[\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{Q}] = |\mathrm{Gal}_{\mathbb{Q}}(f)|$. $\mathrm{Gal}_{\mathbb{Q}}(f)$ is isomorphic to a subgroup of S_3 ($\mathrm{Char}(\mathbb{Q}) = 0$ so f is separable) and the only subgroups of S_3 with orders divisible by 3 are A_3 and S_3.

(ii) The roots are all distinct so $\delta \neq 0$.

(iii) θ permutes $\alpha_1, \alpha_2, \alpha_3$ so $\theta(\delta) = \pm\delta$.

(iv) If $\delta \in \mathbb{Q}$ then every $\theta \in \mathrm{Gal}_{\mathbb{Q}}(f)$ fixes δ. The automorphism given by swapping α_1 and α_2 switches the sign of δ so G cannot be isomorphic to S_3 if $\delta \in \mathbb{Q}$ so must be isomorphic to A_3. If $\delta \notin \mathbb{Q}$ then there must exist a $\theta \in \mathrm{Gal}_{\mathbb{Q}}(f)$ such that $\theta(\delta) = -\delta$. Every θ corresponding to an element of A_3 fixes δ so there must be a θ in the Galois group which doesn't correspond to an element of A_3 and so $G \cong S_3$ if $\delta \notin \mathbb{Q}$.

(v) Δ is fixed by every automorphism in the Galois group so $\Delta \in \mathbb{Q}$.

(vi) It's the same condition as asking if δ is rational.

(vii) $\sqrt{-27 - 4(-3)^3} = 9$ so the Galois group is A_3.

□

Exercise 0.74. *Work through the details of the Galois correspondence for $t^4 - 2t^2 + 9 \in \mathbb{Q}[t]$.*

Proof. $t^4-2t^2+9 = (t^2+3)^2-8t^2 = (t^2+2\sqrt{2}t+3)(t^2-2\sqrt{2}t+3)$. $8-12 < 0$ and $\sqrt{2} \notin \mathbb{Q}$ so t^4-2t^2+9 is irreducible with roots $-\sqrt{2} \pm i, \sqrt{2} \pm i$. Thus $SF_{\mathbb{Q}}(f) = \mathbb{Q}(\sqrt{2}+i, \sqrt{2}-i)$. $\sqrt{2} = \frac{(\sqrt{2}+i)+(\sqrt{2}-i)}{2}$ so $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}+i, \sqrt{2}-i)$. Also, $i = \frac{(\sqrt{2}+i)-(\sqrt{2}-i)}{2}$. Thus $\mathbb{Q}(\sqrt{2}+i, \sqrt{2}-i) = \mathbb{Q}(\sqrt{2}, i)$. $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2*2 = 4$. $\mathrm{Gal}_{\mathbb{Q}}(f)$ acts transitively on the roots of f so we can write the collection of automorphisms $\phi_1, ..., \phi_4$ in the Galois group so that $\phi_i(a_1) = a_i$ after writing the roots in some order $a_1, ..., a_4$. Let $\phi_1 = \mathrm{Id}$. Let $\phi_2 = (z \mapsto \overline{z})$. Let $\phi_3(\sqrt{2}+i) = -\sqrt{2}+i$. Let $\phi_4(\sqrt{2}+i) = -\sqrt{2}-i$. ϕ_1 has order 1 and ϕ_2 has order 2. $\phi_4^2(\sqrt{2}+i) = -\phi_4(\sqrt{2}+i) = \sqrt{2}+i$ so ϕ_4 has order 2. Thus at most one element of the Galois group can be cyclic. There are 2 groups of order 4: The Klein four-group and the cyclic group of order 4. However, the cyclic group of order 4 has 2 cyclic elements and so the Galois group cannot be isomorphic to it. Thus $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. $\mathrm{Gal}_{\mathbb{Q}}(f)$ then has 1 subgroup of order 1, 3 of order 2 and 1 of order 4, each normal. We then have that $\mathrm{Gal}_{\mathbb{Q}}(f)$ has the following subfields: $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2}i)$ and $\mathbb{Q}$, with $\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}i) \subseteq \mathbb{Q}(\sqrt{2}, i)$ and no other inclusions. Clearly $\mathrm{Gal}_{\mathbb{Q}}(f) = \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, i)$ and $\langle \phi_1 \rangle = \mathrm{Aut}_{\mathbb{Q}(\sqrt{2}, i)}\mathbb{Q}(\sqrt{2}, i)$. $\langle \phi_2 \rangle = \mathrm{Aut}_{\mathbb{Q}(\sqrt{2})}\mathbb{Q}(\sqrt{2}, i)$ since ϕ_2 alters i and $\sqrt{2}i$. $\phi_3(i) = \phi_3(\frac{(\sqrt{2}+i)-(\sqrt{2}-i)}{2}) = \frac{(-\sqrt{2}+i)+\phi_3^2(\sqrt{2}+i)}{2} = \frac{(-\sqrt{2}+i)+(\sqrt{2}+i)}{2} = i$ so $\langle \phi_3 \rangle = \mathrm{Aut}_{\mathbb{Q}(i)}\mathbb{Q}(\sqrt{2}, i)$ and $\langle \phi_4 \rangle = \mathrm{Aut}_{\mathbb{Q}(\sqrt{2}i)}\mathbb{Q}(\sqrt{2}, i)$. □

