Some facts from the arithmetics of polynomials:

Roots and reducibility: *If K is a field, $f(x) \in K[x]$ and $\deg f = 2$ or 3 then f is irreducible $\Leftrightarrow$ f has no root in K.*
It is not true for polynomials of higher degree!!

Rational root test: *If $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ ($a_n, a_0 \neq 0$) and $\frac{p}{q} \in \mathbb{Q}$ ($p, q \in \mathbb{Z}$, $\gcd(p,q) = 1$) is a root of f then $p \mid a_0$ and $q \mid a_n$.*

Gauss lemma: *If $f(x) \in \mathbb{Z}[x]$ is reducible in $\mathbb{Q}[x]$ then it can also be factored into a product of polynomials of smaller degree over $\mathbb{Z}[x]$.*

Schönemann–Eisenstein criterion: *Suppose that $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, and there exists a prime p such that p divides $a_{n-1}, \ldots, a_0$ but p does not divide a_n, and p^2 does not divide a_0 then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

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

a) $2x - 3$ *b)* $x^3 - 2x^2 + x + 1$ *c)* $x^4 + 4x + 3$
d) $x^5 + 2x - 6$ *e)* $x^4 + 4$ *f)* $x^4 - x^2 + 1$

Solution: a) $2x - 3$ is irreducible because its degree is 1.

b) Since the polynomial $f(x) = x^3 - 2x^2 + x + 1$ has degree 3, it is irreducible $\Leftrightarrow$ it has no rational root. According to the rational root test, the rational roots can only be ± 1, and $f(1) = 1$, $f(-1) = -3$, so f is irreducible.

c) It is easy to see that $f(-1) = 0$, so $f(x) = (x+1)g(x)$ for some $g(x)$, thus f is not irreducible.

d) $x^5 + 2x - 6$ satisfies the condition of the Schönemann–Eisenstein criterion with $p = 2$, thus the polynomial is irreducible.

e) This polynomial can be written as a difference of two complete squares, so it has a nontrivial factorization: $x^4 + 4 = (x^4 + 4x^2 + 4) - 4x^2 = (x^2 + 2)^2 - (2x)^2 = (x^2 - 2x + 2)(x^2 + 2x + 2)$, showing that $x^4 + 4$ is not irreducible.

f) $f(x) = x^4 - x^2 + 1$ has no rational root (by the rational root test we only need to check ± 1), but we still have to see if it cannot be the product of two irreducible polynomials of degree 2. If it can then by the Gauss lemma we may assume that the factors are from $\mathbb{Z}[x]$: $f(x) = g(x)h(x)$, where $g, h \in \mathbb{Z}[x]$, and $\deg g = \deg h = 2$. The product of the main coefficients is 1, so they can only be both 1 or both -1, and we may assume the former (otherwise we can multiply both polynomials by -1). Similarly, the constant terms can be both 1 or both -1. Finally, since the coefficient of x^3 in f is 0, the sum of the coefficients of x is g and h is 0. So there are two cases:

$$f(x) = (x^2 + ax + 1)(x^2 - ax + 1) \quad \text{or} \quad f(x) = (x^2 + ax - 1)(x^2 - ax - 1).$$

Comparing the coefficent of x^2 on the two sides of the equations, we get $-1 = 2 - a^2$, giving $a^2 = 3$, or in the second case, $-1 = -2 - a^2$, giving $a^2 = -1$, and neither of them has a solution for a in $\mathbb{Z}$. We got a contradiction, so $f(x)$ is irreducible.
(Actually, $x^4 - x^2 + 1$ is the cyclotomic polynomial $\Phi_{12}(x)$, and it is known that all cyclotomic polynomials are irreducible in $\mathbb{Q}[x]$.)

2. *Determine the cardinality of the factor ring $K[x]/(x^2 + x + 1)$ if $K = \mathbb{Z}_2$ or $\mathbb{Z}_3$. Which of the two factor rings is a field?*

Solution: In both cases the polynomials of degree less than 2 form a complete representative set for the cosets of the ideal $(x^2 + x + 1)$, so the cardinality of the factor ring in the

case $K = \mathbb{Z}_2$ is $2^2 = 4$, in the case $K = \mathbb{Z}_3$ is $3^2 = 9$. The polynomial $p(x) = x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$, because it has degree 2, and has no root in $\mathbb{Z}_2$ ($p(0) = p(1) = 1$) but it is reducible over $\mathbb{Z}_3$, since there $p(1) = 1 + 1 + 1 = 0$. So the first factor ring is a field, the second is not.

