Exercise 11

Discrete Mathematics

January 14, 2020

Exercise 101

Task description Let $p(x) = x^4 + 1$.

(a) Is $p(x)$ irreducible over $\mathbb{R}$? If yes, prove it. If no, find a way to write $p(x)$ as a product of two (non-constant) real polynomials.

(b) Is $p(x)$ reducible over $\mathbb{Q}$?

Solution: https://math.stackexchange.com/a/2096676 Even a short hint on Wikipedia

(a) $p(x)$ is reducible. $p(x) = (\underbrace{x^2 - x\sqrt{2} + 1}_{a(x)}) \cdot (\underbrace{x^2 + x\sqrt{2} + 1}_{b(x)})$ All coefficients are real.

(b) No.

Theorem Let F be a field. If $f(x) \in F[x]$ and $\deg f(x)$ is 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

$(\mathbb{R}, +, \cdot)$ is a field. $a(x)$ and $b(x)$ are of degree 2. Neither $a(x)$ nor $b(x)$ have roots in $\mathbb{R}$. Hence, they are irreducible.

We know from the lecture that $(K[x], +, \cdot)$ is a UFD (unique factorization domain, factorial ring) for any field K. For any UFD, the factorization into irreducibles is unique up to associates and the order in which the factors appear by definition.

Hence, the factorization $p(x) = a(x)b(x)$ from task (a) is unique. $a(x)b(x)$ also has $\sqrt{2} \notin \mathbb{Q}$ as coefficient. It follows from those two facts, that there can be no factorization with coefficients in $\mathbb{Q}$.

Exercise 102

Wikipedia

`https://www.physicsforums.com/threads/irreducible-polynomials-over-the-reals.474510/post-3147789`

https://math.stackexchange.com/a/275957

Task description Describe all real polynomials which are irreducible over $\mathbb{R}$.
The tools that you possibly need to use are:

(1) the fundamental theorem of algebra

(2) the fact that if a complex (non-real) number $z = a+bi$ is a root of a real polynomial $p(x)$, then its conjugate $\bar{z} = a - bi$ is a root of $p(x)$ as well.

Solution

By the Fundamental Theorem of Algebra any polynomial $p(x)$ of degree n has n values $z_i \in \mathbb{C}$ (some possibly degenerate) such that $p(z_i) = 0$. Such values are called polynomial roots. This means that $p(x)$ can be written as product of linear factors $p(x) = (x - z_1) \dots (x - z_n)$.

If $z_i \in \mathbb{C}$ is a complex solution of $p(x)$, then there is some $z_j = \overline{z_i}$ in the factorization which is also a solution by fact (2). Then the product $(x - z_i)(x - z_j) \in \mathbb{R}$ is real and a quadratic polynomial. It follows that $p(x)$ can be written as a product linear and quadratic terms. This implies that the only possible irrreducible polynomials are linear or quadratic.

Exercise 103

Task description Let I be the following ideal of $\mathbb{Z} : I = \langle 9, 12\rangle$ (that is, I is the ideal generated by the elements 9 and 12). Show that I is a principal ideal (that is, I can be generated by a single element). Generalize for $I = \langle a, b\rangle$ for any $a, b \in \mathbb{Z}$.

Solution Consider (like in exercise 100) the definition from Joseph A. Gallian's book Abstract Algebra (note that Prof. Drmota uses (m) for "generated by m" and the book uses $\langle m\rangle$):

> **Definition** Let R be a commutative ring with unity and let $a_1, a_2, \dots, a_n$

belong to R. Then $I = \langle a_1, a_2, \dots, a_n \rangle = \{r_1 a_1 + r_2 a_2 + \dots + r_n a_n \mid r_i \in R\}$ is an ideal of R called the ideal generated by $a_1, a_2, \dots, a_n$.

So we get

$$\begin{aligned}\langle 9, 12 \rangle &= \{r_1 \cdot 9 + r_2 \cdot 12 \mid r_1, r_2 \in \mathbb{Z}\} \\ &= \{\dots, 1 \cdot 9 + (-1) \cdot 12, 0 \cdot 9 + 0 \cdot 12, (-1) \cdot 9 + 1 \cdot 12, (-2) \cdot 9 + 2 \cdot 12 \dots\} \\ &= \{\dots, -3, 0, 3, 6 \dots\}\end{aligned}$$

This of course coincides with the definition from the lecture:

> **Definition** If R is an Euclidean ring and $M = \{m_1, m_2, \dots, m_n\}$ consists of a finite number of elements, then the ideal that is generated by M is the principal ideal
>
> $$(M) = (\gcd(m_1, m_2, \dots, m_n)) = \gcd(m_1, m_2, \dots, m_n) \cdot R.$$

of which we also learned that it is principal. So for $M = \{3, 9\}$ we get $\langle 3, 9 \rangle = \gcd(3, 9) \cdot \mathbb{Z} = 3 \cdot \mathbb{Z}$.

We know one very important theorem from the lecture:

> **Theorem** If R is an Euclidean ring then all ideals are principal. More formally, if J is an ideal of R then $\exists r \in R : J = \langle r \rangle = mR$.

and it was exactly the example from the lecture that the integers $\mathbb{Z}$ are a ring and that if J is an ideal of $\mathbb{Z}$ then J has the form $J = m\mathbb{Z}$.

Consequently, it does not matter which $a, b \in \mathbb{Z}$ are chosen, as long as I is an ideal, I will be a principal ideal.

