Leonid Monin
Léo Navarro Chafloque

Solutions – Semaine 8

Exercice 1 (Polynômes irréductibles I). (a) Montrer que $\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}$ est un polynôme irréductible de $\mathbb{Q}[x]$.

(b) Montrer que $x^4+[2]_5$ est un polynôme irréductible de $\mathbb{F}_5[x]$ et conclure que x^4+15x^3+7 est un polynôme irréductible de $\mathbb{Q}[x]$.

(c) Montrer que x^2+y^2+1 est un polynôme irréductible de $\mathbb{R}[x,y]$.

(d) Montrer que $x^2+y^2+[1]_2$ n'est pas un polynôme irréductible de $\mathbb{F}_2[x,y]$.

(e) Montrer que $y^4+x^3+x^2y^2+xy+2x^2-x+1$ est un polynôme irréductible de $\mathbb{Q}[x,y]$.

(f) Montrer que $4x^3+120x^2+8x-12$ est un polynôme irréductible de $\mathbb{Q}[x]$.

(g) Montrer que t^6+t^3+1 est un polynôme irréductible de $\mathbb{Q}[t]$.

(h) Montrer que $y^4+xy^3+xy^2+x^2y+3x^2-2x$ est un polynôme irréductible de $\mathbb{Q}[x,y]$.

Solution.

(a) We write $\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}=\frac{1}{9}(2x^5+15x^4+9x^3+3)\in\mathbb{Q}[x]$.

Now $\frac{1}{9}\in\mathbb{Q}[x]^\times$, as $\frac{1}{9}\in\mathbb{Q}^\times$. Therefore $\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}$ is irreducible in $\mathbb{Q}[x]$ if and only if $2x^5+15x^4+9x^3+3$ is. As $\gcd(2,15,9,3)=1$, we have that $2x^5+15x^4+9x^3+3$ is primitive, hence it is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Gauss Lemma). Using Eisenstein for $p=3$, where $3\in\mathbb{Z}$ is irreducible, we deduce that $2x^5+15x^4+9x^3+3$ is irreducible in $\mathbb{Z}[x]$.

(b) Let $f(x)=x^4+[2]_5\in\mathbb{F}_5[x]$. Note that for all $a\in\mathbb{F}_5$ we have $a^2\in\{[0]_5,[1]_5,[4]_5\}$. Therefore f does not admit roots in $\mathbb{F}_5$. We will now show that f is not a product of two polynomials of degree 2. As $\mathbb{F}_5$ is a field, we can assume that these polynomials are unitary and so assume there exist $a,b,c,d\in\mathbb{F}_5$ such that

$$f(x)=x^4+[2]_5=(x^2+ax+b)(x^2+cx+d)=x^4+(a+c)x^3+(b+ac+d)x^2+(bc+ad)x+bd.$$

Then $c=-a$ and $d=[2]_5b^{-1}$ and substituting in the above gives:

$$x^4+[2]_5=x^4+(b-a^2+[2]_5\cdot b^{-1})x^2+(-ab+[2]_5\cdot ab^{-1})x+[2]_5.$$

Thus $-ab+[2]_5\cdot ab^{-1}=a(-b+[2]_5\cdot b^{-1})=0$ and

- if $a=0$, then $b^2=-[2]_5$, a contradiction.
- if $-b+[2]_5b^{-1}=0$, then $b^2=[2]_5$, a contradiction.

We conclude that f is irreducible in $\mathbb{F}_5[x]$.

Lastly, let $x^4+15x^3+7\in\mathbb{Q}[x]$. As the dominant coefficient is 1, this polynomial is primitive, hence it is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Gauss Lemma). Let $\phi_5:\mathbb{Z}\to\mathbb{F}_5$ be the quotient homomorphism and let $\pi_5:\mathbb{Z}[x]\to\mathbb{F}_5[x]$ be its induced homomorphism. We have that:

$$\pi_5(x^4+15x^3+7)=x^4+[2]_5$$

and, as $x^4+[2]_5$ is irreducible in $\mathbb{F}_5[x]$, we use Proposition 3.9.1 to conclude that x^4+15x^3+7 is irreducible in $\mathbb{Z}[x]$.

