GALOIS THEORY: SOLUTIONS TO HOMEWORK 1

1. Suppose that $\phi : K_1 \to K_2$ is a field isomorphism, and let $f \in K_1[t]$ be a polynomial with $\deg(f) \geq 1$. Show that f is irreducible in $K_1[t]$ if and only if $\phi(f)$ is irreducible in $K_2[t]$.

   Solution: Suppose that $f = gh$, where $g, h \in K_1[t]$ are polynomials with $\deg(g) \geq 1$ and $\deg(h) \geq 1$. Since ϕ is a field homomorphism (and hence is injective) we have $\phi(f) = \phi(g)\phi(h)$ with $\deg(\phi(g)) = \deg(g)$ and $\deg(\phi(h)) = \deg(h)$. Thus f is not irreducible if and only if $\phi(f)$ is not irreducible, whence f is irreducible if and only if $\phi(f)$ is irreducible.

2. For each of the following pairs of polynomials f and g:
   (i) find the quotient and remainder on dividing g by f;
   (ii) use the Euclidean Algorithm to find the highest common factor h of f and g;
   (iii) find polynomials a and b with the property that $h = af + bg$.

   (a) $g = t^3 + 2t^2 - t + 3$, $f = t + 2$ over $\mathbb{F}_5$;
   (b) $g = t^7 - 4t^6 + t^3 - 4t + 6$, $f = 2t^3 - 2$ over $\mathbb{F}_7$.

   Solution: (a)(i) The quotient is $t^2 - 1$, and remainder 0.
   (ii) We have $g = (t^2 - 1)f$, so a highest common factor of f and g is $f = t + 2$.
   (iii) One has $f = f + 0 \cdot g$, so one may take $a = 1$ and $b = 0$.

   (b)(i) The quotient is $4t^4 - 2t^3 + 4t + 2$, and remainder $4t + 3$.
   (ii) We apply the Euclidean algorithm, noting that $g = (4t^4 - 2t^3 + 4t + 2)f + (4t + 3)$, and then $f = (4t^2 + 4t + 4)(4t + 3)$. Then a highest common factor of f and g is $4t + 3$.
   (iii) Running the Euclidean algorithm backwards, we find that

   $$4t + 3 = g - (4t^4 - 2t^3 + 4t + 2)f,$$

   so that one may take $a = 3t^4 + 2t^3 + 3t + 5$ and $b = 1$.

3. (a) Show that $t^3 + 3t + 1$ is irreducible in $\mathbb{Q}[t]$.
   (b) Suppose that α is a root of $t^3 + 3t + 1$ in $\mathbb{C}$. Express α^{-1} and $(1 + \alpha^2)^{-1}$ as linear combinations, with rational coefficients, of 1, α and α^2.
   (c) Is it possible to express $(1 + \alpha)^{-1}$ as a linear combination, with rational coefficients, of 1 and α? Justify your answer.

   Solution: (a) Suppose that the polynomial $f(t) = t^3 + 3t + 1$ is reducible over $\mathbb{Q}[t]$. Then f must possess a linear factor, and hence a rational root, and the latter may be written in the form p/q with $p \in \mathbb{Z}$, $q \in \mathbb{N}$ and p and q coprime. But then $0 = q^3 f(p/q) = p^3 + 3pq^2 + q^3$, and we find that $p|q$ and $q|p$. Thus $p, q \in \{+1, -1\}$, so that $p/q = \pm 1$. The latter yields a contradiction, since $f(1) = 5$ and $f(-1) = -3$. We consequently conclude that f is irreducible over $\mathbb{Q}[t]$.

   (b) If α is a root of $t^3 + 3t + 1$ in $\mathbb{C}$, then $0 = (\alpha^3 + 3\alpha + 1)/\alpha = \alpha^2 + 3 + 1/\alpha$, whence $\alpha^{-1} = -\alpha^2 - 3$.

   We must work harder to evaluate $(1 + \alpha^2)^{-1}$. We apply the Euclidean algorithm with $t^3 + 3t + 1$ and $t^2 + 1$. Thus we have

   $$\begin{aligned} t^3 + 3t + 1 &= t(t^2 + 1) + 2t + 1 \\ t^2 + 1 &= (\tfrac{1}{2}t - \tfrac{1}{4})(2t + 1) + \tfrac{5}{4}, \end{aligned}$$

whence

$$\begin{aligned}\tfrac{5}{4}&=(t^2+1)-(\tfrac{1}{2}t-\tfrac{1}{4})(2t+1)\\&=(t^2+1)-(\tfrac{1}{2}t-\tfrac{1}{4})(t^3+3t+1-t(t^2+1))\\&=(\tfrac{1}{2}t^2-\tfrac{1}{4}t+1)(t^2+1)-(\tfrac{1}{2}t-\tfrac{1}{4})(t^3+3t+1).\end{aligned}$$

Since $\alpha^3+3\alpha+1=0$, we deduce that $\frac{5}{4}=(\frac{1}{2}\alpha^2-\frac{1}{4}\alpha+1)(\alpha^2+1)$, whence

$$(1+\alpha^2)^{-1}=\tfrac{1}{5}(2\alpha^2-\alpha+4).$$

(c) No, it is not possible to express $(1+\alpha)^{-1}$ as a linear combination $a+b\alpha$ with $a,b\in\mathbb{Q}$. If $(1+\alpha)^{-1}$ were such a linear combination, then one would have $(1+\alpha)(a+b\alpha)=1$. Since α is not rational, we have $\alpha^2=c\alpha+d$ for some $c,d\in\mathbb{Q}$. But then $-3\alpha-1=\alpha^3=c\alpha^2+d\alpha=(c^2+d)\alpha+cd$. Since α is not rational, we must have $cd=-1$ and $c^2+d=-3$, whence $1/d^2+d=-3$, which is to say that $d\in\mathbb{Q}$ satisfies $d^3+3d+1=0$. Since $d\in\mathbb{Q}$, we again contradict that α is not rational.

4. Let K be a field. Recall that the polynomial ring $K[t]$ is a unique factorisation domain. Recall also that a non-zero polynomial $f\in K[t]$ is monic if its leading coefficient is 1, meaning that $f=t^n+a_{n-1}t^{n-1}+\ldots+a_0$ for some $a_{n-1},\ldots,a_0\in K$. Show that $K[t]$ contains infinitely many monic, irreducible polynomials.
(Suggestion: First show that $K[t]$ contains at least one monic, irreducible polynomial. Then assume that $K[t]$ contains only finitely many monic, irreducible polynomials, and derive a contradiction. You might want to review Euclid's proof that there are infinitely many primes.)

Solution: Note that t and $t+1$ are both monic, irreducible elements of $K[t]$, and so such polynomials exist. Suppose that there are only finitely many monic, irreducible elements of $K[t]$. Enumerate these polynomials as $f_1,\ldots,f_m$, and let $g=f_1\cdots f_m+1$. It follows that $\deg g\geq 1$, whence g is not a unit and is not 0. Thus g factors essentially uniquely as a product of irreducible elements of $K[t]$, and since g is monic, these factors may be taken to be monic. Hence, for some index j with $1\leq j\leq m$, we have $f_j|g$. But then f_j divides $g-f_1\ldots f_m$, meaning that f_j divides 1. This is impossible, since any multiple of f_j must have degree at least $\deg f_j\geq 1$, and $\deg 1=0$. We are forced to conclude that $K[t]$ must have infinitely many monic, irreducible polynomials.

5. (a) Show that the polynomial t^2+t+1 is irreducible in $\mathbb{F}_2[t]$.
(b) Give a complete list of the coset representatives of the quotient ring $\mathbb{F}_2[t]/(t^2+t+1)$.
(c) For each of the non-zero elements α of $\mathbb{F}_2[t]/(t^2+t+1)$, determine the least integer n (if one exists) for which $\alpha^n=1$.

Solution: (a) Since $f=t^2+t+1$ has degree 2, if it is reducible then it must have a root in $\mathbb{F}_2$, but $f(0)=f(1)=1$, so this is not the case.

(b) The elements of $\mathbb{F}_2[t]/(f)$ are the cosets $h+(f)$, where $h\in\{at+b:a,b\in\mathbb{F}_2\}=\{0,1,t,t+1\}$.

(c) For $\alpha=1+(f)$, clearly $n=1$ works. For $\alpha=t+(f)$ we have $\alpha^2=t^2+(f)=t+1+(f)$ and $\alpha^3=t(t+1)+(f)=1+(f)$, so $n=3$ works. For $\alpha=t+1+(f)$ we have $\alpha^2=t^2+1+(f)=t+(f)$ and $\alpha^3=t(t+1)+(f)=1+(f)$, so again $n=3$ works.

GALOIS THEORY: SOLUTIONS TO HOMEWORK 2

1. Let $L : K$ be a field extension, and suppose that $\theta \in L$ satisfies the property that $[K(\theta) : K] = p$, where p is a prime number. Let

$$\alpha = c_0 + c_1\theta + \ldots + c_{p-1}\theta^{p-1},$$

for some $c_0, \ldots, c_{p-1} \in K$, and suppose that $\alpha \notin K$. By considering $[K(\alpha) : K]$, show that $K(\alpha) = K(\theta)$.

Solution: We have $K(\alpha) \subseteq K(\theta)$, so the tower law yields

$$[K(\theta) : K(\alpha)][K(\alpha) : K] = [K(\theta) : K],$$

whence $[K(\alpha) : K]$ divides $[K(\theta) : K] = p$. Since p is a prime, we therefore see that $[K(\alpha) : K] \in \{1, p\}$. But $\alpha \notin K$, by hypothesis, so $[K(\alpha) : K] \neq 1$. Then we conclude that $[K(\alpha) : K] = p$. By the tower law again, it follows that

$$[K(\theta) : K(\alpha)] = [K(\theta) : K]/[K(\alpha) : K] = 1,$$

and thus $K(\theta) = K(\alpha)$.

2. Let $L : K$ be a field extension with $K \subseteq L$. Let $A \subseteq L$, and let

$$\mathcal{C} = \{C \subseteq A : C \text{ is a finite set}\}.$$

Show that $K(A) = \cup_{C\in\mathcal{C}} K(C)$, and further that when $[K(C) : K] < \infty$ for all $C \in \mathcal{C}$, then $K(A) : K$ is an algebraic extension.

Solution: The field $K(A)$ is the smallest subfield of L containing K and A. Thus, for all $C \in \mathcal{C}$, the field $K(A)$ must contain $K(C)$. So $\cup_{c\in\mathcal{C}} K(C) \subseteq K(A)$.

Now take $\gamma \in K(A)$. Then γ is a quotient of finite K-linear combinations of powers of elements of A. Since this K-linear combination is finite, there is a finite set $D \subseteq A$ so that γ is a quotient of K-linear combinations of powers of elements in D. We therefore have $D \in \mathcal{C}$ and $\gamma \in K(D)$. Thus $K(A) \subseteq \cup_{C\in\mathcal{C}} K(C)$.

We now address the final claim. Take $\alpha \in K(A)$. Then $\alpha \in K(C)$ for some $C \in \mathcal{C}$. Thus we deduce via the tower law that $[K(C) : K(\alpha)][K(\alpha) : K] = [K(C) : K] < \infty$, whence $[K(\alpha) : K] < \infty$. We therefore conclude that α is algebraic over K. Since this holds for all $\alpha \in K(A)$, we have that $K(A) : K$ is an algebraic extension.

3. Let $L : K$ be a field extension, and suppose that $\gamma \in L$ satisfies the property that $\deg m_\gamma(K) = 5$. Suppose that $h \in K[t]$ is a non-zero cubic polynomial. By noting that γ is a root of the cubic polynomial $g(t) = h(t) - h(\gamma) \in K(h(\gamma))[t]$, show that $[K(h(\gamma)) : K] = 5$.

Solution: One has $K \subseteq K(h(\gamma)) \subseteq K(\gamma) \subseteq L$. Then by the tower law, we find that $[K(\gamma) : K] = [K(\gamma) : K(h(\gamma))][K(h(\gamma)) : K]$, whence $[K(\gamma) : K(h(\gamma))]$ divides $[K(\gamma) : K]$. But the degree of the minimal polynomial of γ over K is 5, so that $[K(\gamma) : K] = 5$. We therefore see that $[K(\gamma) : K(h(\gamma))] \in \{1, 5\}$. But over the field $K(h(\gamma))$, the element γ satisifies the cubic equation $h(t) - h(\gamma) = 0$, and thus the minimal polynomial of γ over $K(h(\gamma))$ divides the latter cubic polynomial, so has degree 1, 2 or 3. Consequently, we must have $[K(\gamma) : K(h(\gamma))] \in \{1, 2, 3\}$. In view of our earlier observation, we are forced to conclude that the latter degree is 1, and then the previous application of the tower law implies that $[K(h(\gamma)) : K] = 5$, which is to say that the minimal polynomial of $h(\gamma)$ over K has degree 5.

4. Calculate the minimal polynomial of $\sqrt[5]{7+\sqrt[3]{21}}$ over $\mathbb{Q}$, and hence determine the degree of the field extension $\mathbb{Q}(\sqrt[5]{7+\sqrt[3]{21}}):\mathbb{Q}$.

Solution: Write $\alpha = \sqrt[5]{7+\sqrt[3]{21}}$. Then $\alpha^5 - 7 = \sqrt[3]{21}$, and hence $(\alpha^5-7)^3 = 21$. On putting $f(x) = (x^5-7)^3 - 21 = x^{15} - \ldots - (7^3+21)$, we see that $f(\alpha) = 0$, and thus it follows that the minimal polynomial $m_\alpha(\mathbb{Q})$ of α divides f. But by applying Eisenstein's criterion using the prime 7, we see that f is irreducible: the lead coefficient of f is not divisible by 7, all other coefficients are divisible by 7, and the constant coefficient $-(7^3+21)$ is divisible by 7 but not by 7^2. Hence f is the minimal polynomial of α over $\mathbb{Q}$. The degree of the field extension $\mathbb{Q}(\sqrt[5]{7+\sqrt[3]{21}}):\mathbb{Q}$ is therefore equal to $\deg f = 15$.

5. Let $\mathbb{Q}(\alpha):\mathbb{Q}$ be a simple field extension with the property that the minimal polynomial of α is t^3+2t-2. Calculate the minimal polynomials of $\alpha - 1$ and α^2+1 over $\mathbb{Q}$, and express the multiplicative inverses of these elements in $\mathbb{Q}(\alpha)$ in the form $c_0 + c_1\alpha + c_2\alpha^2$ for suitable rational numbers c_0, c_1, c_2.