3. *Let $K = \mathbb{Z}_2$ and $p(x) = x^3 + x + 1$. Show that $R = K[x]/(p(x))$ is a field of 8 elements. Find all the roots of $x^3 + x^2 + 1$ in R.*

Solution: In the factor ring the polynomials of degree less than 3 form a complete representative set for the cosets, so $|R| = 2^3 = 8$. Furthermore, $p(x)$ is irreducible because it has degree 3, and it has no root in $\mathbb{Z}_2$. So R is a field.
Let $\alpha = x + (p(x)) \in R$. Then we know that $p(\alpha) = 0$, that is, $\alpha^3 = -\alpha - 1 = \alpha + 1$, and the elements of R can be written uniquely as polynomials of α over K of degree less than 3: $\gamma = a + b\alpha + c\alpha^2$. We have to find all $a, b, c \in \mathbb{Z}_2$ for which γ is a root of $f(x) = x^3 + x^2 + 1$. We simplify the expressions, using that $a^2 = a$ for every element $a \in \mathbb{Z}_2$, then that $(x + y)^2 = x^2 + y^2$ in a field of characteristic 2, and that $\alpha^3 = \alpha + 1$, consequently, $\alpha^4 = \alpha^2 + \alpha$.

$$\begin{aligned}
(a + b\alpha + c\alpha^2)^2 &= a + b\alpha^2 + c\alpha^4 = a + b\alpha^2 + c(\alpha^2 + \alpha) \\
&= a + c\alpha + (b + c)\alpha^2 \\
(a + b\alpha + c\alpha^2)^3 &= (a + c\alpha + (b + c)\alpha^2)(a + b\alpha + c\alpha^2) \\
&= a + (ac + ab)\alpha + (ab + bc)\alpha^2 + (b + c + bc)\alpha^3 + (c + bc)\alpha^4 \\
&= (a + b + c + bc) + (b + ac + ab)\alpha + (c + ab)\alpha^2 \\
0 = f(\gamma) &= (1 + b + c + bc) + (b + c + ac + ab)\alpha + (b + ab)\alpha^2 \\
&= (1 + b)(1 + c) + (b + c)(1 + a)\alpha + (b + ab)\alpha^2
\end{aligned}$$

If $b = 1$ then $a = 1$, and $c = 0, 1$, if $b = 0$ then $c = 1$ and $a = 1$.
So the roots are $1 + \alpha$, $1 + \alpha + \alpha^2$ and $1 + \alpha^2$.

4. *Let α be a root of the polynomial $p(x) = x^2 - x + 1 \in \mathbb{Q}[x]$ in $\mathbb{C}$.*

a) What is the dimension of $\mathbb{Q}[\alpha] = \{ f(\alpha) \mid f(x) \in \mathbb{Q}[x] \}$ as a vector space over $\mathbb{Q}$.
b) Prove that α^2 and α^5 are linearly dependent in this vector space.
c) Show that $\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/(p(x))$, and $\mathbb{Q}[\alpha]$ is the smallest subfield of $\mathbb{C}$ containing α, that is, $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.
d) Express $\frac{1}{\alpha^2 - 2\alpha}$ as a polynomial of α of the least possible degree.

Solution: a) The subspace V spanned by 1 and α is closed under multiplication by α ($1 \cdot \alpha = \alpha \in V$ and $\alpha \cdot \alpha = \alpha - 1 \in V$), so it contains all powers of α, thus also the whole $\mathbb{Q}[\alpha]$. On the other hand, 1 and α are independent, since $p(x)$ is an irreducible polynomial with α as a root, so $p(x)$ is the minimal polynomial of α. This gives that $\{ 1, \alpha \}$ is a basis of $\mathbb{Q}[\alpha]$, consequently the dimension of this vector space is 2.

b) $\alpha^2 = \alpha - 1$, $\alpha^3 = \alpha^2 - \alpha = (\alpha - 1) - \alpha = -1$, then $\alpha^5 = \alpha^3 \cdot \alpha^2 = -\alpha^2 (= -\alpha + 1)$, so α^5 is a scalar multiple of α^2.