(c) First we note that $x^2+y^2+1 \in \mathbb{R}[x,y]$ is primitive as its dominant coefficient is 1. Secondly, $y^2+1 \in \mathbb{R}[y]$ is irreducible. We now apply Eisenstein with $p = y^2+1$ to conclude that x^2+y^2+1 is irreducible in $\mathbb{R}[x,y]$.

(d) We have $x^2+y^2+[1]_2 = (x+y+[1]_2)^2$ in $\mathbb{F}_2[x,y]$.

(e) The evaluation homomorphism $\text{ev}_0 : \mathbb{Q}[y] \to \mathbb{Q}$, $\text{ev}_0(y) = 0$, induces the homomorphism $\xi : \mathbb{Q}[y][x] \to \mathbb{Q}[x]$ with $\xi(y) = 0$ and $\xi(x) = x$. We have that:

$$\xi(y^4+x^3+x^2y^2+xy+2x^2-x+1) = x^3+2x^2-x+1$$

and, $y^4+x^3+x^2y^2+xy+2x^2-x+1$ is irreducible in $\mathbb{Q}[x,y]$ if x^3+2x^2-x+1 is irreducible in $\mathbb{Q}[x]$ by a proposition seen in class: if $A \to B$ is any morphism between domains, then if the image in $B[t]$ by the induced morphism $A[t] \to B[t]$ of a polynomnial $p(t) \in A[t]$ is irreducible, then the same goes for $p(t)$. Now $\deg(x^3+2x^2-x+1) = 3$ and thus x^3+2x^2-x+1 is irreducible in $\mathbb{Q}[x]$ if and only if it does not admit roots in $\mathbb{Q}$. Assume $\frac{p}{r} \in \mathbb{Q}$, where $p, r \in \mathbb{Z}$ and $\gcd(p,r) = 1$, is a root of x^3+2x^2-x+1. Then

$$\left(\frac{p}{r}\right)^3 + 2\left(\frac{p}{r}\right)^2 - \left(\frac{p}{r}\right) + 1 = 0.$$

As $\gcd(p,r) = 1$, it follows that $p|1$, $r|1$ and so $\frac{p}{r} \in \{-1,1\}$. One checks that neither -1, nor 1 is a root of x^3+2x^2-x+1 and thus x^3+2x^2-x+1 is irreducible in $\mathbb{Q}[x]$.

(f) We have $4x^3+120x^2+8x-12 = 4(x^3+30x^2+2x-3) \in \mathbb{Q}[x]$. Now $4 \in \mathbb{Q}[x]^\times$ and so $4x^3+120x^2+8x-12$ is irreducible in $\mathbb{Q}[x]$ if and only if x^3+30x^2+2x-3 is. As $\deg(x^3+30x^2+2x-3) = 3$ it follows that x^3+30x^2+2x-3 is irreducible in $\mathbb{Q}[x]$ if and only if it does not admit roots in $\mathbb{Q}$. Assume there exist $\frac{p}{r} \in \mathbb{Q}$, where $p, r \in \mathbb{Z}$ and $\gcd(p,r) = 1$, such that:

$$\left(\frac{p}{r}\right)^3 + 30\left(\frac{p}{r}\right)^2 + 2\left(\frac{p}{r}\right) - 3 = 0.$$

As $\gcd(p,r) = 1$, it follows that $p|3$ and $r|1$. Therefore $\frac{p}{r} \in \{-3,-1,1,3\}$. One checks that none of the elements in $\{-3,-1,1,3\}$ is a root of x^3+30x^2+2x-3. We conclude that x^3+30x^2+2x-3 is irreducible in $\mathbb{Q}[x]$. .

