26 Show the following:

a. If $K/\mathbb{Q}$ and $\sigma \in \operatorname{Aut} K$, then σ fixes $\mathbb{Q}$.

b. The field $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

Solution a. Let $\sigma \in \operatorname{Aut} K$. In particular, it is a homomorphism, so $\sigma(1) = 1$. Similarly, $\sigma(n) = \sigma(1) + \cdots + \sigma(1) = 1 + \cdots + 1 = n$, so σ fixes $\mathbb{Z}$. Now, for $a, b \in \mathbb{Z}$, we have

$$\sigma(a) = \sigma\Big(b\,\frac{a}{b}\Big) = \sigma(b)\,\sigma\Big(\frac{a}{b}\Big) \implies \sigma\Big(\frac{a}{b}\Big) = \frac{\sigma(a)}{\sigma(b)} = \frac{a}{b},$$

so σ fixes $\mathbb{Q}$.

b. Suppose otherwise, and let $\varphi\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ be an isomorphism. So, it fixes $\mathbb{Z}$ and hence $\mathbb{Q}$ also. There exist $a, b \in \mathbb{Q}$ so that $\varphi(\sqrt{2}) = a + b\sqrt{3}$. Then

$$2 = \varphi(\sqrt{2})^2 = (a + b\sqrt{3})^2 = a^2 + 2ab\sqrt{3} + 3b^2.$$

Since $a^2 + 3b^2 \in \mathbb{Q}$, it follows that $2ab = 0$, or else that would imply that $\sqrt{3} \in \mathbb{Q}$. If $b \neq 0$, then $3b^2 \geq 3 > 2$, so we must have $b = 2$. But this implies that $a^2 = 2 \implies \sqrt{2} \in \mathbb{Q}$, which is a contradiction. Hence, φ could not have existed to begin with, so the two fields are not isomorphic.

---

27 A primitive n-th root of unity is an element $z \in \mathbb{C}$ such that $z^n = 1$ and $z^r \neq 1$ for $1 \leq r < n$. Show the following:

a. There exist $\varphi(n) \coloneqq |\{d \mid 0 \leq d < n, \gcd(d, n) = 1\}|$ primitive n-th roots of unity.

b. If ω is a primitive n-th root of unity, then $\mathbb{Q}(\omega)$ is a splitting field of $t^n - 1 \in \mathbb{Q}[t]$ and $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal.

c. If $\omega_1, \ldots, \omega_{\varphi(n)}$ are the $\varphi(n)$ primitive n-th roots of unity of $t^n - 1 \in \mathbb{Q}[t]$ and $\sigma \in \operatorname{Aut} \mathbb{Q}(\omega_1)$, then $\sigma(\omega_1) = \omega_i$ for some i, $1 \leq i \leq \varphi(n)$.

Solution a. Let $n \geq 1$.

We claim that ζ^d is a primitive n-th root for $0 \leq d < n$ and $\gcd(d, n) = 1$, where $\zeta = e^{2\pi i/n}$. It's clear that $(\zeta^d)^n = 1$. Notice that $rd/n \in \mathbb{Z}$ if and only if $n \mid rd$ if and only if $an = rd$ for some $a \in \mathbb{Z}$. But this is impossible: Let p be a prime factor of n. Then $p \mid rd \implies p \mid r$, since n and d are coprime. Since this works for any prime factor of p, this means that $n \mid r$. Thus, $rd/n \notin \mathbb{Z}$, so $e^{2\pi ird/n} \neq 1$, so ζ^d is a primitive root of 1.

Now suppose $0 \leq d < n$, but $\gcd(d, n) = \ell > 1$, so that $n/\ell, d/\ell \in \mathbb{Z}$ and $n/\ell < n$. Then $(\zeta^d)^{n/\ell} = e^{2\pi i d/\ell} = 1$, so ζ^d is not a primitive n-th root.

All the n-th roots must be of the form ζ^d, since $z^n - 1$ has precisely n roots, counting multiplicities. Moreover, we have just shown that if $0 \leq d < n$, then ζ^d is a primitive n-th root of unity if and only if $\gcd(d, n) = 1$. Hence, $\varphi(n)$ is the number of primitive n-th roots of unity.

b. If ω is a primitive n-th root of unity, then $1, \omega, \omega^2, \ldots, \omega^{n-1}$ are the n roots of $t^n - 1$, because they are distinct. If not, then there exist $0 \leq a < b < n$ so that $\omega^a = \omega^b \implies \omega^{b-a} = 1$, which contradicts the fact that ω is primitive. Thus, $t^n - 1$ splits in $\mathbb{Q}(\omega)$.