c) $\mathbb{Q}[\alpha]$ is the image of the ring homomorphism $\varphi : \mathbb{Q}[x] \to \mathbb{C}$, $f(x) \mapsto f(\alpha)$, and $\operatorname{Ker}\varphi = \{ f(x) \mid f(\alpha) = 0 \} = (p(x))$, so $\mathbb{Q}[x]/(p(x)) = \mathbb{Q}[x]/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi = \mathbb{Q}[\alpha]$. Since $p(x)$ is irreducible, $\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/(p(x)$ is a field. It contains α, and it must be included in every field containing α, so $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.

d) By part a)and c), every element of $\mathbb{Q}(\alpha)$ can be uniquely written as $a + b\alpha$ ($a, b \in \mathbb{Q}$). $\alpha^2 - 2\alpha = \alpha - 1 - 2\alpha = -1 - \alpha$, so we want to find $a + b\alpha$ such that $1 = (-1 - \alpha)(a + b\alpha) =$

$-a-(a+b)\alpha-b\alpha^2=-a-(a+b)\alpha-b(\alpha-1)=(b-a)-(a+2b)\alpha$, which gives the system of equations $b-a=1$ and $a+2b=0$, so $b=\frac{1}{3}$, $a=-\frac{2}{3}$, and $\frac{1}{\alpha^2-2\alpha}=-\frac{2}{3}+\frac{1}{3}\alpha$.

5. *Prove that* $\mathbb{Q}[x]/(x^2-2)\cong\mathbb{Q}[x]/(x^2-2x-1)$.

Solution: Both x^2-2 and x^2-2x-1 are irreducible over $\mathbb{Q}$, so they are minimal polynomials for their roots in $\mathbb{C}$ over $\mathbb{Q}$. $\sqrt{2}$ is a root of x^2-2, $1+\sqrt{2}$ is a root of x^2-2x-1, so $\mathbb{Q}[x]/(x^2-2)\cong\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}[x]/(x^2-2x-1)\cong\mathbb{Q}(1+\sqrt{2})$. But the latter two fields are actually equal: $\sqrt{2}=(1+\sqrt{2})-1\in\mathbb{Q}(1+\sqrt{2})$, and $1+\sqrt{2}\in\mathbb{Q}(\sqrt{2})$, hence $\mathbb{Q}[x]/(x^2-2)\cong\mathbb{Q}[x]/(x^2-2x-1)$.
(Alternatively, we may notice that $x^2-2x+1=(x-1)^2-2=p(x-1)$ for $p(x)=x^2-2$, so the (bijective) homomorphism $\varphi:\mathbb{Q}[x]\to\mathbb{Q}[x]$, $f(x)\mapsto f(x-1)$ maps the ideal $(p(x))$ to (x^2-2x-1). This implies that the composition of φ with the natural factoring homomorphism: $\mathbb{Q}[x]\xrightarrow{\varphi}\mathbb{Q}[x]\to\mathbb{Q}[x]/(x^2-2x-1)$ has kernel $(p(x))$, and it is naturally surjective, so by the homomorphism theorem, $\mathbb{Q}[x]/(x^2-2)\cong\mathbb{Q}[x]/(x^2-2x-1)$.)

6. *What is the minimal polynomial of* $\sqrt{2}+\sqrt{3}$ *over* $\mathbb{Q}$ *and over* $\mathbb{Q}(\sqrt{6})$*?*

Solution: Let $\alpha=\sqrt{2}+\sqrt{3}$. Then $\alpha^2=5+2\sqrt{6}\Rightarrow(\alpha^2-5)^2=24\Rightarrow\alpha^4-10\alpha^2+1=0$, so α is a root of the polynomial x^4-10x^2+1. This polynomial is irreducible since on the one hand, it has no rational roots (it could only be ±1 but those are not roots), on the other hand, it cannot be the product of two integral polynomials of degree 2: such a product (where we can assume the main coefficients to be positive) can only be $(x^2+ax+1)(x^2+bx+1)$ or $(x^2+ax-1)(x^2+bx-1)$, but comparing the coefficients, we would get $a^2=12$ or $a^2=8$, and there is no such an integer a. Thus the minimal polynomial of $\alpha=\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ is x^4-10x^2+1.
We have seen that $\alpha^2=5+2\sqrt{6}$, that is, α is a root of the polynomial $x^2-5-2\sqrt{6}\in\mathbb{Q}(\sqrt{6})[x]$. It cannot be the root of a polynomial of smaller degree over $\mathbb{Q}(\sqrt{6})$ because then α would be in $\mathbb{Q}(\sqrt{6})$, and that is only a second degree extension of $\mathbb{Q}$ (with a root of x^2-6). So the minimal polynomial of α over $\mathbb{Q}(\sqrt{6})$ is $x^2-5-2\sqrt{6}$.