Solution: Write $\beta = \alpha - 1$. Then $\alpha = \beta + 1$, so that on substituting into the relation $\alpha^3 + 2\alpha - 2 = 0$ implied by the minimal polynomial of α, we obtain

$$0 = (\beta+1)^3 + 2(\beta+1) - 2 = \beta^3 + 3\beta^2 + 5\beta + 1.$$

Then the minimal polynomial of β divides $f(t) = t^3 + 3t^2 + 5t + 1$. Since the latter polynomial is cubic, if it is not irreducible it has a linear factor, and by Gauss' Lemma that factor may be written with integral coefficients. But since (consider the leading and final coefficients) $t \pm 1$ are the only possible such factors, and $f(\pm 1) \neq 0$, we must conclude that no such factor exists, and hence $f(t)$ is irreducible. Then $\alpha - 1$ has minimal polynomial $t^3 + 3t^2 + 5t + 1$.

Next consider $(\alpha-1)^{-1}$. One has $(\alpha-1)^3 + 3(\alpha-1)^2 + 5(\alpha-1) + 1 = 0$, and hence $(\alpha-1)^{-1} = -(\alpha-1)^2 - 3(\alpha-1) - 5 = -\alpha^2 - \alpha - 3$.

Next write $\gamma = \alpha^2 + 1$. We aim to seek a polynomial relation satisfied by γ in stages. Observe first that since $\alpha^3 + 2\alpha - 2 = 0$, one has

$$\gamma^2 = (\alpha^2+1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(\alpha^3 + 2\alpha - 2) + 2\alpha + 1 = 2\alpha + 1,$$

and hence

$$\gamma^3 = \gamma(2\alpha+1) = (\alpha^2+1)(2\alpha+1) = 2(\alpha^3+2\alpha-2) + \alpha^2 - 2\alpha + 5 = \gamma - 2\alpha + 4.$$

Then $\gamma^3 + \gamma^2 = \gamma + 5$, whence the minimal polynomial of γ divides $g(t) = t^3 + t^2 - t - 5$. Since the latter polynomial is cubic, if it is not irreducible it has a linear factor, and by Gauss' Lemma that factor may be written with integral coefficients. But since (consider the leading and final coefficients) $t \pm 1$ and $t \pm 5$ are the only possible such factors, and $f(\pm 1) \neq 0$ and $f(\pm 5) \neq 0$, we must conclude that no such factor exists, and hence $g(t)$ is irreducible. Then $\alpha^2 + 1$ has minimal polynomial $t^3 + t^2 - t - 5$.

Next consider $(\alpha^2+1)^{-1}$. One has

$$5(\alpha^2+1)^{-1} = \gamma^2 + \gamma - 1 = (2\alpha+1) + (\alpha^2+1) - 1 = \alpha^2 + 2\alpha + 1,$$

and hence $(\alpha^2+1)^{-1} = \frac{1}{5}(\alpha^2 + 2\alpha + 1)$.

GALOIS THEORY: SOLUTIONS TO HOMEWORK 3

1. (a) Show that when p is a prime number, then for every positive integer n the polynomial $X^n - p$ is irreducible over $\mathbb{Q}[X]$.
(b) By making the substitution $y = X - 1$, or otherwise, show that when p is a prime number, the polynomial $X^{p-1} + X^{p-2} + \cdots + X + 1$ is irreducible over $\mathbb{Q}$.

Solution: (a) The polynomial $X^n - p$ has leading coefficient not divisible by p, all other coefficients divisible by p, and final coefficient not divisible by p^2. Then Eisenstein's criterion applies, and establishes that $X^n - p$ is irreducible.
(b) Write $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$. Then one has $(x-1)f(x) = x^p - 1$. Now substitute $x = y + 1$, and we find that

$$yf(y+1) = (y+1)^p - 1 = y^p + \sum_{i=1}^{p-1} \binom{p}{i} y^i = yg(y),$$

say. But since each binomial coefficient $\binom{p}{i}$ is divisible by p for $1 \le i \le p-1$, we find that g has leading coefficient not divisible by p, all other coefficients divisible by p, and final coefficient p not divisible by p^2. Then Eisenstein's criterion applies, and shows that g is irreducible. But by uniqueness of factorisation, one has $g(x-1) = f(x)$, and thus f must also be irreducible.

2. (a) Show that the polynomial $\phi = t^3 - t + 1$ is irreducible over the ring $\mathbb{I} = \mathbb{F}_3[t]$.
(b) Let $\mathbb{K} = \mathbb{F}_3(t)$. Show that the polynomial $X^{2024} + \phi X^2 + \phi$ is irreducible over $\mathbb{K}[X]$.

Solution: (a) If ϕ fails to be irreducible over $\mathbb{I}$, then it has a linear factor, and the only monic such factors over $\mathbb{I}$ are t and $t \pm 1$. But $\phi = t(t+1)(t-1) + 1$, so none of these factors divide f (they leave remainder 1 in each case). Hence ϕ is irreducible over $\mathbb{I}$.
(b) Over $\mathbb{I}[X]$, we see that the leading coefficient of $g = X^{2024} + \phi X^2 + \phi$ is not divisible by ϕ, all other coefficients are divisible by ϕ, and the final coefficient is not divisible by ϕ^2. Since ϕ is irreducible over $\mathbb{I}$, we therefore deduce via Eisenstein's criterion that g is irreducible over $\mathbb{I}[X]$. But then it follows from Gauss' lemma that g is also irreducible over $\mathbb{K}[X]$, since $\mathbb{K}$ is the field of fractions of $\mathbb{I}$.

3. Let $L : K$ be a field extension. Suppose that $\alpha \in L$ is algebraic over K and $\beta \in L$ is transcendental over K. Suppose also that $\alpha \notin K$. Show that $K(\alpha, \beta) : K$ is not a simple field extension.

Solution: Suppose that $K(\alpha, \beta) = K(\gamma)$ for some $\gamma \in L$. Since $\beta \in K(\gamma)$ is transcendental over K, the field extension $K(\gamma) : K$ is not algebraic, and hence γ is transcendental over K. Since $\alpha \in K(\gamma)$, we have $\alpha = f(\gamma)/g(\gamma)$ for some $f, g \in K[t]$ with $g \neq 0$. Thus γ is a root of $h = \alpha g - f \in K(\alpha)[t]$. Since $\alpha \notin K$ and $g \neq 0$, the polynomial h cannot be the zero polynomial, and therefore γ is algebraic over $K(\alpha)$. But then, since α is algebraic over K, this implies that $[K(\gamma) : K] = [K(\gamma) : K(\alpha)][K(\alpha) : K] < \infty$, contradicting the transcendence of γ. So $K(\alpha, \beta) : K$ cannot be a simple extension.

4. (a) Show that the polynomial $f(t) = t^7 - 7t^5 + 14t^3 - 7t - 2$ factorises over $\mathbb{Q}[t]$ in the form $f = g_1 g_3^2$, where $g_1, g_3 \in \mathbb{Z}[t]$ have the property that g_1 is linear, and g_3 is cubic and irreducible.

(b) Using the identity

$$\cos 7\theta = 64\cos^7\theta - 112\cos^5\theta + 56\cos^3\theta - 7\cos\theta,$$

together with the conclusion of part (a), show that the angle $2\pi/7$ is not constructible by ruler and compass. Hence deduce that the regular heptagon is not constructible by ruler and compass.

Solution: (a) By Gauss' Lemma, any linear factor of f must have the shape $t \pm 1$ or $t \pm 2$. Since $f(2) = 0$, we find that f is divisible by $t - 2$, and by long division we find further that

$$\begin{aligned} f &= (t-2)(t^6 + 2t^5 - 3t^4 - 6t^3 + 2t^2 + 4t + 1) \\ &= (t-2)(t^3 + t^2 - 2t - 1)^2. \end{aligned}$$

We therefore have $f = g_1 g_3^2$, with $g_1 = t - 2$ and $g_3 = t^3 + t^2 - 2t - 1$. It remains only to check that g_3 is irreducible. But if it has a factor of positive degree, then it must have a linear factor, and this would necessarily have the shape $t \pm 1$. Since neither of these possibilities is a factor of g_3, we see that g_3 is indeed irreducible.
(b) We seek to derive a contradiction. If $\theta = 2\pi/7$ were constructible, then so too would be the point $(\cos\theta, \sin\theta) \in \mathbb{R}^2$, and hence $[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = 2^r$ for some $r \in \mathbb{Z}_{\geq 0}$. Putting $\sigma = 2\cos\theta$, we deduce via the provided polynomial identity that

$$\begin{aligned} \sigma^7 - 7\sigma^5 + 14\sigma^3 - 7\sigma - 2 &= 2(64\cos^7\theta - 112\cos^5\theta + 56\cos^3\theta - 7\cos\theta - 1) \\ &= 2(\cos 2\pi - 1) = 0, \end{aligned}$$

whence $f(\sigma) = 0$. Since $\sigma \neq 2$, we deduce that σ is a root of the irreducible polynomial g_3, whence $[\mathbb{Q}(\sigma) : \mathbb{Q}] = \deg g_3 = 3$. This is in contradiction to the assumption that $[\mathbb{Q}(\cos\theta) : \mathbb{Q}]$ is a power of 2, and thus we deduce that θ is not constructible. If the regular heptagon were to be constructible, then $2\pi/7$ would be constructible, contradicting the last conclusion (consider the angle suspended by one of the sides). Thus regular heptagons are not constructible.

5. Assume (as has in fact been proved) that $\pi = 3.14159\ldots$ is transcendental over $\mathbb{Q}$.
(a) Show that one cannot "square the circle" – that is, prove that $\sqrt{\pi}$ is not constructible by ruler and compass.
(b) Suppose that a generous benefactor has given you the points $(0, 0)$, $(0, 1)$ and $(0, \pi)$ in the plane. Can you now construct $\pi^{1/5}$ by ruler and compass from these three points? Explain your answer.

Solution: (a) Suppose that $\sqrt{\pi}$ is construcible by ruler and compass, so that for some non-negative integer r one has $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = 2^r$. Observe that $\mathbb{Q}(\pi) \subseteq \mathbb{Q}(\sqrt{\pi})$, and (since π is transcendental over $\mathbb{Q}$), one has $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$. Thus

$$2^r = [\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] \geq [\mathbb{Q}(\pi) : \mathbb{Q}] = \infty,$$

yielding a contradiction. Hence $\sqrt{\pi}$ is indeed not constructible by ruler and compass.
(b) Write K for the minimal field containing all of the coordinates of the initial points, so that $K = \mathbb{Q}(\pi)$. Suppose that $\pi^{1/5}$ is constructible in the manner asserted. Then $[K(\pi^{1/5}) : K] = 2^r$, for some non-negative integer r. Let f be the minimal polynomial of $\pi^{1/5}$ over K. Then since $\pi^{1/5}$ is a zero of $t^5 - \pi \in K[t]$, it follows that f divides $t^5 - \pi$.

From here one can adopt several strategies. The high-brow approach is to observe that the mapping $\psi : \mathbb{Q}(\pi) \to \mathbb{Q}(x)$, defined by taking a rational function $h(\pi)$ and putting $\psi(h(\pi)) = h(x)$, gives an isomorphism. This follows because π is transcendental over $\mathbb{Q}$, and hence $\ker(\psi)$ is trivial. From here we see that $t^5 - \pi$ is irreducible over K if and only if $t^5 - x$ is irreducible over $\mathbb{Q}(x)$. But $\mathbb{Q}[x]$ is a UFD, so the lemma of Gauss shows that $t^5 - x$ is irreducible over $\mathbb{Q}(x)$ if and only if $t^5 - x$ is irreducible over $\mathbb{Q}[x]$. However, the element x is irreducible over $\mathbb{Q}[x]$, so the irreducibility of $t^5 - x$ follows from Eisenstein's criterion using the irreducible element x. We conclude that $t^5 - \pi$ is also irreducible over K, and hence $[K(\pi^{1/5}) : K] = 5$. Since $5 \neq 2^r$, for any non-negative integer r, we derive a contradiction to our initial assumption, and conclude that π^5 is not construcible from this initial set of points.

An alternate brute force approach proceeds as follows. We have $[K(\pi^{1/5}) : K] = \deg(f)$, and this must divide 2^r, so that $\deg(f) \in \{1, 2, 4\}$. Also, we see that f divides $t^5 - \pi$, so that f has roots of the shape $\omega^i \pi^{1/5}$ for some integer i, where ω is a primitive 5-th root of 1. In all of these cases, the constant term $\beta \in \mathbb{Q}(\pi)$ of f is the product of these roots, and thus $\beta^5 = \pi^c$ where $c \in \{1, 2, 4\}$. Hence there exist $g, h \in \mathbb{Q}[t]$, with g non-zero, such that $\pi^c = g(\pi)/h(\pi)$. There is no loss of generality in supposing that the constant term of either g or h is non-zero, by removing common factors of t between g and h. We now see that $g(\pi)^5 = \pi^c h(\pi)^5$, which gives a polynomial $k(t) = g(t)^5 - t^c h(t)^5 \in \mathbb{Q}[t]$ having the zero π. Since π is transcendental over $\mathbb{Q}$, any such polynomial must be identically zero, and thus we see in particular that its constant term must be 0, whence the constant term of g must also be 0. Examining the coefficient of t, since $g(t)^5$ now is seen to have a factor t^5, we find that $h(t)$ must have constant term 0. Then g and h both have constant term 0, contradicting our earlier assumption. Thus, we see that $\pi^{1/5}$ is not, after all, constructible in the prescribed manner.

GALOIS THEORY: SOLUTIONS TO HOMEWORK 4

1. (a) By considering the substitution $t = x + 1$ and applying Eisenstein's criterion, show that the polnomial $t^6 + t^3 + 1$ is irreducible over $\mathbb{Q}[t]$.

   (b) Suppose, if possible, that $[\mathbb{Q}(\cos(2\pi/9), \sin(2\pi/9)) : \mathbb{Q}] = 2^r$, for some non-negative integer r. Prove that the 9-th root of unity $\omega = \cos(2\pi/9) + i\sin(2\pi/9)$ satisfies the property that $[\mathbb{Q}(\omega) : \mathbb{Q}]$ divides 2^{r+1}.

   (c) By considering the factorisation of $t^9 - 1$ over $\mathbb{Q}[t]$, prove that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 6$. Hence deduce that the angle $2\pi/9$ is not constructible by ruler and compass, whence the regular nonagon cannot be constructed by ruler and compass.