(g) As the polynomial t^6+t^3+1 is primitive, it follows that it is irreducible in $\mathbb{Q}[t]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Gauss Lemma). We consider the quotient homomorphism $\phi_2 : \mathbb{Z} \to \mathbb{F}_2$ and its induced homomorphism $\pi_2 : \mathbb{Z}[t] \to \mathbb{F}_2[t]$ under which

$$\pi_2(t^6+t^3+1) = t^6+t^3+[1]_2.$$

Note that t^6+t^3+1 is irreducible in $\mathbb{Z}[t]$ if $t^6+t^3+[1]_2$ is irreducible in $\mathbb{F}_2[t]$ by a proposition seen in class.

Now, one checks that $t^6+t^3+[1]_2$ does not admit roots in $\mathbb{F}_2[t]$. Secondly, the only irreducible polynomial of degree 2 in $\mathbb{F}_2[t]$ is $t^2+t+[1]_2$ and one checks that this does not divide $t^6+t^3+[1]_2$. Lastly, we assume that $t^6+t^3+[1]_2$ is a product of two polynomials of degree 3. As $\mathbb{F}_2$ is a field, we can assume that these polynomials are unitary and we have:

$$\begin{aligned} t^6+t^3+[1]_2 &= (t^3+a_2t^2+a_1t+a_0)(t^3+b_2t^2+b_1t+b_0) \\ &= t^6+(a_2+b_2)t^5+(a_1+a_2b_2+b_1)t^4+(a_0+a_1b_2+a_2b_1+b_0)t^3+ \\ &\quad +(a_0b_2+a_1b_1+a_2b_0)t^2+(a_0b_1+a_1b_0)t+a_0b_0. \end{aligned}$$

Then $a_0 = b_0 = [1]_2$, $a_2 = b_2$ and

$$\begin{cases} a_0b_1+a_1b_0 = [0]_2 \\ a_0b_2+a_1b_1+a_2b_0 = [0]_2 \\ a_0+a_1b_2+a_2b_1+b_0 = [1]_2 \\ a_1+a_2b_2+b_1 = [0]_2 \end{cases} \to \begin{cases} b_1+a_1 = [0]_2 \\ a_1b_1 = [0]_2 \\ b_2(a_1+b_1) = [1]_2 \\ a_2b_2 = [0]_2 \end{cases} \to [1]_2 = [0]_2.$$

We conclude that $t^6 + t^3 + [1]_2$ is irreducible in $\mathbb{F}_2[t]$.

(h) We first note that the ring $\mathbb{Q}[x]$ is factorial, because is Euclidean and that $x \in \mathbb{Q}[x]$ is irreducible. Secondly the polynomial $y^4 + xy^3 + xy^2 + x^2y + 3x^2 - 2x \in \mathbb{Q}[x, y]$ is primitive, as its dominant coefficient is 1. We now apply Eisenstein with $p = x$ to conclude that $y^4 + xy^3 + xy^2 + x^2y + 3x^2 - 2x$ is irreducible in $\mathbb{Q}[x, y]$.

Exercice 2 (Polynômes irréductibles II).
Soit $f(t) = t^4 + 4t^3 + 3t^2 + 7t - 4$ dans $\mathbb{Z}[t]$.

(a) Montrer que $\pi_2(f)$, la réduction modulo 2, n'est pas irréductible.

(b) Montrer que $\pi_3(f)$, la réduction modulo 3, n'est pas irréductible.

(c) Utiliser les décompositions des parties précédentes pour conclure néanmoins que f est irréductible.

Solution.
Let $f(t) = t^4 + 4t^3 + 3t^2 + 7t - 4 \in \mathbb{Z}[t]$.