Moreover, $(t^n - 1)/(t - 1) \in \mathbb{Q}[t]$ is the minimal polynomial of ω, since it is equal to

$$(t - \omega)(t - \omega^2) \cdots (t - \omega^{n-1}).$$

No power of ω is in $\mathbb{Q}[t]$, so it must be that this is the minimal polynomial, so $\mathbb{Q}(\omega)$ is the splitting field of $(t^n - 1)/(t - 1)$ over $\mathbb{Q}$, so it is normal.

c. Notice that $0 = \omega_1^n - 1$. Applying σ, we have $0 = \sigma(\omega_1)^n - 1$, so $\sigma(\omega_1)$ must be a root of unity. Similarly, if $1 \leq r < n$, then

$$1 \neq \omega_1^r \implies 1 \neq \sigma(\omega_1)^r,$$

since σ is an isomorphism. Thus, $\sigma(\omega_1)$ is a primitive root of unity, so it is equal to some ω_i.

28 Show the following:

a. Let $\Phi_n(t) = (t - \omega_1) \cdots (t - \omega_{\varphi(n)})$. Then $\Phi_n(t) \in \mathbb{Q}[t]$.

b. $\Phi_n(t) \in \mathbb{Z}[t]$.

Solution We will show that $\Phi_n(t) \in \mathbb{Z}[t]$, which proves both (a) and (b). We will do this by strong induction on n.

Base step: $n = 1$:

Here, $\Phi_1(t) = t - 1 \in \mathbb{Z}[t]$, so the inductive step holds.

Inductive step:

We will first show the following formula:

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

Let $\zeta = e^{2\pi i/n}$. Then

$$t^n - 1 = \prod_{k=0}^{n} (x - \zeta^k).$$

For each $0 \leq k < n$, $x - \zeta^k$ appears as a factor precisely once in one of the $\Phi_d(t)$. Indeed, if $\gcd(k, n) = 1$, then ζ^k is a primitive root, so $t - \zeta^k$ is a factor of Φ_n. Otherwise, $(\zeta^k)^r = 1$ for some $1 \leq r < n$, so ζ^k is a primitive root for Φ_r, where r is the smallest integer where this happens, which means that $t - \zeta^k$ is a factor of Φ_r.

Conversely, every factor of Φ_d for $d < n$ is an n-th root of unity, since $n/d \in \mathbb{Z}$, so $(e^{2\pi i/d})^n = 1$. This proves the formula.

By the inductive hypothesis, $\Phi_d \in \mathbb{Z}[t]$ for $d \mid n$, $d < n$, so

$$\prod_{\substack{d|n \\ d<n}} \Phi_d(t) \in \mathbb{Z}[t] \implies \Phi_n(t) = \frac{t^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(t)} \in \mathbb{Q}[t].$$

By multiplying by some N, we have $N\Phi_n \in \mathbb{Z}[t]$. Since the content of a polynomial is multiplicative and the product is monic, it follows that the content of $N\Phi_n$ is N, which means that $N\Phi_n/N = \Phi_n \in \mathbb{Z}[t]$, as required.

29 Show the following:

a. $\Phi_n(t) \in \mathbb{Z}[t]$ is irreducible.

b. Calculate $\Phi_n(t)$ for $n = 3, 4, 6, 8$ explicitly, and show directly that $\Phi_n(t) \in \mathbb{Z}[t]$ is irreducible.

Solution a. Let ζ be an n-th primitive root of unity, and let $f = m_{\mathbb{Z}}(\zeta)$, the minimal polynomial of ζ. By definition, f is irreducible, and we will show that $f = \Phi_n$.

Since $\Phi_n(\zeta) = 0$, we have that $f \mid \Phi_n$, so $\Phi_n = fg$, for some $g \in \mathbb{Z}[t]$. Now let p be a prime which does not divide n. Then $\gcd(p, n) = 1$, so ζ^p is also an n-th primitive root of unity, so $\Phi_n(\zeta^p) = 0$, by definition.