Exercise 0.75. *Let p be a prime. Prove that $Gal_{\mathbb{Q}}(t^p - 1) \cong C_{p-1}$.*

Proof. $SF_{\mathbb{Q}}(t^p - 1) = \mathbb{Q}(\omega)$ where $\omega = e^{\frac{2\pi i}{p}}$ with minimal polynomial $t^{p-1} + ... + 1$. Thus $|\mathrm{Gal}_{\mathbb{Q}}(t^p - 1)| = p-1$. $\mathrm{Gal}_{\mathbb{Q}}(t^p-1)$ acts transitively on the roots of $t^{p-1}+...+1$ so there must be $\phi_i \in \mathrm{Gal}_{\mathbb{Q}}(t^p-1)$ such that $\phi_i(\omega) = \omega^i$ for all $1 \leq i \leq p-1$. There are $p-1$ such ϕ_i so they comprise the whole Galois group. The Galois group is then clearly isomorphic to C_{p-1}. □

Exercise 0.76. *(i) Show that when p is prime, $\Phi_p(t) = t^{p-1} + ... + t + 1$.*

(ii) By considering $\theta_* \Phi_n$ for $\theta \in Gal_{\mathbb{Q}}(t^n - 1)$, prove that $\Phi_n \in \mathbb{Q}[t]$.

(iii) Show that $\prod_{d|n} \Phi_d(t) = t^n - 1$.

(iv) use Gauss's lemma on primitive polynomials to show that whenever $f, g \in \mathbb{Q}[t]$ are monic polynomials such that $fg \in \mathbb{Z}[t]$, then $f, g \in \mathbb{Z}[t]$.

(v) Put together the previous parts to conclude that $\Phi_n \in \mathbb{Z}[t]$.

Proof. (i) $\Phi_p(t)$ has roots $e^{\frac{2\pi ik}{p}}, 0 \leq k \leq p-1$. $1 = e^{\frac{2\pi i*0}{p}}$ isn't primitive; however every other root is since k is coprime to p. Thus $\Phi_p(t) = \frac{t^p-1}{t-1} = t^{p-1} + ... + t + 1$.