   Solution: (a) We have $(x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$. This polynomial is irreducible over $\mathbb{Q}[x]$ by Gauss' Lemma and Eisenstein's criterion using the prime 3 (this monic polynomial has all save the leading coefficient divisible by 3, and constant coefficient not divisible by 3^2). But if $(x + 1)^6 + (x + 1)^3 + 1$ is irreducible, then so too is $t^6 + t^3 + 1$.

   (b) Write $K = \mathbb{Q}(\cos(2\pi/9), \sin(2\pi/9))$. Then $\omega \in K(i)$. Hence, by the tower law, one has $[K(i) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = [K(i) : K][K : \mathbb{Q}] = [K(i) : \mathbb{Q}]$. But i is a root of the polynomial $t^2 + 1$ over K, and hence its minimal polynomial has degree 1 or 2. Thus $[K(i) : K] \in \{1, 2\}$. The question directs us to assume that $[K : \mathbb{Q}] = 2^r$, and thus $[K(i) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] \in \{2^r, 2^{r+1}\}$. Then in any case $[\mathbb{Q}(\omega) : \mathbb{Q}]$ divides 2^{r+1}.

   (c) We have $\omega^3 \neq 1$ and $\omega^9 = 1$, so ω is a root of the polynomial $t^9 - 1 = (t^3 - 1)(t^6 + t^3 + 1)$ but not a root of $t^3 - 1$. Then ω must be a root of the irreducible polynomial $t^6 + t^3 + 1$. Thus $m_\omega(\mathbb{Q}) = t^6 + t^3 + 1$, whence $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(t^6 + t^3 + 1) = 6$. But 6 does not divide 2^{r+1} for $r \in \mathbb{Z}_{\geq 0}$, contradicting the assumption that $[K : \mathbb{Q}] = 2^r$. Thus $\cos(2\pi/9)$ and $\sin(2\pi/9)$ are not both constructible by ruler and compass, whence the angle $2\pi/9$ is not constructible. But the construction of a regular nonagon would entail constructing the angle $2\pi/9$, so such cannot be constructed by ruler and compass.

2. (a) Suppose that $P_0, P_1, \ldots, P_n$ are points in $\mathbb{R}^2$ whose coordinates lie in a field extension K of $\mathbb{Q}$. Let $P = (x, y)$ be a point of intersection of two ellipses with equations defined over K. Explain why $[K(x, y) : K] \leq 4$.

   (b) Let $P_0 = (0, 0)$ and $P_1 = (1, 0)$, and suppose that $P_2, P_3, \ldots$ are constructed successively by simple cord-and-nail constructions (as discussed in Definition 13 of section 2.3 from the notes). Let j be a positive integer, write $P_j = (x_j, y_j)$, and put $L_j = \mathbb{Q}(x_j, y_j)$. Explain why, for some non-negative integers r and s, one has $[L_j : \mathbb{Q}] = 2^r 3^s$.

   Solution: (a) We can assume that the equations of the two ellipses in question are

   $$c_{20}x^2 + c_{11}xy + c_{02}y^2 + c_{10}x + c_{01}y + c_{00} = 0,$$

   with $c_{ij} \in K$, and

   $$d_{20}x^2 + d_{11}xy + d_{02}y^2 + d_{10}x + d_{01}y + d_{00} = 0,$$

   with $d_{ij} \in K$. By eliminating the x^2 term, we obtain a new equation of the shape

   $$e_{11}xy + e_{02}y^2 + e_{10}x + e_{01}y + e_{00} = 0.$$

   If both e_{11} and e_{10} are zero, then this new equation is independent of x and we may solve for y (or possibly all terms except the constant one are zero, and there is no solution).

Then y lies in a quadratic field extension of K, and by back substitution we find that at worst x lies in a quadratic field extension of this first extension. Otherwise, when one at least of e_{11} and e_{10} is non-zero, then we may substitute for x from this equation into the first so as to obtain a quartic equation for y. Back substituting into the linear equation for x then shows that x lies in the same quartic field extension. The latter conclusion, then, remains true in both cases, and $[K(x,y):K] \leq 4$.

(b) We expand on the conclusion of part (a) a little. Let $P_i = (x_i, y_i) \in K^2$ $(i \geq 0)$. Then the ellipse defined by taking P_j and P_k as foci, and P_l a third point on the ellipse, has equation given by

$$\sqrt{(x-x_j)^2+(y-y_j)^2} = \sqrt{(x_l-x_i)^2+(y_l-y_i)^2} + \sqrt{(x_l-x_k)^2+(y_l-y_k)^2} \\ - \sqrt{(x-x_k)^2+(y-y_k)^2}.$$

The coefficients here all lie in K, and moreover the distance between any two points from $\{P_1, \ldots, P_n\}$ all lie in a field extension K_0 of K with $[K_0 : K] = 2^m$ for some non-negative integer m. We see this by adjoining the relevant square-roots of elements of K in sequence, making use of the Tower Law. By squaring and cancelling terms, and squaring again to remove the final square-root, we obtain an equation of the first shape described in part (a), with $c_{ij} \in K_0$. The intersection of such a curve with a line generates points lying in a quadratic field extension, as is the case for ruler-and-compass constructions. If instead we consider the intersection of such a curve with a second such curve (of the second shape described in part (a), with $d_{ij} \in K_0$), then we are in the situation considered in part (a). In such circumstances we find that any point of intersection (x,y) satisfies the property that $[K_0(x,y) : K_0] \leq 4$. Hence, as a consequence of the Tower Law we conclude that $[K_0(x,y) : K] = 2^m u$ for some integer u with $1 \leq u \leq 4$.

Now put $M_0 = \mathbb{Q}$ and $M_j = M_{j-1}(x_j, y_j)$ $(j \geq 1)$. By part (a), one has $[M_j : M_{j-1}] = 2^{m_j}3^{n_j}$ for some $m_j \geq 0$ and $n_j \in \{0,1\}$ for each j. Then it follows from the Tower Law that

$$[M_j : \mathbb{Q}] = [M_j : M_{j-1}][M_{j-1} : M_{j-2}] \ldots [M_1 : M_0]$$

is a product of terms, each of the shape $2^u 3^v$, and hence divisible only by 2 or 3. Then $[M_j : \mathbb{Q}] = 2^a 3^b$ for some $a, b \in \mathbb{Z}_{\geq 0}$. But, again by the Tower Law, since $L_j \subseteq M_j$, we have $[M_j : L_j][L_j : \mathbb{Q}] = [M_j : \mathbb{Q}] = 2^a 3^b$, so that $[L_j : \mathbb{Q}]$ is a divisor of $2^a 3^b$. Then we are forced to conclude that $[L_j : \mathbb{Q}] = 2^r 3^s$ for some $r, s \in \mathbb{Z}_{\geq 0}$, as required.

3. (a) Prove that the polynomial $t^5 - 2$ is irreducible over $\mathbb{Q}[t]$.
   (b) Prove that $2^{1/5}$ is not constructible by cord-and-nail.

   Solution: (a) The polynomial $t^5 - 2$ is irreducible over $\mathbb{Q}$, by Eisenstein's criterion using the prime 2, since this polynomial is monic, has 2 dividing all coefficients save the leading coefficient, and 2^2 does not divide the constant term.

   (b) Let $\theta = 2^{1/5}$. Then θ is a root of the monic irreducible polynomial $t^5 - 2$, and hence has the latter as its minimal polynomial over $\mathbb{Q}$. Thus $[\mathbb{Q}(\theta) : \mathbb{Q}] = \deg(t^5 - 2) = 5$. But if $\theta = 2^{1/5}$ lies in some field L constructible by cord-and-nail, then $\mathbb{Q}(\theta) \subseteq L$. By the tower law and question 2(b), therefore, there exist $r, s \in \mathbb{Z}_{\geq 0}$ having the property that $[L : \mathbb{Q}(\theta)][\mathbb{Q}(\theta) : \mathbb{Q}] = 2^r 3^s$, which implies that 5 divides $2^r 3^s$. The latter yields a contradiction, and so $2^{1/5}$ is not constructible by cord-and-nail.

4. Suppose that $L : K$ is a field extension with $K \subseteq L$, and that $\tau : L \to L$ is a K-homomorphism. Suppose also that $f \in K[t]$ has the property that $\deg f \geq 1$, and additionally that $\alpha \in L$.

(a) Show that when $f(\alpha) = 0$, then $f(\tau(\alpha)) = 0$.
(b) Deduce that when τ is a K-automorphism of L, we have that $f(\alpha) = 0$ if and only if $f(\tau(\alpha)) = 0$.

Solution: (a) Write $f = c_0 + c_1 t + \ldots + c_n t^n$, where $c_n \neq 0$, and suppose that $f(\alpha) = 0$. Since $f \in K[t]$, we have $c_i \in K$ for each i. Hence, since τ is a K-homomorphism,

$$0 = \tau(f(\alpha)) = c_0 + c_1\tau(\alpha) + \ldots + c_n(\tau(\alpha))^n = f(\tau(\alpha)).$$

(b) If τ is a K-automorphism of L, then $\tau^{-1} : L \to L$ exists and is a K-homomorphism. Thus, as in (a), when $f(\tau(\alpha)) = 0$, we have $0 = \tau^{-1}(f(\tau(\alpha))) = f(\tau^{-1}(\tau(\alpha))) = f(\alpha)$. Thus $f(\alpha) = 0$ if and only if $f(\tau(\alpha)) = 0$.

5. Let $L : K$ be a field extension. Show that $\mathrm{Gal}(L : K)$ is a subgroup of $\mathrm{Aut}(L)$.

Solution: Suppose first that $K \subseteq L$. Since the identity map ι on L is in $\mathrm{Aut}(L)$, and it leaves K pointwise fixed, we have $\iota \in \mathrm{Gal}(L : K)$. Now consider $\sigma, \tau \in \mathrm{Gal}(L : K)$. Thus $\sigma, \tau \in \mathrm{Aut}(L)$, and hence $\sigma \circ \tau$ and σ^{-1} both lie in $\mathrm{Aut}(L)$. Also, for each $\alpha \in K$, we have $\sigma(\alpha) = \alpha$ and $\tau(\alpha) = \alpha$, since σ and τ leave K pointwise fixed. Thus we have $\sigma \circ \tau(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha) = \alpha$. Also, one has $\sigma^{-1}(\alpha) = \alpha$ for all $\alpha \in K$ (for we have $\sigma^{-1}(\beta) = \alpha$ for the value of β satisfying $\sigma(\beta) = \alpha$). Hence $\sigma \circ \tau$ and σ^{-1} both lie in $\mathrm{Gal}(L : K)$, whence $\mathrm{Gal}(L : K)$ is a subgroup of $\mathrm{Aut}(L)$.

Now suppose that $L : K$ is a field extension relative to an embedding $\varphi : K \to L$. Then in the above argument, for $\alpha \in K$ we have $\sigma(\varphi(\alpha)) = \varphi(\alpha)$ and $\tau(\varphi(\alpha)) = \varphi(\alpha)$, and so $\sigma \circ \tau(\varphi(\alpha)) = \varphi(\alpha)$ and $\sigma^{-1}(\varphi(\alpha)) = \varphi(\alpha)$. Thus the identity map, together with $\sigma \circ \tau$ and σ^{-1} are K-homomorphisms. Thus $\mathrm{Gal}(L : K)$ is a subgroup of $\mathrm{Aut}(L)$.

GALOIS THEORY: SOLUTIONS TO HOMEWORK 5

1. Suppose that $L : F$ and $L : F'$ are finite extensions with $F \subseteq L$ and $F' \subseteq L$, and further that $\psi : F \to F'$ is an isomorphism. Explain why there are at most $[L : F]$ ways to extend ψ to a homomorphism from L into L. [This is Corollary 3.6 – consider F-homomorphisms acting on L.]

   Solution: We apply the argument of the proof of Theorem 3.5, writing $K_0 = F$ and $K_0' = F'$, and taking $\sigma_0 = \psi$ as the isomorphism mapping K_0 into K_0' in place of the identity map. The remainder of the proof of Theorem 3.5 now remains identical, and shows that there are at most $[L : F]$ ways of extending $\sigma_0 = \psi$ to a homomorphism from L into L, as required.

2. Let M be a field. Show that the following are equivalent:
   (i) the field M is algebraically closed;
   (ii) every non-constant polynomial $f \in M[t]$ factors in $M[t]$ as a product of linear factors;
   (iii) every irreducible polynomial in $M[t]$ has degree 1;
   (iv) the only algebraic extension of M containing M is M itself.

   Solution: Suppose that (i) holds. Consider $f \in M[t] \setminus M$, and note that f has a root $\alpha_1 \in M$. With $n = \deg f$, we define g_i inductively as follows. Define $g_1 \in M[t]$ by means of the relation $f = (t - \alpha_1)g_1$. Then, for $1 < i \leq n$, define $g_i \in M[t]$ by means of the relation $g_{i-1} = (t - \alpha_i)g_i$. Since $\deg g_i = n - i$, we see that g_{i-1} is non-constant for $1 < i \leq n$, and hence has a root $\alpha_i \in M$. We note in this context that $g_n \in M^\times$ is the leading coefficient of f. Thus $f = g_n(t - \alpha_1) \cdots (t - \alpha_n)$, and thus (i) implies (ii).

   Suppose next that (ii) holds, and suppose that $f \in M[t]$ is irreducible. Then f is non-zero and non-constant. Since f factors as a product of $\deg f$ linear factors, we must have $\deg f = 1$, and thus (ii) implies (iii).

   Next suppose that (iii) holds, and suppose that α lies in some algebraic extension field N extending M. Assume $M \subseteq N$. Then α is algebraic over M, and hence there is some irreducible polynomial $m_\alpha(M) \in M[t]$, which, in view of the hypothesis (iii), has degree 1. Since this polynomial is also monic, we infer that $t - \alpha = m_\alpha(M) \in M[t]$, whence $\alpha \in M$. But then $N = M$, and so (iii) implies (iv).

   Finally, suppose that (iv) holds. Let $f \in M[t] \setminus M$, and let N be a field extension of M with $M \subseteq N$ containing a root α of f. Then $M(\alpha) : M$ is an algebraic extension. The hypothesis (iv) thus implies that $M(\alpha) = M$, whence $\alpha \in M$. Then (iv) implies (i).

   In this way, we have confirmed the equivalence of (i), (ii), (iii) and (iv).

GALOIS THEORY: SOLUTIONS TO HOMEWORK 6

1. Suppose that L and M are fields with an associated homomorphism $\psi : L \to M$. Show that whenever L is algebraically closed, then $\psi(L)$ is also algebraically closed.