Now suppose that $f(\zeta^p) \neq 0$. Then necessarily $g(\zeta^p) = 0$, and thus, ζ is a root of $g(t^p)$. By definition of f, $f \mid g(t^p)$, and so $g(t^p) = fh$, for some $h \in \mathbb{Z}[t]$. Lastly, by the previous problem, we have that $\Phi_n \mid t^n - 1$, so $p\Phi_n = t^n - 1$ for some $p \in \mathbb{Z}[t]$. Altogether, we have

$$\begin{aligned} f(t)g(t)p(t) &= t^n - 1 \\ g(t^p) &= f(t)h(t). \end{aligned}$$

Now consider their canonical projection to $(\mathbb{Z}/p\mathbb{Z})[t]$, which gives

$$\begin{aligned} [f(t)][g(t)][p(t)] &= [t^n - 1] \\ [g(t^p)] &= [f(t)][h(t)]. \end{aligned}$$

Since $\mathbb{Z}/p\mathbb{Z}$ is a field with characteristic p, we have that $[g(t^p)] = [g(t)]^p = [f(t)][h(t)]$. Now let $[q(t)]$ be an irreducible factor of $[f(t)]$, so that $[q] \mid [g]^p \implies [q] \mid [g]$. Hence, from the first equation above, we see that $[q]^2 \mid [t^n - 1]$, i.e., $[t^n - 1]$ has a multiple root, and so, $[t^n - 1]' = [nt^{n-1}] = [n]t^{n-1} = 0$, since $\operatorname{char} \mathbb{Z}/p\mathbb{Z} = p$. But this is a contradiction, as we assumed that $p \nmid n$, so $[n] \neq 0$.

Hence, $f(\zeta^p) = 0$, so $f = m_{\mathbb{Z}}(\zeta^p)$ also. By repeating the argument with ζ replaced with ζ^p, we get that $f(\zeta^{p_1 p_2 \cdots p_m}) = 0$, for primes $p_i \nmid n$. In particular, $f(\zeta^d) = 0$ if $\gcd d, n = 1$, so every primitive n-th root of unity is a root of f. Thus, $\Phi_n \mid f$, so $f = \Phi_n$, hence irreducible, as required.

b. We have:

$$\begin{aligned} \Phi_3(t) &= \frac{t^3 - 1}{t - 1} = t^2 + t + 1 \\ \Phi_4(t) &= \frac{t^4 - 1}{t^2 - 1} = t^2 + 1 \\ \Phi_6(t) &= \frac{t^6 - 1}{(t+1)(t^3 - 1)} = t^2 - t + 1 \\ \Phi_8(t) &= \frac{t^8 - 1}{t^4 - 1} = t^4 + 1. \end{aligned}$$

The first three are irreducible by looking at the discriminants

$$\begin{aligned} \Delta_3 &= 1 - 4 = -3 < 0 \\ \Delta_4 &= 0 - 4 = -3 < 0 \\ \Delta_6 &= 1 - 4 = -3 < 0. \end{aligned}$$

As for Φ_8, we can use Eisenstein with $p = 2$: $\Phi_8(t + 1) = t^4 + 4t^3 + 6t^2 + 4t + 2$, so Φ_8 is irreducible. Thus, these are indeed the cyclotomic polynomials.

33 Let $\operatorname{char} F = p \neq 0$ and $a \in F$. Let $f = t^p - t - a \in F[t]$. Show the following:

a. f has no multiple roots.

b. If α is a root of f, then so is $\alpha + k$ for all $0 \leq k \leq p-1$.

c. f is irreducible if and only if f has no root in F.

d. Suppose that $a \neq b^p - b$ for any $b \in F$. Find $\operatorname{Gal}(K/F)$ where K is a splitting field of $t^p - t - a \in F[t]$.

Solution a. Notice that the derivative is $f' = pt^p - 1 = -1$, which is relatively prime to f, so f has no multiple roots.

b. Let α be a root of f. Then

$$f(\alpha + k) = (\alpha + k)^p - (\alpha + k) - a = \alpha^p + k^p - \alpha - k - a = (\alpha^p - \alpha - a) + k^p - k = k^p - k.$$

Since $k \in \mathbb{Z}/p\mathbb{Z} \subseteq F$, $k^p = k^{p-1}k = k$, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is a group of order $p-1$. Thus, $f(\alpha + k) = 0$.

c. "$\Longrightarrow$"

This is trivial.