(a) We have $\pi_2(f(t)) = t^4 + t^2 + t = t(t^3 + t + [1]_2) \in \mathbb{F}_2[t]$. Moreover, we remark that $t^3 + t + [1]_2$ is irreducible in $\mathbb{F}_2[t]$, as it does not admit roots in $\mathbb{F}_2$.

(b) We have $\pi_3(f(t)) = t^4 + t^3 + t - [1]_3 = (t^2 + [1]_3)(t^2 + t - [1]_3) \in \mathbb{F}_3[t]$.

(c) Assume that $f(t)$ is reducible in $\mathbb{Z}[t]$. Then either $f(t) = (t - a)g(t)$, where $a \in \mathbb{Z}$ and $g(t) \in \mathbb{Z}[t]$ is a polynomial of degree 3, or $f(t) = f_1(t)f_2(t)$, where $f_1(t), f_2(t) \in \mathbb{Z}[t]$ are two polynomials of degree 2.

In the first case, $a|4$ but none of the elements of $\{\pm 1, \pm 2, \pm 4\}$ are roots of f. Hence, we only need to consider the case when $f(t) = f_1(t)f_2(t)$, where $\deg(f_1(t)) = \deg(f_2(t)) = 2$, and we have:

$$\pi_2(f(t)) = \pi_2(f_1(t)f_2(t)) = \pi_2(f_1(t))\pi_2(f_2(t).$$

Now, as $\deg(\pi_2(f(t))) = 4$ and as $\deg(\pi_2(f_1(t))) = \deg(\pi_2(f_2(t))) \leq 2$, it follows that $\deg(\pi_2(f_1(t))) = 2$ and $\deg(\pi_2(f_2(t))) = 2$.

On the other hand, we have $\pi_2(f(t)) = t^4 + t^2 + t = t(t^3 + t + [1]_2)$, where $t^3 + t + [1]_2 \in \mathbb{F}_2[t]$ is irreducible. We have arrived at a contradiction. We conclude that $f(t) \in \mathbb{Z}[t]$ is irreducible.

Exercice 3 (Polynômes irréductibles III).
Montrer que les polynômes suivants sont irréductibles dans $\mathbb{Q}[t]$.

1. $t^3 + 67t + 2027$
2. $3t^2 + 12t + 3$
3. $t^n - p$ où $n \in \mathbb{N}$ et p un nombre premier.
4. $7t^3 + 2t^2 + 2t + 20$

Indication: Pour le dernier point, on peut procéder ainsi. On montre que $\mathbb{Z}[\frac{1}{7}] = \{\frac{a}{7^n} \mid a \in \mathbb{Z} \quad n \in \mathbb{N}\}$ *est un anneau factoriel de corps des fractions* $\mathbb{Q}$*. On montre qu'on a un morphisme surjectif* $\mathbb{Z}[\frac{1}{7}] \to \mathbb{Z}/p\mathbb{Z}$ *pour tout premier* $p \neq 7$*. Ensuite on choisit un premier arrangeant pour montrer que la réduction de* $7t^3 + 2t^2 + 2t + 20$ *est irréductible dans* $\mathbb{F}_p[t]$*.*

Solution.
On profite de rappeler les critères, techniques utiles, pour montrer qu'un polynôme est irréductible. Soit A un anneau intègre et $p(t) \in A[t]$ un polynôme.

(a) Si $p(t)$ est monique et que $A \to B$ est n'importe quel morphisme vers un autre anneau intègre, alors si l'image par le morphisme induit de $p(t)$ dans $B[t]$ est irréductible, on peut conclure que $p(t)$ est irréductible dans $A[t]$. Cela est particulièrement pour simplifier l'anneau A. Par exemple on peut passer de A à n'importe quel quotient $B = A/\mathfrak{m}$ où $\mathfrak{m}$ est un idéal maximal. L'anneau B est alors un corps est c'est parfois plus aisé de montrer qu'un polynôme est irréductible sur un corps. Par exemple on peut prendre $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ pour tout premier p.