(ii) $\Phi_n = \prod_{\gcd(k,n)=1}(t-\omega^k)$ for $\omega = e^{\frac{2\pi i}{n}}$ so $\theta_*\Phi_n = \prod_{\gcd(k,n)=1}(t-\theta(\omega)^k) = \prod_{\gcd(k,n)=1}(t-\omega^k) = \Phi_n$ since θ permutes primitive nth roots of unity. Thus every $\theta \in \text{Gal}_{\mathbb{Q}}(t^n-1)$ fixes the coefficients of Φ_n so $\Phi_n \in \mathbb{Q}[t]$.

(iii) Each root of $t^n - 1$ is a primitive dth root of unity for some $d|n$ by Lagrange's theorem.

(iv) Let $F, G \in \mathbb{Z}[t]$ be primitive polynomials such that $f, g = \frac{a}{b}F, \frac{c}{d}G$ respectively, for $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. FG is primitive by Gauss's lemma and $\frac{ac}{bd}FG \in \mathbb{Z}[t]$ so $\frac{ac}{db} \in \mathbb{Z}$. Furthermore, $\frac{ac}{bd}FG$ is monic so $\frac{ac}{bd} = 1$. Thus both F and G are monic so $\frac{a}{b} = \frac{c}{d} = 1$. Hence $f, g \in \mathbb{Z}[t]$.

(v) Φ_d is monic and $\Phi_d \in \mathbb{Q}[t] \forall d|n$ and $\prod_{d|n} \Phi_d(t) \in \mathbb{Z}[t]$ so each $\Phi_d \in \mathbb{Z}[t]$, including Φ_n.

□

Exercise 0.77. *Work through the Galois correspondence for $t^3 - 2$ over $\mathbb{Q}$.*

Proof. $t^3 - 2 = (t - \sqrt[3]{2})(t - \sqrt[3]{2}\omega)(t - \sqrt[3]{2}\omega^2)$ where $\omega = e^{\frac{2\pi i}{3}}$ so $SF_{\mathbb{Q}}(t^3-2) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. $\sqrt{-27*4} \notin \mathbb{Q}$ so $\text{Gal}_{\mathbb{Q}}(t^3-2) \cong S_3$. $\mathbb{Q}(\omega)$ is the splitting field of $t^3 - 1$ so $\mathbb{Q}(\omega) : \mathbb{Q}$ is normal. A_3 is the only normal subgroup of S_3 other than S_3 and the trivial subgroup so $\text{Aut}_{\mathbb{Q}(\omega)}\mathbb{Q}(\sqrt[3]{2}, \omega) \cong A_3$ by the fundamental theorem of Galois theory. We then have 3 more subfields to find, since S_3 has 6 subgroups. The remaining subgroups of S_3 all have order 2 so $[\mathbb{M}_i : \mathbb{K}] = 6/2 = 3$ for the remaining subfields $\mathbb{M}_i$. One of the remaining subfields is $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{4})$ (since $(2^{\frac{2}{3}})^2 = 2\sqrt[3]{2}$). We also have a subfield $\mathbb{Q}(\sqrt[3]{2}\omega) = \mathbb{Q}(\sqrt[3]{4}\omega^2)$ and a subfield $\mathbb{Q}(\sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{4}\omega)$. No intermediate subfield contains any other intermediate subfield. Let ϕ_1 swap $\sqrt[3]{2}$ and $\sqrt[3]{2}\omega$ and fix $\sqrt[3]{2}\omega^2$. Then $\text{Aut}_{\mathbb{Q}(\sqrt[3]{2}\omega^2)}SF_{\mathbb{Q}}(t^3-2) = \langle\phi_1\rangle$. There are similar ϕ_i for $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{2}\omega)$ and then $\text{Aut}_{\mathbb{Q}(\omega)}\mathbb{Q}(\sqrt[3]{2}, \omega)$ is generated by the automorphism given by $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}$. □

Proposition 0.78. *Let $\mathbb{M} : \mathbb{K}$ be a finite normal extension. Then the conjugacy classes of $\mathbb{M}$ are precisely the orbits of the action of $Aut_{\mathbb{K}}\mathbb{M}$.*