"$\Longleftarrow$"

Suppose f has no root in F. By part (b), we know that f has the form

$$f(t) = \prod_{j=0}^{p-1} (t - (\alpha + k)).$$

Suppose f is reducible, so that $f = gh$ for some $g, h \in F[t]$. Then g has the form

$$g(t) = \prod_{j \in J \subseteq \{0,\ldots,p-1\}} (t - (\alpha + j)) = t^n - \sum_{j \in J} (\alpha + j) t^{n-1} + \cdots,$$

where $0 < n = |J| < p$, or else g or h is a constant. Since $g \in F[t]$, by expanding the sum, we see that $\sum_{j \in J} j \in F$ and so $n\alpha \in F$. We must have $n \neq 0, p$, or else n^{-1} exists since F is a field, which implies that $\alpha = n^{-1} n\alpha \in F$, which is impossible. Thus, $n = 0$ or $n = p$, which is a contradiction. Thus, f is irreducible, as required.

d. By assumption and (c), f is irreducible. Thus, $|\operatorname{Gal}(K/F)| = [K : F] = \deg f = p$. Thus, by Cauchy's theorem, $\operatorname{Gal}(K/F)$ is cyclic and every element other than the identity is a generator. Notice that $\alpha \mapsto \alpha + 1$ is an automorphism which fixes F. Thus,

$$\operatorname{Gal}(K/F) = \langle \alpha \mapsto \alpha + 1 \rangle = \{\alpha \mapsto \alpha + k \mid 0 \leq \alpha \leq p-1\} \simeq \mathbb{Z}/p\mathbb{Z}.$$

36 Let $f, g \in F[t]$ be relatively prime and suppose that $u = f/g$ lies in $F(t) \setminus F$.

a. Show that $F(t)/F(u)$ is finite of degree $d = \max\{\deg f, \deg g\}$.

b. $\mathrm{Gal}(F(t)/F)$ consists of all F-automorphisms of $F(t)$ mapping t to $(at + b)/(ct + d)$ where $a, b, c, d \in F$ satisfies $ad - bc \neq 0$.

Solution a. Assume without loss of generality that $d = \deg f \geq \deg g = \ell$. In the other case, we may replace u with $1/u$, which gives the same field extension as $F(u)$.

Consider $f(x) - u(t)g(x) \in F(u)[x]$. This is irreducible, since f and g are relatively prime. Moreover, since $d \geq \ell$, $\deg(f(x) - u(t)g(x)) = d$, so $[F(t) : F(u)] = d$, as required.

b. Since F is fixed by $\sigma \in \mathrm{Gal}(F(t)/F)$, we just need to consider how σ acts on t. Since σ is an automorphism, $t \mapsto f(t)/g(t) := u(t)$, for some polynomials $f, g \in F[t]$. We may assume that f and g are relatively prime, by removing common factors. Moreover, $f/g \notin F$, or else σ would not be an automorphism.

By (a), $[F(t) : F(u)] = \max\{\deg f, \deg g\}$. Since we want σ to be an automorphism, we need $[F(t) : F(u)] = 1$, which means that $\deg f = \deg g = 1$. Thus, σ is of the form

$$t \mapsto \frac{at + b}{ct + d} = \frac{t + \frac{b}{a}}{t + \frac{d}{c}}.$$

To ensure f and g have no common factors, we need $b/a \neq d/c \iff ad - bc \neq 0$, so σ has the correct form.

Conversely, $t \mapsto (at + b)/(ct + d)$ with $ad - bc \neq 0$ is in $\mathrm{Gal}(F(t)/F)$. It's easy to see that it's a homomorphism, and it has the inverse

$$s \mapsto \frac{ds - b}{-cs + a},$$

so it is an automorphism. Thus, $\mathrm{Gal}(F(t)/F)$ consists of all F-automorphisms of the form described.

---

42 Suppose that $|K| = p^m$ and $F \subseteq K$. Show that $|F| = p^n$ for some n with $n \mid m$. Moreover, $\mathrm{Gal}(K/F)$ is generated by the Frobenius automorphism $\alpha \mapsto \alpha^{p^n}$.

Solution Notice that $\mathrm{char}\, F = \mathrm{char}\, K = p$, since F is a subfield of K. Thus, $|F| = p^n$, for some $n \geq 1$.

Consider K/F, which is finite since K is a finite field, and let $\{\alpha_1, \ldots, \alpha_k\}$ be a basis. Then we have p^n choices for each coefficient of α_i, so $|K| = (p^n)^k = p^{nk} = p^m \implies nk = m$. Hence, $n \mid m$.

Now, let σ be the Frobenius automorphism $\alpha \mapsto \alpha^p$. Since $F^\times$ has order $p^n - 1$, $\sigma(\alpha) = \alpha$ for all $\alpha \in F$, so σ fixes F. We know that σ is a field homomorphism, and fields are simple, so σ is actually injective. Since K is a finite group, σ is an isomorphism, hence $\sigma \in \mathrm{Gal}(K/F)$.