(b) Si A est factoriel on a de plus le critère d'Eisenstein: s'il existe un irréductible $p \in A$ tel que p divise tout les coefficients du polynôme sauf le dominant, et que p^2 ne divise pas le coefficient constant, alors le polynôme est irréductible.

(c) Encore dans le cas factoriel, si de plus le polynôme est primitif, il est équivalent de montrer que $p(t)$ est irréductible dans $K[t]$ où K est le corps des fractions de A. Ce principe est dénommé le lemme de Gauss.

(d) Si $\phi\colon A[t] \to A[t]$ est un automorphisme d'anneau alors $p(t)$ est irréductible si et seulement $\phi(p(t))$ l'est. Par exemple on peut utiliser des changements de variable linéaires $t \mapsto t + a$ pour $a \in A$.

(e) Si $A = k$ est un corps, et que $p(t)$ est de degré 2 ou 3, alors $p(t)$ est irréductible si et seulement si $p(t)$ ne s'annule en aucun élément de k.

On passe maintenant à la correction de l'exercice.

1. Ici on peut utiliser Gauss, puis on peut réduire modulo 3 pour obtenir $t^3 + t + 2$ qui n'a pas de racine dans $\mathbb{Z}/3\mathbb{Z}$ ce qui implique qu'il est irréductible dans $\mathbb{Z}/3\mathbb{Z}[t]$. On déduit que $t^3 + 67t + 2027$ est irréductible dans $\mathbb{Z}[t]$ puis dans $\mathbb{Q}[t]$ par Gauss.

2. Ici pour montrer que ce polynôme dans $\mathbb{Q}[t]$ est irréductible on peut multiplier par l'inversible $1/3$. Alors on a $t^2 + 4t + 1$ qui n'as pas de racine modulo 5, est ainsi irréductible modulo 5. On conclut comme au point précédent.

3. Ici on peut utiliser le critère d'Eisenstein dans $\mathbb{Z}[t]$ en conjonction avec Gauss.

4. Premièrement comme le polynôme est primitif Ici, il est tentant d'utiliser Eisenstein avec 2 mais $4 \mid 20$ alors ce n'est pas possible.

   On passe alors dans $\mathbb{Z}[\frac{1}{7}][t]$. Notons que si $p \neq 7$ alors comme $(p, 7) = 1$, donc qu'il existe des entiers $m, n \in \mathbb{Z}$ avec $7m = 1 + pn$ on voit que 7 est inversible dans $\mathbb{Z}/p\mathbb{Z}$ ce qui montre que le morphisme naturel $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}[1/7]/p\mathbb{Z}[1/7]$ est surjectif. Il est injectif en tant que morphisme de source un corps vers un anneau non-nul, c'est donc une bijection.

   On note également que $7 \equiv 1$ modulo $3\mathbb{Z}$. Alors, comme le coefficient dominant de $7t^3 + 2t^2 + 2t + 20$ est invesible dans $\mathbb{Z}[1/7]$, on se ramène à montrer en réduisant modulo 3 à montrer que $t^3 + 2t^2 + 2t + 2$ est irréductible dans $\mathbb{Z}/3\mathbb{Z}[t]$, ce qui est correct car il n'a pas de racines. Ainsi on conclut que $7t^3 + 2t^2 + 2t + 20$ est irréductible dans $\mathbb{Z}[1/7][t]$.

   Maintenant, en utilisant que $\mathbb{Z}[1/7]$ est factoriel (voir ci-dessous) de corps des fractions $\mathbb{Q}$ on conclut en utilisant Gauss. À noter que grâce à Gauss pour passer de $\mathbb{Q}$ à $\mathbb{Z}$, ce polynôme est aussi irréductible dans $\mathbb{Z}[t]$.