   Solution: Suppose that L is algebraically closed, and that $f' \in \psi(L)[t]$ is irreducible. Then we have $f' = \psi(f)$ for some $f \in L[t]$, and $\deg f' = \deg f$. For the sake of deriving a contradiction, suppose that $\deg f' > 1$. Then $\deg f > 1$. Since L is algebraically closed, it follows that irreducible polynomials in $L[t]$ have degree 1. We are forced to conclude, therefore, that f is reducible, and hence that $f = gh$ for some polynomials $g, h \in L[t]$ with $\deg g \geq 1$ and $\deg h \geq 1$. Consequently, we have $f' = g'h'$, where $g' = \psi(g)$ and $h' = \psi(h)$ satisfy the property that $\deg g' \geq 1$ and $\deg h' \geq 1$. However, this contradicts the assumption that f' is irreducible in $\psi(L)[t]$. We must therefore have $\deg f' = 1$. Thus we conclude that $\psi(L)$ is algebraically closed.

2. Let $L : K$ be a field extension with $K \subseteq L$. Let $\gamma \in L$ be transcendental over K, and consider the simple field extension $K(\gamma) : K$. Show that $K(\gamma)$ is not algebraically closed.

   Solution: Put $M = K(\gamma)$, and suppose that M is algebraically closed. We show that the polynomial $t^2 - \gamma$ is irreducible over $M[t]$, contradicting that M is algebraically closed, and thereby establishing the desired conclusion. Suppose then that $\alpha \in M$ satisfies the relation $\alpha^2 = \gamma$. Since $\alpha \in M = K(\gamma)$, it follows that there exists $n, m \in \mathbb{Z}_{\geq 0}$ and $a_i, b_i \in K$ $(0 \leq i \leq n)$, with $a_n \neq 0$ and $b_m \neq 0$, having the property that

   $$\alpha = \frac{a_0 + a_1\gamma + \ldots + a_n\gamma^n}{b_0 + b_1\gamma + \ldots + b_m\gamma^m},$$

   whence

   $$(a_0 + a_1\gamma + \ldots + a_n\gamma^n)^2 = \gamma(b_0 + b_1\gamma + \ldots + b_m\gamma^m)^2.$$

   Hence

   $$a_n^2\gamma^{2n} + \ldots + a_0^2 = b_m^2\gamma^{2m+1} + \ldots + b_0^2\gamma.$$

   Either $2n > 2m + 1 \geq 1$, in which case γ is a root of the polynomial

   $$a_n^2 t^{2n} + \ldots + a_0^2 \in K[t] \setminus K,$$

   or else $2m + 1 > 2n \geq 0$, in which case γ is a root of the polynomial

   $$b_m^2 t^{2m+1} + \ldots - a_0^2 \in K[t] \setminus K.$$

   We therefore deduce that γ is algebraic over K, contradicting our hypotheses that γ is transcendental over K. Thus $K(\gamma)$ cannot be algebraically closed.

GALOIS THEORY: SOLUTIONS TO HOMEWORK 7

1. Suppose that $\overline{K}$ is an algebraic closure of K, and assume that $K \subseteq \overline{K}$. Take $\alpha \in \overline{K}$ and suppose that $\sigma : K \to \overline{K}$ is a homomorphism.
(a) Show that σ can be extended to a homomorphism $\tau : \overline{K} \to \overline{K}$.
(b) Prove that the number of distinct roots of $m_\alpha(K)$ in $\overline{K}$ is equal to the number of distinct roots of $\sigma(m_\alpha(K))$ in $\overline{K}$.
Solution: (a) Since $\overline{K}$ is an algebraic extension of K with $K \subseteq \overline{K}$, and $\sigma : K \to \overline{K}$ is a homomorphism, Theorem 4.6 shows that σ extends to a homomorphism $\tau : \overline{K} \to \overline{K}$.
(b) In $\overline{K}[t]$, we have $m_\alpha(K) = \prod_{i=1}^{d}(t - \gamma_i)^{r_i}$, where $\gamma_1, \ldots, \gamma_d$ are distinct, and $r_1, \ldots, r_d \in \mathbb{N}$. By part (b) there is a homomorphism $\tau : \overline{K} \to \overline{K}$ extending σ. Recall that τ is necessarily injective. Then $\sigma(m_\alpha(K)) = \tau(m_\alpha(K)) = \prod_{i=1}^{d}(t - \tau(\gamma_i))^{r_i}$. Since τ is injective, one has that $\tau(\gamma_1), \ldots, \tau(\gamma_d)$ are distinct, and the conclusion follows.

2. Suppose that $L : K$ is an algebraic extension of fields.
(a) Show that $\overline{L}$ is an algebraic closure of K, and hence $\overline{L} \simeq \overline{K}$.
(b) Suppose that $K \subseteq L \subseteq \overline{L}$. Show that one may take $\overline{K} = \overline{L}$.
Solution: (a) Consider $L : K$ as an extension relative to the embedding φ, and $\overline{L} : L$ as an extension relative to the embedding ψ. Then $\overline{L} : K$ is an extension of fields relative to the embedding $\psi \circ \varphi$, and since $\overline{L}$ is algebraically closed, then $\overline{L}$ is an algebraic closure of K. Thus Proposition 4.9 shows that, since $\overline{K}$ is also an algebraic closure of K, then $\overline{L} \simeq \overline{K}$.
(b) Suppose that there is a smaller algebraic closure $\overline{K}$ of K than $\overline{L}$. We may suppose that $\overline{K}$ is an algebraic extension of K with $K \subseteq \overline{K}$. We have that $\overline{L}$ is an algebraic closure of K and $K \subseteq \overline{L}$. Take $\varphi : K \to \overline{L}$ to be the inclusion mapping. Theorem 4.6 shows that φ can be extended to a homomorphism from $\overline{K}$ into $\overline{L}$. Thus $\overline{L} : \overline{K}$ is a field extension with $[\overline{L} : \overline{K}] > 1$ (since $\overline{K}$ is smaller than $\overline{L}$). But this contradicts the fact that $\overline{K}$ is algebraically closed. Thus we may take $\overline{K} = \overline{L}$, as claimed.

3. For each of the following polynomials, construct a splitting field L over $\mathbb{Q}$ and compute the degree $[L : \mathbb{Q}]$.
(a) $t^3 - 1$
(b) $t^7 - 1$
Solution: (a) One has $t^3 - 1 = (t-1)(t-\omega)(t-\omega^2)$, where $\omega = e^{2\pi i/3} = \frac{1}{2}(-1+\sqrt{-3})$. So $\mathbb{Q}(\omega) : \mathbb{Q}$ is a splitting field extension for $t^3 - 1$. We see that $(t^3-1)/(t-1) = t^2+t+1$ is monic, and it is easy to check that this polynomial has no linear factor and hence is irreducible. Hence $m_\omega(\mathbb{Q}) = t^2 + t + 1$, and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.
(b) One has $t^7 - 1 = (t-1)(t-\zeta)(t-\zeta^2)\cdots(t-\zeta^6)$, where $\zeta = e^{2\pi i/7}$. So $\mathbb{Q}(\zeta) : \mathbb{Q}$ is a splitting field extension for $t^7 - 1$. We see that $(t^7-1)/(t-1) = t^6 + \ldots + t + 1$ is monic, and we have seen that $(t^p - 1)/(t-1)$ is irreducible over $\mathbb{Q}$ when p is prime. Hence $m_\zeta(\mathbb{Q}) = t^6 + \ldots + t + 1$, and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$.

4. For each of the following polynomials, construct a splitting field L over $\mathbb{Q}$ and compute the degree $[L : \mathbb{Q}]$.
(a) $t^4 + t^2 - 6$
(b) $t^8 - 16$

Solution: (a) We have $t^4+t^2-6=(t^2-2)(t^2+3)=(t+\sqrt{2})(t-\sqrt{2})(t+\sqrt{-3})(t-\sqrt{-3})$. Then with $L=\mathbb{Q}(\sqrt{2},\sqrt{-3})$, we have that $L:\mathbb{Q}$ is a splitting field extension for t^4+t^2-6. The polynomial t^2-2 has $\sqrt{2}$ as a root, and t^2-2 is irreducible by Eisenstein's criterion using the prime 2. Thus $m_{\sqrt{2}}(\mathbb{Q})=t^2-2$ and $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=\deg m_{\sqrt{2}}(\mathbb{Q})=2$. Put $K=\mathbb{Q}(\sqrt{2})$, and note that $\sqrt{-3}$ is a root of the polynomial t^2+3. This polynomial is irreducible over $K[t]$, since $\sqrt{-3}$ is not real, and yet $K\subset\mathbb{R}$. Thus $m_{\sqrt{-3}}(K)=t^2+3$ and $[K(\sqrt{-3}):K]=\deg m_{\sqrt{-3}}(K)=2$. The tower law thus yields

$$[L:\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{-3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2\cdot 2=4.$$

(b) We have $t^8-16=t^8-2^4=(t-\alpha)(t-\zeta\alpha)\cdots(t-\zeta^7\alpha)$, where $\alpha=\sqrt[8]{16}=\sqrt{2}\in\mathbb{R}_+$ and $\zeta=e^{2\pi i/8}$. Thus, with $L=\mathbb{Q}(\alpha,\zeta\alpha,\zeta^2\alpha,\ldots,\zeta^7\alpha)$, we see that $L:\mathbb{Q}$ is a splitting field extension for t^8-16. Note that $\zeta=(\zeta\alpha)/\alpha\in L$, and hence $\mathbb{Q}(\alpha,\zeta)\subseteq L$. Also, for $k\in\mathbb{N}$, one has $\zeta^k\alpha\in\mathbb{Q}(\alpha,\zeta)$, and so $L\subseteq\mathbb{Q}(\alpha,\zeta)$. We therefore conclude that $L=\mathbb{Q}(\alpha,\zeta)$. Next, noting that $m_\alpha(\mathbb{Q})=t^2-2$, we see that $[\mathbb{Q}(\alpha):\mathbb{Q}]=2$. Also, we have $\zeta=(1+i)/\alpha$, so $\alpha\zeta-1$ is a root of the polynomial t^2+1, whence ζ is a root of the polynomial $\alpha^2t^2-2\alpha t+2=2t^2-2\alpha t+2$. But $\zeta\notin\mathbb{R}$, and so this polynomial is irreducible over $\mathbb{Q}(\alpha)$. Thus $m_\zeta(\mathbb{Q}(\alpha))=t^2-\alpha t+1$, and $[\mathbb{Q}(\alpha,\zeta):\mathbb{Q}]=2$. It therefore follows from the tower law that $[L:\mathbb{Q}]=[\mathbb{Q}(\alpha,\zeta):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]=4$.

5. Suppose that $L:K$ is a splitting field extension for the polynomial $f\in K[t]\setminus K$.
(a) Prove that $[L:K]\le(\deg f)!$.
(b) Prove that $[L:K]$ divides $(\deg f)!$.

Solution: (a) The conclusion in part (a) follows of course from that of part (b), but we nonetheless provide the slightly simpler argument available in this case. We use induction on $n=\deg(f)$. In the base case $n=1$, we have $[L:K]=1$, so the conclusion holds. Suppose now that $n>1$ and that the desired conclusion holds for all polynomials of degree smaller than n. Let $\alpha\in L$ be any root of f. Then f factors as $(t-\alpha)g$ for some polynomial $g\in K(\alpha)[t]$ of degree $n-1$. Moreover, we have that L is a splitting field for g over $K(\alpha)$. By induction, we therefore see that $[L:K(\alpha)]\le(n-1)!$. Since $[K(\alpha):K]=n$, the Tower Law shows that $[L:K]\le n\cdot(n-1)!=n$. This confirms the inductive step, and the desired conclusion follows.

(b) In the second case we again proceed by induction on $n=\deg(f)$, and again the case $n=1$ is immediate. Now, when $n>1$, we split the argument according to whether f is reducible or not over K. If f is irreducible, let $\alpha\in L$ be any root of f. Then f again factors as $(t-\alpha)g$ for some other polynomial $g\in K(\alpha)[t]$ of degree $n-1$. Moreover, we have that L is a splitting field for g over $K(\alpha)$. By induction, we therefore see that $[L:K(\alpha)]$ divides $(n-1)!$. Since $[K(\alpha):K]=n$, the Tower Law shows that $[L:K]$ divides $n\cdot(n-1)!=n!$.

On the other hand, if $f=gh$ is reducible, let M be the subfield of L generated by K and the roots of g. Then M is a splitting field for g over K and L is a splitting field for h over M. By induction, we have that $[M:K]$ divides $r!$ and $[L:M]$ divides $(n-r)!$, where $r=\deg(g)$. Hence $[L:K]=[L:M][M:K]$ divides $r!(n-r)!$, which in turn divides $n!$ (with quotient equal to the binomial coefficient $\binom{n}{r}$).

We confirm the inductive step in both cases, and the desired conclusion follows by induction.