Notice that $|\mathrm{Gal}(K/\mathbb{Z}/p\mathbb{Z})| = [F : \mathbb{Z}/p\mathbb{Z}] = n$. Indeed, suppose $F/(\mathbb{Z}/p\mathbb{Z})$ has dimension k. Then it has k basis elements, and for each one, we have p coefficients from $\mathbb{Z}/p\mathbb{Z}$, which gives p^k total elements. Since $|F| = p^n$, this implies that $k = n$.

We now calculate the order of σ: Let $k \geq 1$ be so that $\sigma^k(t) = t^{p^k}$ is the identity on K, so we have that the function $\alpha^{p^k} - \alpha = 0$ for every $\alpha \in K$. The polynomial $t^{p^k} - t$ has at most p^k roots, so $p^n \leq p^k$, since every element of K is a root. Thus, $p^n = p^k \implies n = k$, so σ has order n and hence σ generates $\mathrm{Gal}(K/F)$, as required.

46 Let $F = \mathbb{R}$. Let $f = t^3 - a_1t^2 - a_2t - a_3 \in \mathbb{R}[t]$. Show:

a. The discriminant is $\Delta = -4a_1^3a_3 + a_1^2a_2^2 - 18a_1a_2a_3 + 4a_2^3 - 27a_3^2$.

b. f has multiple roots if and only if $\Delta = 0$.

c. f has three distinct real roots if and only if $\Delta > 0$.

d. f has one real root and two non-real roots if and only if $\Delta < 0$.

Solution a. If α_1, α_2, and α_3 are roots of f, then

$$f = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3) = t^3 - (\alpha_1+\alpha_2+\alpha_3)t^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)t - \alpha_1\alpha_2\alpha_3,$$

so

$$\begin{aligned} a_1 &= \alpha_1 + \alpha_2 + \alpha_3 \\ a_2 &= -(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\ a_3 &= \alpha_1\alpha_2\alpha_3. \end{aligned}$$

Now suppose $\alpha_1 = \alpha_2$, so that $a_1 = 2\alpha_1 + \alpha_3$, $a_2 = -(\alpha_1^2 + 2\alpha_1\alpha_3)$, and $a_3 = \alpha_1^2\alpha_3$. Substituting into the expression given,

$$\begin{aligned} -4(2\alpha_1+\alpha_3)^3 a_1^2\alpha_3 + (2\alpha_1+\alpha_3)^2\left[-(\alpha_1^2+2\alpha_1\alpha_3)\right]^2 \\ + 18(2\alpha_1+\alpha_3)(\alpha_1^2+2\alpha_1\alpha_3)\alpha_1^2\alpha_3 - 4(\alpha_1^2+2\alpha_1\alpha_3)^3 - 27(\alpha_1^2\alpha_3)^2 = 0, \end{aligned}$$

by WolframAlpha. By symmetry, $\Delta = 0$ whenever $\alpha_i = \alpha_j$, $i \neq j$. By definition,

$$\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2.$$

Thus, if we let α_1 vary, we may regard $\Delta \in \mathbb{R}[\alpha_1]$, and Δ has degree 4 with roots α_2 and α_3, both with multiplicity 2. The expression given is also a degree 4 polynomial and by the argument before the above, its zeros are also α_2 and α_3 with multiplicity 2, by taking derivatives and using WolframAlpha again. Thus, they must be the same polynomial, as required.

b. "$\Longrightarrow$" is clear by definition of Δ. The converse is true by the argument above: if we regard $\Delta \in \mathbb{R}[\alpha_1]$, then its roots are precisely α_2 and α_3. By symmetry of the α_i, we conclude that $\Delta = 0$ means that $\alpha_i = \alpha_j$ for some $i \neq j$.

c. Recall the Vandermonde matrix

$$M = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{pmatrix}$$

and that its determinant is $\det M = \sqrt{\Delta} = (\alpha_2\alpha_3^2 - \alpha_3\alpha_2^2) - (\alpha_1\alpha_3^2 - \alpha_3\alpha_1^2) + (\alpha_1\alpha_2^2 - \alpha_2\alpha_1^2)$.

"$\Longrightarrow$"

Then no factors of the discriminant are 0, and every factor in the product is a real, positive number, so $\Delta > 0$.

"$\Longleftarrow$"

Assume without loss of generality that $\alpha_1 \in \mathbb{R}$.