On montre le fait suivant: soit A un anneau factoriel et $a \in A$ non-nul. Alors $A[1/a]$ est encore factoriel. En effet écrivons $a = p_1 \cdots p_r$ comme un produit d'irréductibles. Alors notons que $p_1, \ldots, p_r$ deviennent inversibles dans $A[1/a]$.

Soit q un irréductible de A qui n'apparaît pas dans la décomposition de a. On affirme que q est alors encore irréductible dans $A[1/a]$. En effet si $q = (b/a^n)(c/a^m)$ pour $a, b \in A$ et $n, m \in \mathbb{N}$ avec $(b, a) = (c, a) = 1$ alors on a que $a^{m+n}q = bc$ comme les premiers dans le décomposition de a ne

divisent ni q ni b ni c on voit que $m = n = 0$ et donc que soit b soit c est inversible dans A, ce qui conclut la preuve de l'affirmation.

Notons également que si u est inversible dans $A[1/a]$ alors si l'on écrit $u = f/a^n$ pour $f \in A$ et $n \in \mathbb{N}$, alors f est inversible dans $A[1/a]$ ce qui implique qu'il existe $m \in \mathbb{N}$ et $g \in A$ avec $fg = a^m$ dans A. Alors les facteurs irréductibles de f sont forcément communs à ceux de A.

Notons dès lors que si $q' = q/a^n \in A[1/a]$ avec $q \in A$, $n \in \mathbb{N}$ et $(q, a) = 1$ est irréductible dans $A[1/a]$ cela implique que q est irréductible dans A. En effet si ce n'est pas le cas $q = q_1 q_2$ avec q_1, q_2 non-inversibles dans A avec $(q_1, a) = (q_2, a) = 1$. Ainsi $q/a^n = (q_1)(q_2/a^n)$ une décomposition en produit d'éléments non-inversibles par le paragraphe précédent.

Soit maintenant $x/a^n \in A[1/a]$ avec $x \in A$ et $n \in \mathbb{N}$. Alors on doit montrer l'existence et l'unicité d'une décomposition en irréductibles. Comme a est inversible il suffit de le monter pour x. Soit $x = q_1 \cdots q_s$ une décomposition dans A avce q_i irréductibles. Comme les $p_1, \ldots, p_r$ sont inversibles dans $A[1/a]$ on peut supposer qu'ils n'apparaissent pas dans la décomposition de x (quitte à multiplier par leur inverses dans $A[1/a]$). Le paragraphe précédent montre désormais que cet élément admet une décomposition en irréductibles dans $A[1/a]$.

Pour l'unicité: supposons maintenant qu'on ait

$$uq_1/a^{n_1} \cdots q_r/a^{n_r} = t_1/a^{m_1} \cdots t_s/a^{m_s}$$

des décompositions en irréductibles avec $(q_i, a) = (t_j, a) = 1$ pour tout i, j et les $q_i, t_j \in A$ irréductibles – on utilise pour cela la dernière remarque du paragraphe précédent. Ici u est inversible de $A[1/a]$. Comme en dessus, si on écrit $u = f/a^n$ pour $f \in A$ et $n \in \mathbb{N}$. Alors f est inversible dans $A[1/a]$ cela implique qu'il existe $m \in \mathbb{N}$ et $g \in A$ avec $fg = a^m$ dans A. Alors les facteurs irréductibles de f sont forcément communs à ceux de A.

On voit qu'en multipliant par a^M pour M suffisamment grand, on peut utiliser l'unicité des décompositions dans A: en effet on a $(a, q_i) = (a, t_j) = (f, q_i) = (f, t_j) = 1$ pour tout i, j.

Exercice 4.
Soient $a, b \in \mathbb{Z}$.

1. Quand est-ce que les corps $\mathbb{Q}(\sqrt{a})$ et $\mathbb{Q}(\sqrt{b})$ sont isomorphes en tant que $\mathbb{Q}$-espaces vectoriels?
2. Quand est-ce que les corps $\mathbb{Q}(\sqrt{a})$ et $\mathbb{Q}(\sqrt{b})$ sont isomorphes en tant que corps?