GALOIS THEORY: SOLUTIONS TO HOMEWORK 8

1. Recall the splitting field L over $\mathbb{Q}$ that you constructed in question 4(b) of Problem Sheet 7 for the polynomial $t^8 - 16$. Determine the subgroup of S_4 to which $\mathrm{Gal}(L : \mathbb{Q})$ is isomorphic.
Solution: Recall that $L = \mathbb{Q}(\alpha, \zeta)$, where $\alpha = \sqrt{2}$ and $\zeta = (1 + i)/\alpha$. Thus in fact $L = \mathbb{Q}(\alpha, i)$. Take $\tau \in \mathrm{Gal}(L : \mathbb{Q})$. Then τ is determined by its action on $\alpha = \sqrt{2}$ and $i = \sqrt{-1}$. We begin by constructing $\mathbb{Q}$-homomorphisms $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha, i)$. We know that $\sigma(\alpha)$ must be a root of $m_\alpha(\mathbb{Q}) = t^2 - 2$, so $\sigma(\alpha) = \pm\alpha$. We can extend σ to $\tau : \mathbb{Q}(\alpha, i) \to \mathbb{Q}(\alpha, i)$ by taking $\tau|_{\mathbb{Q}(\alpha)} = \sigma$ and $\tau(i) = \pm i$, with the choice of sign independent of the previous choice. Here, since $m_i(\mathbb{Q}(\alpha)) = t^2 + 1$, we find that $\tau(i)$ must be one of the roots of $t^2 + 1$, explaining the previous assertion. We thus conclude that τ is one of the permutations τ_{lm} $(l, m \in \{0, 1\})$, where $\tau_{lm}(\alpha) = (-1)^l\alpha$ and $\tau_{lm}(i) = (-1)^m i$. Thus τ acts as one of the four permutations
$$(\alpha\ \ -\alpha)(i\ \ -i), \quad (\alpha\ \ -\alpha), \quad (i\ \ -i), \quad \mathrm{id}.$$
The group $\mathrm{Gal}(L : \mathbb{Q})$ is therefore isomorphic to the group of permutations
$$\{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}.$$

2. Suppose that K is a field and that $L : K$ is a splitting field extension for an irreducible polynomial $f \in K[t]$ of degree n. Assume that $K \subseteq L$.
   (a) Show that whenever α and β are roots of f in L, and σ is a K-automorphism of L, then $\sigma(\alpha) = \sigma(\beta)$ if and only if $\alpha = \beta$;
   Solution: Since σ is a K-automorphism of L, it is bijective and hence invertible. Then $\sigma(\alpha) = \sigma(\beta)$ if and only if $\sigma^{-1}(\sigma(\alpha)) = \sigma^{-1}(\sigma(\beta))$, which is to say, if and only if $\alpha = \beta$.
   (b) Show that the elements of $\mathrm{Gal}(L : K)$ act as permutations on the n roots of f, and hence deduce that $\mathrm{Gal}(L : K)$ has order dividing $n!$;
   Solution: Let $\alpha \in L$ be a root of f, and consider $\tau \in \mathrm{Gal}(L : K)$. Then $\tau(f(\alpha)) = f(\tau(\alpha))$. Thus, under the action of any element τ of $\mathrm{Gal}(L : K)$, a root α of f is taken to another root β of f. Since this mapping is bijective, it follows that σ acts as a permutation on the set of roots of f. A permutation group on a set of n objects is a subset of S_n (the permutation group on n letters), and hence by Lagrange's theorem has order dividing $n!$.
   (c) Let g be a degree m polynomial in $K[t]$, not necessarily irreducible, and let $M : K$ be a splitting field extension for g. Show that $|\mathrm{Gal}(M : K)|$ divides $m!$.
   Solution: Let $\alpha \in M$ be a root of g, and consider $\tau \in \mathrm{Gal}(M : K)$. Then again $\tau(g(\alpha)) = g(\tau(\alpha))$. Thus, just as in the discussion for part (b), the mapping τ acts as a permutation on the distinct roots of g. If the number of distinct roots of g is n, then it follows that $|\mathrm{Gal}(M : K)|$ divides $n!$. But $n \le m$, so $n!$ divides $m!$, whence $|\mathrm{Gal}(M : K)|$ divides $m!$.

3. Suppose that $L : K$ is a normal extension, and that $K \subseteq L \subseteq \overline{K}$. Recall that since $L : K$ is algebraic, then any algebraic closure of K is an algebraic closure of L.
   (a) Show that for any K-homomorphism $\tau : L \to \overline{K}$, one has $\tau(L) = L$;

Solution: Let $\tau : L \to \overline{K}$ be a K-homomorphism. Let $\alpha \in L$. Then since $L : K$ is algebraic, one sees that α is algebraic over K, and so $m_\alpha(K)$ exists. Write $g = m_\alpha(K)$. Then on noting that g is a K-homomorphism, we deduce that $0 = \tau(g(\alpha)) = g(\tau(\alpha))$. But $L : K$ is normal, so $\tau(\alpha) \in L$. Since this holds for all $\alpha \in L$, we infer that $\tau(L) \subseteq L$. Finally, since $L : K$ is algebraic, it follows from Theorem 3.4 that $\tau(L) = L$.

(b) Suppose that M is a field satisfying $K \subseteq M \subseteq L$. Show that $L : M$ is a normal extension.

Solution: Assume $K \subseteq M \subseteq L$, and let $f \in M[t] \setminus M$ be irreducible. Suppose that $\alpha \in L$ is a root of f. Then $f = \lambda m_\alpha(M)$ for some $\lambda \in M^\times$. But $m_\alpha(M)$ divides $m_\alpha(K)$, and since $L : K$ is normal, one has that $m_\alpha(K)$ splits over L. Hence $m_\alpha(M)$ also splits over L, and thus f splits over L. Then $L : M$ is a normal extension.

4. Which of the following field extensions are normal? Justify your answers.

(a) $\mathbb{Q}(\sqrt{3}) : \mathbb{Q}$

(b) $\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}$

(c) $\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}$

(d) $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}$

(e) $\mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}$.

Solution: (a) Normal: this is a splitting field extension for $t^2 - 3$ over $\mathbb{Q}$, since $t^2 - 3 = (t - \sqrt{3})(t + \sqrt{3})$ splits over $\mathbb{Q}(\sqrt{3})$, and splitting field extensions are normal extensions.

(b) Not normal: the polynomial $t^3 - 3$ has one root $\sqrt[3]{3}$ lying in $\mathbb{Q}(\sqrt[3]{3})$, yet does not split over the latter field. For writing $\omega = e^{2\pi i/3}$, the remaining roots $\sqrt[3]{3}\omega$ and $\sqrt[3]{3}\omega^2$ over $\overline{\mathbb{Q}}$ are not real, and cannot lie in $\mathbb{Q}(\sqrt[3]{3})$.

(c) Normal: this is a splitting field extension for $t^2 + 1$ over $\mathbb{Q}$, since the polynomial $t^2 + 1 = (t - \sqrt{-1})(t + \sqrt{-1})$ splits over $\mathbb{Q}(\sqrt{-1})$, and splitting field extensions are normal extensions.

(d) Not normal: the polynomial $t^3 - 3$ has one root $\sqrt[3]{3}$ lying in $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$, yet does not split over the latter field, for the remaining roots $\sqrt[3]{3}\omega$ and $\sqrt[3]{3}\omega^2$ over $\overline{\mathbb{Q}}$ are not real, and cannot lie in $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$.

(e) Normal: this is a splitting field extension for $(t^2 + 1)(t^3 - 3)$ over $\mathbb{Q}$, since

$$(t^2 + 1)(t^3 - 3) = (t - \sqrt{-1})(t + \sqrt{-1})(t - \sqrt[3]{3})(t - \omega\sqrt[3]{3})(t - \omega^2\sqrt[3]{3}),$$

with $\omega = \frac{1}{2}(-1 + \sqrt{-1}\sqrt{3}) \in \mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt[3]{3})$. Here, we confirm that this satisfies the minimality condition on noting that $\sqrt{3} = (1 + 2\omega\sqrt[3]{3}/\sqrt[3]{3})/\sqrt{-1} \in \mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt[3]{3})$. Moreover, splitting field extensions are normal extensions.

5. Let $K = \mathbb{F}_5(t)$. Find an algebraic field extension $L : K$ which is not normal, and justify your answer.

Solution: Let $\overline{K}$ denote an algebraic closure of K with $K \subset \overline{K}$, and consider the element $t^{1/3} \in \overline{K}$ that is a root of the polynomial $X^3 - t \in K[X]$. We claim that the algebraic extension $L : K$, where $L = K(t^{1/3})$, is not a normal extension. If $\alpha \in \overline{K}$ satisfies the equation $\alpha^3 - t = 0$, then we have $(\alpha/t^{1/3})^3 = 1$, so that $\alpha = \beta t^{1/3}$ with $\beta^3 = 1$. Thus, we find that β satisfies the equation $(\beta - 1)(\beta^2 + \beta + 1) = 0$. Then either $\beta = 1$, or else $(2\beta + 1)^2 = -3$. There is no element $\gamma \in \mathbb{F}_5$ with $\gamma^2 = -3$, since $1^2 \equiv 4^2 \equiv 1 \pmod 5$ and $2^2 \equiv 3^2 \equiv -1 \pmod 5$. Observe that $K(t^{1/3}) = \mathbb{F}_5(t^{1/3})$. Then if $\gamma \in \mathbb{F}_5(t^{1/3}) \setminus \mathbb{F}_5$ satisfies $\gamma^2 = -3$, then there is a non-constant polynomial $h \in \mathbb{F}_5[X]$ having the property that $h(t^{1/3}) = 0$. The existence of such a polynomial would show that $t^{1/3}$, and hence also t, are algebraic over $\mathbb{F}_5$, contradicting the (implicit) assumption that t is transcendental over $\mathbb{F}_5$. Then no element $\gamma \in K(t^{1/3})$ satisfies the equation $\gamma^2 = -3$, and thus the only solution $\beta \in K(t^{1/3})$ of $\beta^3 = 1$ is $\beta = 1$. The only linear factor of $X^3 - t$ over $L[X]$ is therefore $X - t^{1/3}$. Finally, since $X^3 - t \neq (X - t^{1/3})^3$, we conclude that $X^3 - t$ does not split over $K(t^{1/3})$, whence $L : K$ is not a splitting field extension, and consequently is not normal.

GALOIS THEORY: SOLUTIONS TO HOMEWORK 9

1. Suppose that $E : K$ and $F : K$ are finite extensions having the property that K, E and F are contained in a field L.
   (a) Show that $EF : K$ is a finite extension;
   Solution: Since $E : K$ and $F : K$ are both finite extensions, then for some natural number n there exist elements $\alpha_1, \ldots, \alpha_n \in E$, all algebraic over K, such that $E = K(\alpha_1, \ldots, \alpha_n)$. Thus $EF = F(\alpha_1, \ldots \alpha_n)$, and it follows from the tower law that $[EF : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F] < \infty$. But then, again by the tower law, one has $[EF : K] = [EF : F][F : K] < \infty$, and so $EF : F$ is a finite extension.
   (b) Show that when $E : K$ and $F : K$ are both normal, then $E \cap F : K$ is a normal extension;
   Solution: For any $\alpha \in E \cap F$, one sees that since E is algebraic over K, then α is algebraic over K. Hence $E \cap F : K$ is algebraic. Suppose next that $f \in K[t] \setminus K$ has the property that f is irreducible over K, and $f(\alpha) = 0$ for some $\alpha \in E \cap F$. Thus f splits over E and over F, and so f splits over $E \cap F$. Hence $E \cap F : K$ is a normal extension.
   (c) Show that when $E : K$ and $F : K$ are both normal, then $EF : E \cap F$ is a normal extension.
   Solution: Theorem 6.7 shows that $EF : K$ is normal. Since $EF : E \cap F : K$ is a tower of field extensions with $EF : K$ normal, it follows from Proposition 6.3 that $EF : E \cap F$ is also normal.
2. Suppose that $L : M$ is an algebraic extension with $M \subseteq L$. Show that when $\alpha \in L$ and $\sigma : M \to \overline{M}$ is a homomorphism, then $\sigma(m_\alpha(M))$ is separable over $\sigma(M)$ if and only if $m_\alpha(M)$ is separable over M.
   Solution: Suppose that $\alpha \in L$ and $\sigma : M \to \overline{M}$ is a homomorphism. This homomorphism may be extended to a homomorphism $\sigma : \overline{M} \to \overline{M}$. Since $L : M$ is algebraic, we know that $m_\alpha(M)$ exists. Over $\overline{M}$, we have
   $$m_\alpha(M) = (t - \alpha_1)^{r_1} \cdots (t - \alpha_d)^{r_d},$$
   where $\alpha_1, \ldots, \alpha_d$ are distinct and $r_1, \ldots, r_d \in \mathbb{N}$. Then
   $$\sigma(m_\alpha(M)) = (t - \sigma(\alpha_1))^{r_1} \cdots (t - \sigma(\alpha_d))^{r_d},$$
   and since σ is necessarily injective, we know that $\sigma(\alpha_1), \ldots, \sigma(\alpha_d)$ are distinct. Thus $m_\alpha(M)$ has multiple roots if and only if $\sigma(m_\alpha(M))$ has multiple roots. We know that $\sigma(m_\alpha(M))$ is irreducible over $\sigma(M)$ since $m_\alpha(M)$ is irreducible over M. Hence $m_\alpha(M)$ is separable over M if and only if $\sigma(m_\alpha(M))$ is separable over $\sigma(M)$.
3. (a) Suppose that $f \in K[t]$ is separable over K and that $L : K$ is a splitting field extension for f. Show that $L : K$ is separable.
   Solution: Assume that $K \subseteq L$. Since $L : K$ is a splitting field extension for f, we have that $L = K(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n \in L$ are the roots of f. For each i with $1 \leq i \leq n$, we have that $m_{\alpha_i}(K)$ divides f, and since f is separable over K and $m_{\alpha_i}(K)$ is irreducible over K, we know by definition that $m_{\alpha_i}(K)$ is separable over K. Thus α_i is separable over K for each i, and hence by Theorem 7.4, the field extension $L : K$ is separable.

(b) Suppose that $L : K$ is a splitting field extension for $S \subseteq K[t]$ where each $f \in S$ is separable over K. Show that $L : K$ is a separable extension.
Solution: Let $\alpha \in L$. Then by Proposition 1.9, we have that $\alpha \in D$, where D is some finite subset of $A = \{\beta \in L : g(\beta) = 0 \text{ for some } g \in S\}$. For each $\beta \in D$, choose $g_\beta \in S$ in such a manner that β is a root of g_β. Put $h = \prod_{\beta \in D} g_\beta$, and let $M : K$ be a splitting field extension for h. We may assume here that $K \subseteq M \subseteq L$. Since g_β is separable over K for each $\beta \in D$, we deduce that h is separable over K. Thus, by part (a), we conclude that $M : K$ is separable. But $\alpha \in K(D) \subseteq M$, and so α is separable over K. Finally, since this argument holds for all $\alpha \in L$, we find that $L : K$ is separable.

4. Let p be a prime number, let $\mathbb{F}_p$ denote the finite field of p elements, and let $K = \mathbb{F}_p(t)$. Suppose that $L : K$ is a field extension, and $s \in L$ is transcendental over K.