7. *Suppose that for some* $\alpha,\beta\in\mathbb{C}$*, the numbers* $\alpha+\beta$ *and* $\alpha\beta$ *are algebraic over* $\mathbb{Q}$*. Prove that* α *and* β *are also algebraic.*

Solution: Let $c=\alpha+\beta$ and $d=\alpha\beta$. We know that then α and β are the roots of the polynomial $x^2-cx+d\in\mathbb{Q}(c,d)[x]$, so $\mathbb{Q}(c,d,\alpha)=\mathbb{Q}(c,d,\beta)=\mathbb{Q}(\alpha,\beta)$ has a finite degree over $\mathbb{Q}(c,d)$. But c is algebraic over $\mathbb{Q}$, and d algebraic over $\mathbb{Q}$, so it is also algebraic over $\mathbb{Q}(c)$, thus

$$(\mathbb{Q}(\alpha,\beta):\mathbb{Q})=(\mathbb{Q}(\alpha,\beta):\mathbb{Q}(c,d))\cdot(\mathbb{Q}(c,d):\mathbb{Q}(c))\cdot(\mathbb{Q}(c):\mathbb{Q})$$

is finite, so every element of $\mathbb{Q}(\alpha,\beta)$, in particular, α and β are algebraic over $\mathbb{Q}$.

8. *Let* $\alpha\in\mathbb{C}$ *be a root of the polynomial* $x^3-2x^2+x+1\in\mathbb{Q}[x]$*. Express the reciprocal of* α^2+2 *as an at most second degree polynomial of* α*.*

Solution: We want to find those rational coefficients $A,B,C\in\mathbb{Q}$ for which $(A\alpha^2+B\alpha+C)(\alpha^2+2)=1$, that is,

$$A\alpha^4+B\alpha^3+(2A+C)\alpha^2+2B\alpha+2C=1.$$

We use that $\alpha^3-2\alpha^2+\alpha+1=0$, that is,

$$\begin{aligned}\alpha^3=&2\alpha^2-\alpha-1\text{ and}\\ \alpha^4=&2\alpha^3-\alpha^2-\alpha=2(2\alpha^2-\alpha-1)-\alpha^2-\alpha=\\ =&3\alpha^2-3\alpha-2.\end{aligned}$$

$$(5A+2B+C)\alpha^2+(-3A+B)\alpha+(-2A-B+2C)=1.$$

Solving the linear system of equations, $5A+2B+C=0$, $-3A+B=0$, $-2A-B+2C=1$, we get $A=-\frac{1}{27}$, $B=-\frac{3}{27}$, $C=\frac{11}{27}$, so $\dfrac{1}{\alpha^2+2}=\dfrac{1}{27}(-\alpha^2-3\alpha+11)$.

9. *What are the degrees of the extensions $\mathbb{Q}(i\sqrt{3})$ and $\mathbb{Q}(i+\sqrt{3})$ over $\mathbb{Q}$?*

Solution: The minimal polynomial of $i\sqrt{3}$ is x^2+3, because $i\sqrt{3}$ is a root of this polynomial, and the polynomial is clearly irreducible over $\mathbb{Q}$. So $(\mathbb{Q}(i\sqrt{3}):\mathbb{Q})=2$

Let $\alpha=i+\sqrt{3}$. Then $(\alpha-\sqrt{3})^2=-1\Rightarrow\alpha^2-2\sqrt{3}\alpha+4=0\Rightarrow\sqrt{3}=\frac{\alpha^2+4}{2\alpha}\in\mathbb{Q}(\alpha)$, and $i=\alpha-\sqrt{3}\in\mathbb{Q}(\alpha)$, so $\mathbb{Q}(\sqrt{3},i)\le\mathbb{Q}(i+\sqrt{3})\le\mathbb{Q}(\sqrt{3},i)$, that is, $\mathbb{Q}\le\mathbb{Q}(\sqrt{3})\le\mathbb{Q}(\sqrt{3},i)=\mathbb{Q}(\alpha)$, where the degree of the first extension is 2 (with minimal polynomial x^2-3), and the second cannot have degree 1, since $\mathbb{Q}(\sqrt{3})\le\mathbb{R}$, but $\mathbb{Q}(\alpha)\not\le\mathbb{R}$. On the other hand, i is a root of the polynomial $x^2+1\in\mathbb{Q}[x]\le\mathbb{Q}(\sqrt{3})[x]$, so the second extension also has degree 2. Hence by the multiplicativiy theorem, $(\mathbb{Q}(\alpha):\mathbb{Q})=2\cdot2=4$.