If $\alpha_1 = 0$, then $a_3 = 0$, so $f = t(t^2 - a_1t - a_2)$. Hence, $\Delta = a_2^2(a_1^2 + 4a_2) > 0 \iff a_1^2 + 4a_2 > 0$, which corresponds to the usual discriminant for quadratics, so f has three real roots. Thus, from now on, assume that $\alpha_1 \neq 0$.

Notice that

$$\sqrt{\Delta} = \alpha_1\alpha_2\alpha_3\left(\frac{\alpha_3 - \alpha_2}{\alpha_1} - \frac{\alpha_3 - \alpha_1}{\alpha_2} + \frac{\alpha_2 - \alpha_1}{\alpha_3}\right) > 0$$

Now suppose that one of α_2 and α_3 are complex. Then because the coefficients of f are real, α_2 and α_3 are non-zero complex conjugates, so $\alpha_2\alpha_3 = |\alpha_2|^2$. Assume further, without loss of generality, that $\operatorname{Im}\alpha_2 > 0$. Then

$$\begin{aligned}\sqrt{\Delta} = \alpha_1|\alpha_2|^2\left(\frac{\alpha_3-\alpha_2}{\alpha_1} - \frac{\alpha_3^2-\alpha_1\alpha_3}{|\alpha_2|^2} + \frac{\alpha_2^2-\alpha_1\alpha_2}{|\alpha_2|^2}\right) &= \alpha_1|\alpha_2|^2\left(\frac{\alpha_3-\alpha_2}{\alpha_1} + \frac{\alpha_2^2-\alpha_3^2-\alpha_1(\alpha_2-\alpha_3)}{|\alpha_2|^2}\right)\\ &= 2i\alpha_1|\alpha_2|^2\operatorname{Im}\alpha_2\left(-\frac{1}{\alpha_1} + \frac{2\operatorname{Re}\alpha_2-\alpha_1}{|\alpha_2|^2}\right)\\ &= 2i\operatorname{Im}\alpha_2\big(2\alpha_1\operatorname{Re}\alpha_2 - |\alpha_2|^2 - \alpha_1^2\big).\end{aligned}$$

But this is purely imaginary, which is impossible since it implies that $\Delta < 0$. Hence, α_2 and α_3 must have been real.

d. Without loss of generality, assume that α_1 is the real root.

“$\Longrightarrow$”

Because f has real coefficients, α_2 and α_3 are complex conjugates. Thus, $\alpha_2 - \alpha_3 = 2i\operatorname{Im}\alpha_2$, whereas $\alpha_2 + \alpha_3 = 2\operatorname{Re}\alpha_2$. Hence, in the product for Δ, exactly one of the terms is the square of a purely imaginary number, so $\Delta < 0$.

“$\Longleftarrow$”

By the same calculation above,

$$\sqrt{\Delta} \in i\mathbb{R} \implies \Delta < 0,$$

as required.

---

47 Let $x^3 + px + q$ be irreducible over a finite field K of characteristic not 2 or 3. Show that $-4p^3 - 27q^2$ is a square in K.

Solution Notice that the discriminant of the polynomial is $-4p^3 - 27q^2$, but discriminants of polynomials are squares by definition, so $-4p^3 - 27q^2$ is a square.

---

49 Let K be a subfield of the real numbers, f an irreducible quartic over K. Suppose that f has exactly two real roots. Show that the Galois group of f is either S_4 or of order 8.

Solution Let L be the splitting field of f. Since f is irreducible and because there are 4 roots, $\operatorname{Gal}(L/K)$ is a transitive subgroup of S_4. Because K is a subfield of $\mathbb{R}$, f has real coefficients, so the two complex roots must be conjugates of each other.

The transitive subgroups of S_4, A_4, the subgroups of order 8, $\mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The Galois group is non-trivial, since conjugation is a non-trivial permutation, so it is not the trivial group.

Complex conjugation is a single transposition, so it is an odd permutation. Thus, $\operatorname{Gal}(L/K)$ cannot be A_4 or its subgroup $\mathbb{Z}/4\mathbb{Z}$.

Now suppose that $\operatorname{Gal}(L/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Conjugation is an element of the group, flipping the real roots is also one, their product is another one, and the identity is one, so these would have to be the only elements. But then there are no permutations sending a real root to a complex one, which is impossible, as $\operatorname{Gal}(L/K)$ is transitive. Hence, $\operatorname{Gal}(L/K)$ must be S_4 or a group of order 8.