(a) Write $J = K(s)$, and let E denote a splitting field for the polynomial $x^p - t \in J[x]$. Show that for some $\xi \in E$, one has $x^p - t = (x - \xi)^p$, and deduce that $[E : J] = p$.
Solution: Let E denote a splitting field for $x^p - t$ over J. Write $h(x) = x^p - t$. Since E is a splitting field for h, there exists some $\xi \in E$ with $h(\xi) = 0$. In particular, one has $\xi^p = t$. But since the binomial coefficients $\binom{p}{r}$ are divisible by p, and hence zero in $\mathbb{F}_p$ for $1 \le r < p$, we have $(x - \xi)^p = x^p - \xi^p = x^p - t$, as desired.
We next show that h is irreducible over J. If $(x - \xi)^p = x^p - t = fg$, with $f, g \in J[x]$ monic polynomials of degree at least one, then since $E[x]$ is a UFD, one finds that $f = (x - \xi)^u$ and $g = (x - \xi)^{p-u}$ for some integer u with $1 \le u \le p - 1$. Since p and u are coprime, so too are $p - u$ and u, and hence there exist $a, b \in \mathbb{Z}$ with $au + b(p - u) = 1$. Thus $x - \xi = f^a g^b \in J[x]$, whence $\xi \in J$. But then there exist $c, d \in \mathbb{F}_q[s, t] \setminus \{0\}$ with $\xi = c/d$. Hence $t = \xi^p = c^p/d^p$, so that $c^p = td^p$. The degree of the polynomial on the left hand side of the last relation is divisible by p, while on the right hand side the degree is congruent to 1 modulo p, a contradiction. Thus, the hypothesised factorisation does not exist, and so h is irreducible over J. Finally, since h is irreducible over $J[x]$, one has $h = m_\xi(J)$. Since $E = J(\xi)$, we deduce that $[E : J] = \deg(m_\xi(J)) = p$, as desired.

(b) Let $U : J$ be a splitting field extension for the polynomial $(x^p - t)(x^p - s)$. By considering a splitting field extension F for the polynomial $x^p - s \in E[x]$, show that $[U : J] = p^2$.
Solution: We have $E = J(\xi) \subseteq \mathbb{F}_p(\xi, s)$. The same argument as in part (a), in all essentials, shows that $[F : E] = p$. For some $\eta \in U$ we have $x^p - s = (x - \eta)^p$. Were $x^p - s$ to fail to be irreducible over $E[x]$, then for some integer v with $1 \le v \le p - 1$, we would have $\eta^v = s$. But then we deduce as before that $\eta \in E$. Then the relation $\eta^p = s$ implies the existence of polynomials $c', d' \in \mathbb{F}_p(\xi)[s]$ with $(c')^p = s(d')^p$, leading to a contradiction (on considering the degrees of left and right hand sides as polynomials in s). Then $x^p - s$ is irreducible over $E[x]$. Since $F = E(\eta)$, we obtain $[F : E] = \deg(m_\eta(E)) = p$, as required. Finally, by the Tower Law, we have $[F : J] = [F : E][E : J] = p^2$. But $E \subsetneq U \subseteq F$. Then by the Tower Law we see that $[U : J]$ is a divisor of p^2 exceeding p, which is to say that $[U : J] = p^2$.

5. With the same notation as in the previous question:

(a) Show that if $\gamma \in U$, then $\gamma^p \in J$.
Solution: The field U contains elements ξ and η with $\xi^p = t$ and $\eta^p = s$, and one has $(x^p - t)(x^p - s) = (x - \xi)^p (x - \eta)^p$, so that $U = J(\xi, \eta)$. Then if $\gamma \in U$, we may find non-zero polynomials $q, r \in J[x_1, x_2]$ for which $\gamma = q(\xi, \eta)/r(\xi, \eta)$.

But then by our earlier observation concerning pth powers, one finds that $\gamma^p = q(\xi^p, \eta^p)/r(\xi^p, \eta^p) = q(t, s)/r(t, s) \in J$.

(b) What is the degree of the field extension $J(\gamma) : J$? Explain.
Solution: Let $\delta = \gamma^p \in J$. Then the minimal polynomial of γ over J divides $t^p - \delta$, hence has degree at most p. In particular, one has $1 \leq [J(\gamma) : J] \leq p$. On the other hand, since $J \subseteq J(\gamma) \subseteq U$, it follows from the Tower Law that $[J(\gamma) : J]$ divides $[U : J] = p^2$. Thus we conclude that $[J(\gamma) : J] = 1$ or p.

(c) Deduce that $U : J$ is a finite field extension which is not simple.
Solution: Suppose that $U : J$ is a simple extension, so that for some element $\gamma \in U$, one has $U = J(\gamma)$. Then from part (b) we have $[U : J] = [J(\gamma) : J] = 1$ or p, yet from 4(b) we must have $[U : J] = p^2$. This yields a contradiction, and so the finite field extension $U : J$ is not simple.

GALOIS THEORY: SOLUTIONS TO HOMEWORK 10

1. Let $f \in K[t] \setminus K$, and let $L : K$ be a splitting field extension for f. Assume that $K \subseteq L$.
   (a) Show that when f has a repeated root over L, then there exists $\alpha \in L$ for which $f(\alpha) = 0 = (Df)(\alpha)$.
   Solution: The situation with f is reducible simplifies to the case that f is irreducible, so we may suppose that f is irreducible with a repeated root $\alpha \in L$. Then $f = (t-\alpha)^k g$ for some $k > 1$ and $g \in L[t]$. Hence $Df = k(t-\alpha)^{k-1}g + (t-\alpha)^k Dg$, whence $(Df)(\alpha) = 0$ and $f(\alpha) = 0$.
   (b) Show that when $\alpha \in L$ satisfies $f(\alpha) = 0 = (Df)(\alpha)$, then there exists $g \in K[t]$ having the property that $\deg g \geq 1$ and g divides both f and Df.
   Solution: Suppose that there exists $\alpha \in L$ such that $f(\alpha) = (Df)(\alpha) = 0$. Then $m_\alpha(K)|f$ and $m_\alpha(K)|Df$, and so the conclusion holds with $g = m_\alpha(K)$.
   (c) Show that when $g \in K[t] \setminus K$ divides both f and Df, then f has a repeated root over L.
   Solution: Suppose that there exists $g \in K[t]$ such that $\deg g \geq 1$, having the property that $g|f$ and $g|Df$. One therefore has $f = gh$ for some $h \in K[t]$. Since f splits over L, then so does g. Let α be a root of g in L. Then $f = (t-\alpha)q$, for some $q \in L[t]$, and hence $Df = q + (t-\alpha)Dq$. But $(t-\alpha)|Df$ in $L[t]$, since $g|Df$, and so $(t-\alpha)|q$. Thus $(t-\alpha)^2|f$, and so f has a repeated root in L.
2. Suppose that $\mathrm{char}(K) = p > 0$ and f is irreducible over $K[t]$.
   (a) Show that there is an irreducible and separable polynomial $g \in K[t]$ and a non-negative integer n with the property that $f(t) = g(t^{p^n})$.
   Solution: Let n be the largest non-negative integer having the property that $f(t) \in K[t^{p^n}]$. Thus, there exists a polynomial $g \in K[t]$ having the property that $f(t) = g(t^{p^n})$. It follows from Theorem 8.2 that if g is inseparable, then $g \in K[t^p]$, which implies that $f \in K[t^{p^{n+1}}]$, contradicting the maximality of n. It follows that g is separable, and its irreducibility is an immediate consequence of that of f.
   (b) Let $L : K$ be a splitting field extension for f. Show that there exists a non-negative integer n with the property that every root of f in L has multiplicity p^n.
   Solution: From part (a) we see that $f(t) = g(t^{p^n})$ for some non-negative integer n and an irreducible separable polynomial $g \in K[t]$. Since g is separable, there exist distinct roots $\beta_1, \ldots, \beta_d \in \overline{K}$ having the property that $g(t) = (t-\beta_1)\cdots(t-\beta_d)$. Hence $f(t) = (t^{p^n} - \beta_1)\cdots(t^{p^n} - \beta_d)$. Writing $\alpha_i = \beta_i^{1/p^n} \in \overline{K}$ for $1 \leq i \leq d$, we see that the α_i are distinct elements of $\overline{K}$, and moreover a splitting field extension for f is $L : K$, where $L = K(\alpha_1, \ldots, \alpha_d)$, since we have
   $$f(t) = (t-\alpha_1)^{p^n} \cdots (t-\alpha_d)^{p^n}.$$
   Thus every root of f in L has multiplicity p^n for some non-negative integer n.

GALOIS THEORY: SOLUTIONS TO HOMEWORK 11

1. Suppose that $L : M : K$ is an algebraic tower of fields. Prove that $L : K$ is separable if and only if $L : M$ and $M : K$ are both separable. [Hint: try using the Primitive Element Theorem].
   Solution: We showed in Proposition 7.1 that when $L : K$ is separable, then so too is $L : M$. Meanwhile, the separability, in such circumstances, of $M : K$ is inherited from that of $L : K$. Conversely, suppose that $L : M$ and $M : K$ are both separable, and suppose that $\alpha \in L$. Then since $L : M$ is separable, one finds that α is separable over M. The polynomial $m_\alpha(M)$ has its coefficients defined in a subfield M' of M with $M' : K$ a finite separable extension. Since $m_\alpha(M') = m_\alpha(M)$ is separable, we deduce that α is separable over M'. Thus, since $M' : K$ is finite and separable, it follows from the primitive element theorem that there exists $\beta \in M'$ such that $M' = K(\beta)$, whence Theorem 7.4 implies that $M'(\alpha) : K$, or equivalently $K(\alpha, \beta) : K$, is separable. Consequently, we deduce that $\alpha \in K(\alpha, \beta)$ is separable over K. Since this conclusion holds for all $\alpha \in L$, we conclude that $L : K$ is separable.
2. Suppose that $E : K$ and $F : K$ are finite extensions with $K \subseteq E \subseteq L$ and $K \subseteq F \subseteq L$, with L a field.
   (a) Show that when $E : K$ is separable, then so too is $EF : F$.
   Solution: By the primitive element theorem, we may suppose that $E = K(\alpha)$ for some $\alpha \in E$ separable over K. Thus $EF = F(\alpha)$. Since α is separable over K, it is also separable over F, and hence it follows from Theorem 7.4 that $F(\alpha) : F$, or equivalently $EF : F$, is separable.
   (b) Show that when $E : K$ and $F : K$ are both separable, then so too are $EF : K$ and $E \cap F : K$.
   Solution: When $E : K$ and $F : K$ are both separable, then $EF : F$ is separable, and hence $EF : F : K$ is a tower of extensions with $EF : F$ and $F : K$ both separable. Then it follows from problem 1 that $EF : K$ is separable. Likewise, one has the tower $E : E \cap F : K$ of extensions with $E : K$ separable. Then it follows from problem 1 that $E \cap F : K$ is separable.
3. Suppose that $\mathrm{char}(K) = p > 0$ and that $L : K$ is a totally inseparable algebraic extension (thus, every element of $L \setminus K$ is inseparable). Show that whenever $\alpha \in L$, then there is a non-negative integer n and an element $\theta \in K$ having the property that $m_\alpha(K) = t^{p^n} - \theta$.
   Solution: Suppose that $\alpha \in L$. Then $m_\alpha(K)$ is an irreducible polynomial over K, so by question 4(a) has the shape $g(t^{p^n})$ for some non-negative integer n and an irreducible separable polynomial g. Suppose that g has degree 2 or more, and that its distinct roots in $\overline{K}$ are $\beta_1, \dots, \beta_d$. Then for some index i one has $\beta_i = \alpha^{p^n}$ and $m_{\beta_i}(K) = g(t)$, by the irreducibility of

g. But then $\beta_i \in L$ is separable, because g is separable, contradicting the totally inseparable property of the extension $L : K$. It follows that g must have degree 1, and hence $m_\alpha(K) = t^{p^n} - \theta$, where $\theta = \alpha^{p^n} \in K$.

GALOIS THEORY: SOLUTIONS TO HOMEWORK 12

1. Let $L : K$ be a finite Galois extension with Galois group G. For any $\alpha \in L$, define the polynomial $f_\alpha(t) = \prod_{\sigma \in G}(t - \sigma(\alpha))$.

   (a) Show that $f_\alpha \in K[t]$.

   Solution: Since $L : K$ is Galois, the fixed field of G is K. Then $\beta \in K$ if and only if $\tau(\beta) = \beta$ for every $\tau \in G$. Thus, whenever $\tau \in G$, one has

   $$\tau(f_\alpha(t)) = \prod_{\sigma \in G}(t - \tau(\sigma(\alpha))) = \prod_{\rho \in G}(t - \rho(\alpha)) = f_\alpha(t).$$

   Then $f_\alpha(t)$ has each of its coefficients in the fixed field of G, so $f_\alpha \in K[t]$.

   (b) Prove that if $\sigma(\alpha) \neq \tau(\alpha)$ whenever $\sigma, \tau \in G$ satisfy $\sigma \neq \tau$, then $f_\alpha = m_\alpha(K)$.

   Solution: Since the identity element belongs to G, one has $f_\alpha(\alpha) = 0$, whence the minimal polynomial $m_\alpha(K)$ of α over K must divide f_α. But over $L[t]$ one has that $t - \alpha$ divides $m_\alpha(K)$. Then since $m_\alpha(K)$ is fixed by the action of G (its coefficients lie in K), we find that $t - \sigma(\alpha)$ divides $\sigma(m_\alpha(K)) = m_\alpha(K)$ for each $\sigma \in G$. By hypothesis, moreover, the elements $\sigma(\alpha)$ are distinct for $\sigma \in G$, and thus $\prod_{\sigma \in G}(t - \sigma(\alpha)) = f_\alpha(t)$ divides $m_\alpha(K)$. Thus we find that $m_\alpha(K)$ and f_α divide each other, and this implies that f_α is the minimal polynomial of α.

2. Use question 1 to calculate the minimal polynomial of $2\sqrt{-3} - \sqrt{2}$ over $\mathbb{Q}$.

   Solution: The field extension $\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q}$ is a splitting field extension for the polynomial $(t^2 - 2)(t^2 + 3)$, and hence is finite and Galois. One checks easily (via the Tower Law) that $[\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q}] = 4$, and thus the conjugates of $2\sqrt{-3} - \sqrt{2}$ under the action of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q})$ are $\pm(2\sqrt{-3} - \sqrt{2})$ and $\pm(2\sqrt{-3} + \sqrt{2})$. Then applying the conclusion of part (ii), we find that the minimal polynomial of $2\sqrt{-3} - \sqrt{2}$ is

   $$(t^2 - (2\sqrt{-3} - \sqrt{2})^2)(t^2 - (2\sqrt{-3} + \sqrt{2})^2) = t^4 + 20t^2 + 196.$$

3. Let f denote the polynomial $t^3 + t + 1$.

   (a) Write down a splitting field extension for f over $\mathbb{F}_2$.

   Solution: If α is a root of $t^3 + t + 1$ lying in a splitting field extension L for this polynomial over $\mathbb{F}_2$, then

$$f(t) = t^3 + t + 1 = (t + \alpha)(t^2 + \alpha t + \alpha^2 + 1) = (t + \alpha)(t + \alpha^2)(t + \alpha^2 + \alpha).$$

   Then $\mathbb{F}_2(\alpha) : \mathbb{F}_2$ is a splitting field extension for $t^3 + t + 1$ over $\mathbb{F}_2$.