10. *Determine the degrees of the following extensions over $\mathbb{Q}$.*

a) $\mathbb{Q}(\sqrt{2})$ *b)* $\mathbb{Q}(\sqrt[3]{2})$ *c)* $\mathbb{Q}(\sqrt[3]{2}+\sqrt[3]{4})$ *d)* $\mathbb{Q}(\sqrt[3]{2}+\sqrt{2})$

Solution: a) The minimal polynomial of $\sqrt{2}$ is $x^2-2\Rightarrow(\mathbb{Q}(\sqrt{2}):\mathbb{Q})=2$.

b) $\sqrt[3]{2}$ is a root of the polynomial x^3-2, which is irreducible (for example, by the Schönemann–Eisenstein criterion), so this is the minimal polynomial of $\sqrt[3]{2}$, and this gives $(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q})=3$.

c) $\alpha:=\sqrt[3]{2}+\sqrt[3]{4}=\sqrt[3]{2}+(\sqrt[3]{2})^2\in\mathbb{Q}(\sqrt[3]{2})$, so $\mathbb{Q}\le\mathbb{Q}(\alpha)\le\mathbb{Q}(\sqrt[3]{2})$, and then

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

But $\sqrt[3]{2}$ is a root of the polynomial $x^2+x-\alpha\in\mathbb{Q}(\alpha)[x]$, hence $(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}(\alpha))\le2$, and this degree is a divisor of 3, so it can only be 1. It follows that $(\mathbb{Q}(\alpha):\mathbb{Q})=3$.

d) It is clear that for $\alpha=\sqrt[3]{2}+\sqrt{2}$ we have $\mathbb{Q}(\alpha)\le\mathbb{Q}(\sqrt[3]{2},\sqrt{2})$, on the other hand, $(\alpha-\sqrt{2})^3=2\Rightarrow\alpha^3-3\sqrt{2}\alpha^2+6\alpha-2\sqrt{2}=2\Rightarrow\sqrt{2}=\dfrac{\alpha^3+6\alpha-2}{3\alpha^2+2}\in\mathbb{Q}(\alpha)$, and $\sqrt[3]{2}=\alpha-\sqrt{2}\in\mathbb{Q}(\alpha)$, so $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$. The degree of the latter is at most $2\cdot3=6$, as can be seen from the extensions

$$\mathbb{Q}\le\mathbb{Q}(\sqrt{2})\le\mathbb{Q}(\sqrt{2},\sqrt[3]{2})=\mathbb{Q}(\alpha),$$

where the minimal polynomial of the first extension is x^2-2, while that of the second must be a divisor of x^3-2. However, if we consider the extensions

$$\mathbb{Q}\le\mathbb{Q}(\sqrt[3]{2})\le\mathbb{Q}(\alpha),$$

we see that $(\mathbb{Q}(\alpha):\mathbb{Q})$ is divisible both by 2 and 3, so it can only be 6.

11. *Let α be a root of the polynomial x^3+x+1 over $\mathbb{Z}_2$, and let $K=\mathbb{Z}_2(\alpha)$. Is the polynomial $x^2+x+\alpha$ irreducible over K?*

Solution: We only have to check if the polynomial $x^2+x+\alpha$ has a root in K, that is, if there is a polynomial $A\alpha^2+B\alpha+C$ with coefficients $A,B,C\in\mathbb{Z}_2$ for which

$$(A\alpha^2+B\alpha+C)^2+(A\alpha^2+B\alpha+C)+\alpha=0.$$

We can rewrite the equation, using that $A,B,C\in\{0,1\}$ implies $A^2=A$, $B^2=B$ s $C^2=C$, and $\alpha^3=\alpha+1$, implying also $\alpha^4=\alpha^2+\alpha$. We get that $A\alpha^4+(A+B)\alpha^2+(B+1)\alpha=0$, that is, $B\alpha^2+(A+B+1)\alpha=0$, so $A=1$, $B=0$ and C is arbitrary, hence α^2 and α^2+1 are roots of $x^2+x+\alpha$, showing that the polynomial is not irreducible.