Solution.

1. There are two options for $\mathbb{Q}(\sqrt{a})$. If a is a square in $\mathbb{Q}$, then it holds that $\sqrt{a}$ is contained in $\mathbb{Q}$, and hence $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}$, and so $[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 1$. If a is no square, then $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{a})$, and the degree of this field extension is equal to 2, since the polynomial $x^2 - a$ is zero for $\sqrt{a}$, and the polynomial is irreducible (since a is no square). The same holds for $\mathbb{Q}(\sqrt{b})$. We now use the fact (seen in Linear Algebra) that any two vector spaces over the same field are isomorphic if and only if they are of the same dimension. In our case, both $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ can be of dimension 1 or 2 over $\mathbb{Q}$, depending on whether or not a resp. b is a square. We conclude that $\mathbb{Q}(\sqrt{a})$ is of the same dimension over $\mathbb{Q}$ as $\mathbb{Q}(\sqrt{b})$, and hence isomorphic, if and only if both a and b are simultaneously squares in $\mathbb{Q}$, or both are simultaneously not squares.

2. We now assume that $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ are isomorphic as fields. We claim that this holds if and only if they are equal as subfields of $\mathbb{C}$. This means that there exists $c \in \mathbb{Q}$ such that $\sqrt{a} = c\sqrt{b}$.

   First, we assume that $\sqrt{a} = c\sqrt{b}$. Then, $\sqrt{a}$ and $\sqrt{b}$ generate the same field extension of $\mathbb{Q}$, and hence clearly the two fields are isomorphic.

   Secondly, assume that the fields $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ are isomorphic. Denote the isomorphism $\varphi : \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}(\sqrt{b})$. We note that from $\varphi(1) = 1$, it follows that φ acts as the identity on $\mathbb{Z}$,

and furthermore on $\mathbb{Q}$. On one hand, we have that $\varphi(\sqrt{a}) = u + \sqrt{b}v$ for some $u, v \in \mathbb{Q}$. On the other hand, with $a \in \mathbb{Q}$, it holds that

$$a = \varphi(a) = \varphi(\sqrt{a}^2) = \varphi(\sqrt{a})^2 = (u + \sqrt{b}v)^2 = (u^2 + bv^2) + \sqrt{b}(2uv).$$

We now distinguish between two cases.

- If $\sqrt{b} \in \mathbb{Q}$, then $\varphi(\sqrt{a}) \in \mathbb{Q}$, and hence $\sqrt{a} \in \mathbb{Q}$. (If $\sqrt{a}$ was not contained in $\mathbb{Q}$, then φ would be an isomorphism from $\mathbb{Q}(\sqrt{a}) \neq \mathbb{Q}$ to $\mathbb{Q}$. This is a contradiction to φ being injective.) Then,

  $$\sqrt{a} = \frac{\sqrt{a}}{\sqrt{b}} \cdot \sqrt{b},$$

  and $\sqrt{a} = c\sqrt{b}$ with $c := \frac{\sqrt{a}}{\sqrt{b}} \in \mathbb{Q}$.

- If $\sqrt{b} \notin \mathbb{Q}$, then

  $$a = (u^2 + bv^2) + \sqrt{b}(2uv),$$

  with $\sqrt{b} \notin \mathbb{Q}$. Since $a \in \mathbb{Q}$, it follows that $2uv = 0$, and hence either $u = 0$ or $v = 0$. If $u = 0$, then $a = bv^2 \Rightarrow \sqrt{a} = \sqrt{b}v$, and hence the property is satisfied. If $v = 0$, then $\varphi(\sqrt{a}) = u \in \mathbb{Q}$. It then follows that the image of φ is contained in $\mathbb{Q}$, which means that φ can not be an isomorphism. Hence this case does not occur.