   (b) What is $\mathrm{Gal}_{\mathbb{F}_2}(f)$? Justify your answer, and determine all subfields of the splitting field that you wrote down in part (a).

   Solution: Observe that f is irreducible over $\mathbb{F}_2$, since otherwise, as a polynomial of degree 3, it would have a linear factor over $\mathbb{F}_2$, and hence have 0 or 1 as a root, which is not the case. It follows that $m_\alpha(\mathbb{F}_2) = f$.

Hence, since f is a separable polynomial, we find that $\mathbb{F}_2(\alpha) : \mathbb{F}_2$ is a Galois extension, with Galois group of order $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 3$. Then $\mathrm{Gal}(\mathbb{F}_2)$ must be cyclic.

In this case it is not too difficult to write down the automorphisms. If $\phi(x) = x^2$ for $x \in \mathbb{F}_2(\alpha)$, we have seen that this Frobenius monomorphism is an automorphism, with $\phi(\alpha) = \alpha^2$. We get another automorphism by squaring ϕ, so that $\phi^2(x) = \phi(\phi(x)) = \phi(x^2) = x^4$, and in particular $\phi^2(\alpha) = \alpha^4 = \alpha^2 + \alpha$. Thus, the identity, ϕ and ϕ^2 are the three automorphisms. One can also check directly that ϕ has order 3, thus $\phi^3(\alpha) = \alpha^8 = \alpha$.

Since the cyclic group $\langle \phi \rangle$ of order 3 has no proper subgroups, it follows from the Fundamental Theorem of Galois Theory that $\mathbb{F}_2(\alpha)$ has no proper subfields, and hence the only subfields are the trivial ones $\mathbb{F}_2$ and $\mathbb{F}_2(\alpha)$.

4. Let f denote the polynomial $t^4 + t^3 + t^2 + t + 1$.

 (a) Write down a splitting field extension for f over $\mathbb{Q}$.

 Solution: If α is a root of f, then $\alpha^5 = 1$. Thus, we see that on putting $\zeta = e^{2\pi i/5}$, we have $f(t) = (t-\zeta)(t-\zeta^2)(t-\zeta^3)(t-\zeta^4)$. Then $\mathbb{Q}(\zeta) : \mathbb{Q}$ is a splitting field extension for f over $\mathbb{Q}$.

 (b) Show that $\mathrm{Gal}_{\mathbb{Q}}(f) \cong C_4$, where C_4 is the cyclic group of order 4.

 Solution: Observe that f is irreducible over $\mathbb{Q}$, since 5 is prime and the polynomial $t^{p-1} + \ldots + t + 1$ is irreducible for primes p. Then $m_\zeta(\mathbb{Q}) = f$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(f) = 4$. Moreover, the extension $\mathbb{Q}(\zeta) : \mathbb{Q}$ is separable and normal, and hence Galois, so that $\mathrm{Gal}(f)$ has order $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$. The Galois group acts transitively on the roots of f, and so there is an automorphism $\sigma \in \mathrm{Gal}(f)$ having the property that $\sigma(\zeta) = \zeta^2$. One then sees that

$$\begin{aligned}
\sigma^2(\zeta) &= \sigma(\zeta^2) = \zeta^4 = -(1 + \zeta + \zeta^2 + \zeta^3),\\
\sigma^3(\zeta) &= \sigma(\zeta^4) = \zeta^8 = \zeta^3,\\
\sigma^4(\zeta) &= \sigma(\zeta^3) = \zeta^6 = \zeta.
\end{aligned}$$

 Thus σ is an automorphism of order 4, and one must have $\mathrm{Gal}(f) = \langle \sigma \rangle \cong C_4$.

5. Use the Galois correspondence to determine all subfields of the splitting field that you wrote down in part (a) of question 4. Draw the lattice of subfields and corresponding lattice of subgroups of C_4.

 Solution: The cyclic group of order 4 given by $G = \langle \sigma^i \,|\, \sigma^4 = 1 \rangle$ has the trivial subgroups $\{1\}$ and G, and the additional subgroup $H = \{1, \sigma^2\}$ of order 2, and no other subgroups. Then by the Fundamental Theorem of Galois Theory, the field $\mathbb{Q}(\zeta)$ has only one non-trivial subfield, and this is $\mathrm{Fix}_{\mathbb{Q}(\zeta)}(H)$. In this case, we can apply brute force easily enough to determine the fixed field. Given arbitrary rational numbers a, b, c, d, one sees that $a + b\zeta + c\zeta^2 + d\zeta^3 = \sigma^2(a + b\zeta + c\zeta^2 + d\zeta^3)$ if and only if

$$a + b\zeta + c\zeta^2 + d\zeta^3 = a - b(1 + \zeta + \zeta^2 + \zeta^3) + c\zeta^3 + d\zeta^2.$$

Thus we must have $a-b=a$, $b=-b$, $c=-b+d$, $d=-b+c$, whence $b=0$ and $c=d$. We therefore conclude that the fixed field of the group generated by σ^2 is $\mathbb{Q}(\zeta^2+\zeta^3)$. The lattices of subfields and corresponding subgroups:

$$\begin{tikzcd}
G=\langle\sigma\rangle \arrow[d, dash] & \mathbb{Q} \arrow[d, dash] \\
\langle\sigma^2\rangle \arrow[d, dash] & \mathbb{Q}(\zeta^2+\zeta^3) \arrow[d, dash] \\
\langle 1\rangle & \mathbb{Q}(\zeta)
\end{tikzcd}$$

GALOIS THEORY: SOLUTIONS TO HOMEWORK 13

1. Let f denote the polynomial $t^3 - 7$.

   (a) Write down a splitting field extension for f over $\mathbb{Q}$.
   Solution: Let $\zeta = e^{2\pi i/3} = \frac{1}{2}(-1+\sqrt{-3}) \in \mathbb{Q}$ be a primitive cube root of unity, and put $\alpha = \sqrt[3]{7} \in \mathbb{Q}$. Then f splits as $(t-\alpha)(t-\zeta\alpha)(t-\zeta^2\alpha)$ over $\mathbb{Q}$, and a splitting field for f is $L = \mathbb{Q}(\alpha, \zeta) = \mathbb{Q}(\sqrt[3]{7}, \sqrt{-3})$.

   (b) Show that $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_3$.
   Solution: Note that f is irreducible by Eisenstein's criterion using the prime 7 and Gauss' lemma. The Galois group is thus isomorphic to a transitive subgroup of S_3, and hence either S_3 or A_3. Since $\sqrt{-3} \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$, the Tower Law yields

   $$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

   Therefore, the Galois group of f has order 6, and hence is isomorphic to S_3.

2. Use the Galois correspondence to determine all subfields of the splitting field that you wrote down in part (a) of question 1. Draw the lattice of subfields and corresponding lattice of subgroups of S_3.
   Solution: Write $\beta_1 = \alpha$, $\beta_2 = \zeta\alpha$, $\beta_3 = \zeta^2\alpha$, and consider the Galois group G of $t^3 - 7$, namely $\mathrm{Gal}(L : \mathbb{Q}) \cong S_3$. Since all possible permutations of roots must occur as automorphisms in G, we have in particular the automorphism σ that cyclically permutes the β_i, so that

   $$\alpha \mapsto \zeta\alpha \quad \text{and} \quad \zeta \mapsto \zeta,$$

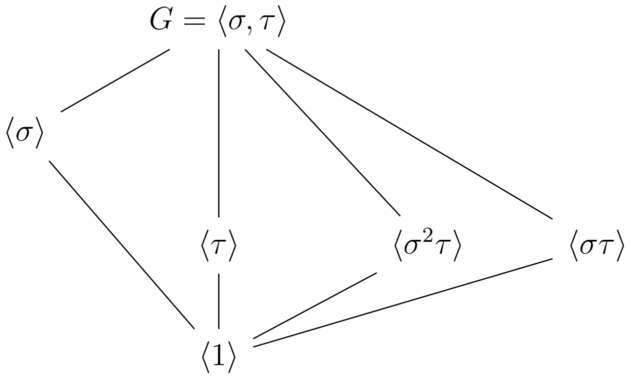
   and also the permutation τ that interchanges two of the roots, leaving the third fixed, so that

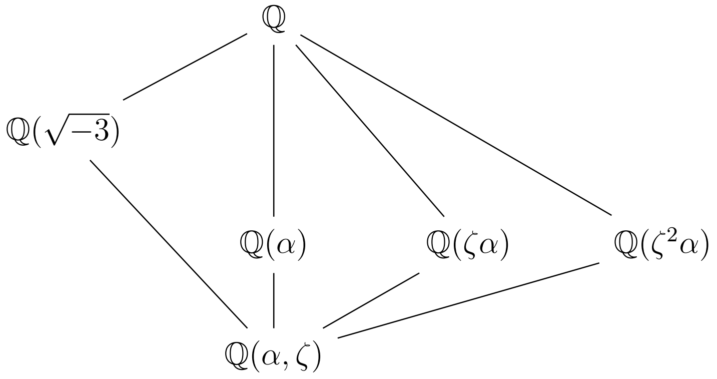
   $$\alpha \mapsto \alpha \quad \text{and} \quad \zeta \mapsto \zeta^2.$$

   Notice that one has

   $$G \cong \langle \sigma, \tau | \sigma^3 = \tau^2 = 1, \tau\sigma = \sigma^2\tau \rangle.$$

   The fields L, and $\mathbb{Q}$, are the fixed fields of $\{\mathrm{id}\}$, and G, respectively. As for the intermediate fields, we have the three cubic extensions $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\zeta\alpha)$ and $\mathbb{Q}(\zeta^2\alpha)$, corresponding to the subgroups $\langle\tau\rangle$, $\langle\sigma^2\tau\rangle$ and $\langle\sigma\tau\rangle$, respectively, of index 3 in G. Finally, the subgroup $\langle\sigma\rangle$ of index 2 in G fixes the quadratic extension $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$.


$G = \langle \sigma, \tau \rangle$
$\langle \sigma \rangle$
$\langle \tau \rangle$
$\langle \sigma^2 \tau \rangle$
$\langle \sigma \tau \rangle$
$\langle 1 \rangle$


$\mathbb{Q}$
$\mathbb{Q}(\sqrt{-3})$
$\mathbb{Q}(\alpha)$
$\mathbb{Q}(\zeta\alpha)$
$\mathbb{Q}(\zeta^2\alpha)$
$\mathbb{Q}(\alpha, \zeta)$

3. Suppose that L is a finite field having p^n elements, where p is a prime number. Recall that $\text{Gal}(L : \mathbb{F}_p) = \langle \varphi \rangle$, where φ denotes the Frobenius mapping.
   (a) Show that whenever K is a subfield of L, then $|K| = p^d$ for some divisor d of n.

   Solution: Suppose that K is a subfield of L, and write $\mathbb{F}_p$ for the prime subfield of L. Then, by the Fundamental Theorem of Galois Theory, we see that $\text{Gal}(K : \mathbb{F}_p)$ is a subgroup of $\text{Gal}(L : \mathbb{F}_p)$. But the latter group is cyclic of order n, so that by Lagrange's theorem, any subgroup of $\text{Gal}(L : \mathbb{F}_p)$ must have order dividing n. Thus we see that $\text{Gal}(K : \mathbb{F}_p)$ has order d for some divisor d of n. Furthermore, we know that any subgroup of a cyclic group is normal. Thus, again by the Fundamental Theorem, we see that the field extension $K : \mathbb{F}_p$ is normal. But L is algebraic over its prime subfield, hence K is separable, and thus Galois. Then we deduce that $[K : \mathbb{F}_p] = |\text{Gal}(K : \mathbb{F}_p)| = d$, whence $|K| = p^d$.

   (b) Show that for each divisor d of n, there is a unique subfield K of L with $|K| = p^d$.

   Solution: Suppose that $d|n$. Observe that $\text{Gal}(L : \mathbb{F}_p)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and is generated by the Frobenius monomorphism ϕ. But there is precisely one subgroup of $\mathbb{Z}/n\mathbb{Z}$ of index d, and so $\text{Gal}(L : \mathbb{F}_p)$ likewise has precisely one subgroup of index d, namely $\langle \phi^d \rangle$. Then it follows from the Fundamental Theorem of Galois Theory that there is precisely one subfield K of L with $[K : \mathbb{F}_p] = d$, or equivalently, having p^d elements.

4. Let $L : K$ be a finite Galois extension with Galois group G.
   (a) For any $\alpha \in L$, define the *norm* of α by $\mathrm{N}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$. Show that $\mathrm{N}(\alpha) \in K$.
   Solution: Since $L : K$ is Galois, the fixed field of G is K. Then $\beta \in K$ if and only if $\tau(\beta) = \beta$ for every $\tau \in G$. But whenever $\tau \in G$, one has
$$\tau(\mathrm{N}(\alpha)) = \prod_{\sigma \in G} \tau(\sigma(\alpha)) = \prod_{\rho \in G} \rho(\alpha),$$
   since the action of τ on G is simply to permute the elements of G. Thus we see that $\tau(\mathrm{N}(\alpha)) = \mathrm{N}(\alpha)$ for every $\tau \in G$, whence $\mathrm{N}(\alpha) \in K$.
   (b) For any $\alpha \in L$, define the *trace* of α by $\mathrm{Tr}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$. Show that $\mathrm{Tr}(\alpha) \in K$.
   Solution: Whenever $\tau \in G$, one has
$$\tau(\mathrm{Tr}(\alpha)) = \sum_{\sigma \in G} \tau(\sigma(\alpha)) = \sum_{\rho \in G} \rho(\alpha),$$
   since the action of τ on G is simply to permute the elements of G. Thus we see that $\tau(\mathrm{Tr}(\alpha)) = \mathrm{Tr}(\alpha)$ for every $\tau \in G$, whence $\mathrm{Tr}(\alpha) \in K$.

5. Let p be a prime number, and n a natural number, and denote by $\mathbb{F}_q$ the finite field of $q = p^n$ elements with prime field $\mathbb{F}_p$. Let ϕ denote the Frobenius monomorphism from $\mathbb{F}_q$ into $\mathbb{F}_q$. Recall that $\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p) = \langle \phi \rangle$.
   (a) Defining the trace of $\alpha \in \mathbb{F}_q$ as in question 4(b) above, show that there exists an element $\alpha \in \mathbb{F}_q$ having non-zero trace.
   Solution: Since $\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p) = \langle \phi \rangle$ and $\phi^j(\alpha) = \alpha^{p^j}$ for each $\alpha \in \mathbb{F}_q$, we have
$$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}} = f(\alpha),$$
   where $f(t) = t + t^p + \ldots + t^{p^{n-1}}$. The polynomial f has at most $\deg(f) = p^{n-1}$ roots over $\mathbb{F}_q$, yet $\mathbb{F}_q$ has p^n elements. Thus $\mathbb{F}_q$ has at least $p^n - p^{n-1}$ elements α with $\mathrm{Tr}(\alpha) = f(\alpha) \neq 0$. So there exists $\alpha \in \mathbb{F}_q$ having non-zero trace.
   (b) Defining the norm of $\alpha \in \mathbb{F}_q$ as in question 4(a) above, show that there exists a non-zero element $\alpha \in \mathbb{F}_q^\times$ having norm different from 1.
   Solution: For each $\alpha \in \mathbb{F}_q^\times$, one has $\mathrm{N}(\alpha) = \alpha \cdot \alpha^p \cdot \ldots \cdot \alpha^{p^{n-1}} = \alpha^{(p^n-1)/(p-1)}$. Recalling that $\mathbb{F}_q^\times = \langle g \rangle$ for a suitable primitive element $g \in \mathbb{F}_q^\times$, we see that g has order $p^n - 1$, and thus (when $p \neq 2$) one has $N(g) = g^{(p^n-1)/(p-1)} \neq 1$. So there exists $\alpha \in \mathbb{F}_q$ having norm different from 1, *unless* $p = 2$, in which case *every* non-zero element of $\mathbb{F}_q$ has norm equal to 1.

GALOIS THEORY: SOLUTIONS TO HOMEWORK 14

1. (a) Show that $f = t^3 - 3t + 1$ is irreducible over $\mathbb{Q}$.
Solution: Reduce modulo 2 to get $t^3 + t + 1$, which is irreducible over $\mathbb{F}_2$ since neither 0 nor 1 is a root. Thus f is irreducible over $\mathbb{Z}$ and hence over $\mathbb{Q}$ by Gauss' Lemma.

(b) Show that whenever α is a root of f in a splitting field extension of $\mathbb{Q}$, then $\beta = \alpha^2 - 2$ is also a root of f.
Solution: We have $\beta^2 = \alpha^4 - 4\alpha^2 + 4 = -\alpha^2 - \alpha + 4$ and

$$\beta^3 = -\alpha^4 - \alpha^3 + 6\alpha^2 + 2\alpha - 8 = 3\alpha^2 - 7,$$

so $\beta^3 - 3\beta + 1 = (3\alpha^2 - 7) - 3(\alpha^2 - 2) + 1 = 0$.

(c) Let L be a splitting field for f over $\mathbb{Q}$. Use your answer to part (b) to show that $[L : \mathbb{Q}] = 3$, and conclude that the Galois group of f is isomorphic to $A_3 \cong C_3$.
Solution: Let α be a root of f in L. By part (b), we have that $\beta = \alpha^2 - 2$ is a root of f. Note also that $(\alpha^2 - 2) - \alpha \neq 0$ since the minimal polynomial of α is f, and thus $\beta \neq \alpha$. Therefore, the polynomial f has at least two roots in $\mathbb{Q}(\alpha) \subseteq L$. If f were to split as $(t - \alpha)(t - \beta)(t - \delta)$ in L, then by equating coefficients with $t^3 - 3t + 1$ we see that one would have $\alpha + \beta + \delta = 0$, whence $\mathbb{Q}(\alpha)$ contains δ as well. Thus f splits over $\mathbb{Q}(\alpha)$, so we must have $L = \mathbb{Q}(\alpha)$ and $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Since L is a splitting field for f and $\mathbb{Q}$ has characteristic 0, the field extension $L : \mathbb{Q}$ is Galois and the Galois group $\mathrm{Gal}(L : \mathbb{Q})$ has order $[L : \mathbb{Q}] = 3$. Finally, note that there is a unique group (up to isomorphism) of order 3, isomorphic to $C_3 \cong A_3$.

(d) Show that there is no $\gamma \in L$ such that $\gamma \notin \mathbb{Q}$ and $\gamma^3 \in \mathbb{Q}$, and conclude that $L : \mathbb{Q}$ is not a radical extension.
Solution: Suppose that $\gamma \in L \backslash \mathbb{Q}$ and that γ is a root of $t^3 - \lambda$ for some $\lambda \in \mathbb{Q}$. By the Tower Law we have $3 = [L : \mathbb{Q}] = [L : \mathbb{Q}(\gamma)][\mathbb{Q}(\gamma) : \mathbb{Q}]$. Since 3 is prime and $\gamma \notin \mathbb{Q}$, we must have $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 3$, from which it follows that $t^3 - \lambda$ is irreducible over $\mathbb{Q}$. Since $L : \mathbb{Q}$ is a normal extension containing a root of $t^3 - \lambda$, that polynomial must split over L, so L contains another root, say γ'. Now let $\omega = \gamma'/\gamma \in L$. Then one may check that ω is a root of $t^3 - 1$ different from 1, so it is a root of $t^2 + t + 1$. Since the latter polynomial is irreducible over $\mathbb{Q}$, it must be the minimal polynomial of ω. But then the Tower Law implies that $[L : \mathbb{Q}] = 3$ is divisible by $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, which is false. Thus no such γ can exist.

(e) By Cardano's formula, the equation $f = 0$ is soluble by radicals. How do you reconcile this observation with your answer to part (d)?
Solution: This does not contradict the fact that $f = 0$ is soluble by radicals, since for that to occur it is sufficient (and also necessary) for

the splitting field L to be *contained* in a radical extension. In the present example, $L = \mathbb{Q}(\alpha)$ is contained in $\mathbb{Q}(\alpha, \omega)$, where ω is a root of t^2+t+1, and $\mathbb{Q}(\alpha, \omega) : \mathbb{Q}$ is a radical extension. In fact, Cardano's formula shows that α may be expressed in terms of cube roots of elements of $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$.

2. Is the polynomial $t^5 - 4t^4 + 2$ soluble by radicals over $\mathbb{Q}$?
Solution: No. The polynomial $f(t) = t^5 - 4t^4 + 2$ is irreducible over $\mathbb{Q}$, as a consequence of Eisenstein's theorem using the prime 2. Let $L : \mathbb{Q}$ be a splitting field extension for f, and let $\alpha \in L$ be a root of f. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 5$, and from the tower law we find that 5 divides $[L : \mathbb{Q}]$. Thus $G = \mathrm{Gal}_{\mathbb{Q}}(f)$ is a subgroup of S_5 of order $|G| = [L : \mathbb{Q}]$ divisible by 5. In particular, since 5 is a prime number, we perceive that G has an element of order 5. Observe next that $f'(x) = x^3(5x - 16)$, so that $f'(x) = 0$ for precisely 2 real values of x, and so since
$$f(-1) = -3, \quad f(0) = 2, \quad f(1) = -1, \quad f(4) = 2,$$
then f has 3 real roots and 2 complex roots. Hence $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains a transposition fixing the real roots and interchanging the 2 complex roots by conjugation. Then since $\mathrm{Gal}_{\mathbb{Q}}(f)$ is isomorphic to a subgroup of S_5, and contains an element of order 5 and a transposition, it follows that in fact $\mathrm{Gal}_{\mathbb{Q}}(f)$ is isomorphic to the whole of S_5 (the group of permutations on 5 symbols). But S_5 contains the insoluble subgroup A_5, and hence is itself insoluble. We therefore conclude that $\mathrm{Gal}_{\mathbb{Q}}(f)$ is insoluble, and hence that $f(t) = 0$ cannot be solved by using radical extensions of $\mathbb{Q}$.

3. Is the polynomial $t^6 - 4t^2 + 2$ soluble by radicals over $\mathbb{Q}$?
Solution: Yes. The polynomial $g(x) = x^3 - 4x + 2$ is soluble by radicals since it is cubic (this is due to Cardano). Since $f(t) = t^6 - 4t^2 + 2 = g(t^2)$, it follows that if α is any root of f lying in a splitting field extension, then $g(\alpha^2) = 0$, so that $a = \alpha^2$ lies in a radical extension L of $\mathbb{Q}$. But $\alpha = \pm\sqrt{a}$, and hence α lies in $L(\sqrt{a})$, which is a radical extension of L, and hence also a radical extension of $\mathbb{Q}$. Thus $t^6 - 4t^2 + 2$ is indeed soluble by radicals over $\mathbb{Q}$.

4. Let n be a positive integer and K a field with characteristic not dividing n. Let $L = K(\zeta)$, where ζ is a primitive nth root of unity.
   (a) Show that $\mathrm{Gal}(L : K)$ is isomorphic to a subgroup of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$.
   Solution: The group of all nth roots of unity in L is easily seen to be generated by the primitive root ζ. From this it follows that L is a splitting field for $t^n - 1$ over K. Since the characteristic of K does not divide n, the polynomial $t^n - 1$ is relatively prime to its derivative nt^{n-1}, so $t^n - 1$ is a separable polynomial. Therefore $L : K$ is normal and separable, and hence is a Galois extension.
   Next, let $\sigma \in \mathrm{Gal}(L : K)$. Applying σ to the equation $\zeta^n = 1$, we have $\sigma(\zeta)^n = 1$, and thus $\sigma(\zeta)$ is also an nth root of unity. Thus, we find

that $\sigma(\zeta) = \zeta^{e(\sigma)}$ for some integer $e(\sigma)$. Let $\sigma' \in \mathrm{Gal}(L : K)$. Then

$$(\sigma' \circ \sigma)(\zeta) = \sigma'(\sigma(\zeta)) = \sigma'(\zeta^{e(\sigma)}) = \sigma'(\zeta)^{e(\sigma)} = (\zeta^{e(\sigma')})^{e(\sigma)} = \zeta^{e(\sigma')e(\sigma)}.$$

On the other hand, reversing the roles of σ and σ' and using the commutativity of integer multiplication (so that $e(\sigma')e(\sigma) = e(\sigma)e(\sigma')$), we arrive at the same expression. That is to say that σ and σ' commute, so $\mathrm{Gal}(L : K)$ is abelian.

We now take $\sigma' = \sigma^{-1}$ in the above to obtain $\zeta = \zeta^{e(\sigma^{-1})e(\sigma)}$. Since ζ is a primitive nth root of unity, it follows that $e(\sigma^{-1})e(\sigma) - 1$ is divisible by n, and thus $e(\sigma^{-1})e(\sigma) \equiv 1 \pmod{n}$. In particular, $e(\sigma)$ is invertible modulo n. Thus the reduction of $e(\sigma)$ modulo n defines a map $\varphi : \mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$. Again since ζ is a primitive root, it follows from the above equation that $e(\sigma'\sigma) \equiv e(\sigma')e(\sigma) \pmod{n}$, whence φ is a homomorphism.

Finally, note that since $L = K(\zeta)$, any $\sigma \in \mathrm{Gal}(L/K)$ is determined by its action on ζ. Thus, if $e(\sigma) \equiv e(\sigma') \pmod{n}$ then $\sigma(\zeta) = \sigma'(\zeta)$, so that $\sigma = \sigma'$. Therefore, φ is injective, and $\mathrm{Gal}(L/K)$ is isomorphic to its image in $(\mathbb{Z}/n\mathbb{Z})^\times$ under φ.

(b) Show that if n is prime and $K = \mathbb{Q}$ then either $L = K$ or $\mathrm{Gal}(L : K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Solution: If K already contains a primitive nth root of unity then we have $L = K$ and there is nothing to prove. Otherwise ζ is a root of $t^n - 1$ that does not lie in K; in particular, $\zeta \neq 1$, so it is a root of $\frac{t^n-1}{t-1} = t^{n-1}+\ldots+1$. We know already that this polynomial is irreducible when n is prime, and thus it is the minimal polynomial of ζ. Therefore $[L : \mathbb{Q}] = n - 1$, so $\mathrm{Gal}(L : \mathbb{Q})$ has order $n - 1$, and thus is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

Note: There was a question in class about what happens in general, when K is not necessarily equal to $\mathbb{Q}$ – can $\mathrm{Gal}(L : \mathbb{Q})$ be a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$? The answer is yes, one can have that this is a proper subgroup. The reason for this is that K may already contain d-th roots of unity for certain divisors d of n. For example, if $p \equiv 1 \pmod{3}$, then $\mathbb{F}_p$ contains primitive cube-roots of unity. Then, when $K = \mathbb{F}_p$, a situation wherein $\mathrm{char}(K) = p$, one has $(p, 3) = 1$ and yet when ζ is a primitive cube root of unity we have $L = K(\zeta) = K$ and $\mathrm{Gal}(L : \mathbb{Q})$ is trivial.

5. Let n be a positive integer. By Dirichlet's theorem, there exists a prime number p with $p \equiv 1 \pmod{n}$.

(a) Let $L = \mathbb{Q}(e^{2\pi i/p})$. Show that $\mathrm{Gal}(L : \mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

Solution: The desired conclusion here is immediate from part (b) of question 4, since $e^{2\pi i/p}$ is a primitive p-th root of unity.

(b) Show that $\mathbb{Q}(e^{2\pi i/p})$ contains a subfield M with the property that $\mathrm{Gal}(M : \mathbb{Q}) \cong C_n$.

Solution: Let p be a prime number with $p \equiv 1 \pmod{n}$. Recall that the multiplicative group of residues modulo p is cyclic for each prime number p. Thus, from part (a), there is some $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$ with the property that $\mathrm{Gal}(L:\mathbb{Q}) = \langle \sigma \rangle$, and moreover σ has order $p-1 = nd$, say. But then it follows that $\mathrm{Gal}(L:\mathbb{Q})$ has the subgroup $H = \langle \sigma^n \rangle$ of index d. Let $M = \mathrm{Fix}_L(H)$. Then, by the Fundamental Theorem of Galois Theory, one has $\mathrm{Gal}(L:M) = H$ and

$$\mathrm{Gal}(M:\mathbb{Q}) \cong \mathrm{Gal}(L:\mathbb{Q})/\mathrm{Gal}(L:M) \cong \langle \sigma \rangle / \langle \sigma^n \rangle \cong C_n,$$

since the cosets of $H = \langle \sigma^n \rangle$ within $\langle \sigma \rangle$ take the shape $\sigma^r H$ with $r = 0, 1, \ldots, n-1$.