Proof of the theorem Suppose that J is an ideal of R.

Case 1 Then $J = \{0\} = (0) = 0 \cdot R$ is a principal ideal.

Case 2 $\exists a \in J \setminus \{0\}$. Then we have the euclidean evaluation $n(a)$. Consider an element $a_0 \in J \setminus \{0\}$ such that $n(a_0) = \min\{n(A) \mid a \in J \setminus \{0\}\}$. Note that in general $n(a)$ is only defined for non-zero elements. Also note that all $n(a)$ are natural numbers. It is known that every non-empty set of natural numbers has a minimal element. So a_0 can actually be found. Take now some element $b \in J$ then there exist $q, r \in R : b = q \cdot a_0 + r$ with $r = 0$ or $n(r) < n(a_0)$because we're in an euclidean ring and a_0 was chosen to be non-zero. If $r = 0$ then b is just a multiple of a_0. It holds $b = q \cdot a_0$. If $r \neq 0$ then certainly $r = b - q \cdot a_0$ is in J because $b, a_0 \in J$. But now $n(r) < n(a_0)$ which is a contradiction to our definition of a_0. Consequently, $r = 0$ is the only case that occurs. So finally, $J = a_0 \cdot R = (a_0)$.

Exercise 104

See StackExchange and also

- StackExchange
- StackExchange
- StackExchange
- StackExchange

Task description Let I be the following ideal of $(Z[x], +, \cdot) : I = \langle x, 2\rangle$. Show that I is not a principal ideal.

Solution

> **Definition** Let R be a commutative ring with unity and let $a_1, a_2, \ldots, a_n$ belong to R. Then $I = \langle a_1, a_2, \ldots, a_n\rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R\}$ is an ideal of R called the ideal generated by $a_1, a_2, \ldots, a_n$.

Therefore, if we define all constants a_i, b_i for x of too high degree to be 0, we get

$$\begin{aligned}\langle x, 2\rangle &= \{xf(x) + 2g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}\\ &= a_nx^{n+1} + a_{n-1}x^n + \cdots + a_1x^2 + a_0x + 2b_mx^m + 2b_{m-1}x^{m-1} + \cdots + 2b_1x + 2b_0\\ &= c_kx^k + c_{k-1}x^{k-1} + \cdots + \underbrace{(a_0 + 2b_1)}_{c_1}x + 2b_0\end{aligned}$$

where $c_i = a_{i-1} + 2b_i$ for $1 \leq i \leq k = \max(n+1, m)$. For example, for $n = m$ we get the terms $c_{k-1}x^{k-1} = (a_{n-1} + 2b_m)\,x^{k-1}$ and $c_kx^k = (a_n + 2b_{m+1})\,x^k$ with $b_{m+1} = 0$.

Observation $\langle x, 2\rangle$ is all polynomials with even (or zero) constant term.

This can be checked by taking such a polynomial $d_jx^j + d_{j-1}x^{j-1} + \cdots + d_1x + 2d_0$ and transforming it to

$$x\underbrace{\left(d_jx^{j-1} + d_{j-1}x^{j-2} + \cdots + d_1\right)}_{f(x)} + 2\underbrace{d_0}_{g(x)}$$

and we see that this is of the form $\{xf(x) + 2g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$ and hence in the ideal.

> **Definition** Let R be a commutative ring with unity and let $a \in R$. The set $\langle a \rangle = \{ra \mid r \in R\}$ is an ideal of R called the principal ideal generated by a.

> **Definition** A subring A of a ring R is called a (two-sided) ideal of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A.

Now suppose for a contradiction that I is generated by a single polynomial $h(x)$, that is $I = \langle x, 2 \rangle = \langle h(x) \rangle$ for some $h(x) \in I$.

Case 1 $h(x) = c \in I$ is a constant polynomial. Then it is even by our previous observation. Then

$$\langle c \rangle = \{cf(x) \mid f(x) \in \mathbb{Z}[x]\} .$$

Consequently the ideal contains only polynomials with even coefficients and we do not get x alone.

Case 2 $h(x)$ is not a constant polynomial. Then it has degree at least 1. Then non-zero polynomials in $\langle h(x) \rangle = \{h(x)f(x) \mid f(x) \in \mathbb{Z}[x]\}$ have degree at least 1. Examples are

- $\underbrace{(b_1 x + b_0)}_{h(x)} a_0$
- and $\underbrace{(b_2 x^2 + b_1 x + b_0)}_{h(x)}(a_1 x + a_0)$
- but not $\underbrace{b_0}_{h(x)}(a_1 x + a_0)$ or $\underbrace{b_0}_{h(x)} \cdot a_0$

So here we do not get the constant 2 alone.

As a consequence, I is not of the form $\langle h(x) \rangle$, so I is not principal.

Exercise 105

Task description Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

(a) Determine the invertible elements of $\mathbb{Z}[i]$.

(b) Is $\mathbb{Z}[i]$ an integral domain?

Solution

(a) **Definition** A unity (or identity) in a ring is a nonzero element that is an identity under multiplication. It need not exist.

Definition A nonzero element of a commutative ring with unity need not have a multiplicate inverse. When it does, it is called a unit (or multiplicatively invertible) of the ring. Thus, a is a unit if a^{-1} exists. The set of units is

$$R^* = \{a \in R : \exists b \in R : a \cdot b = 1\}$$

and $(R^*, \cdot)$ is a commutative group.

Wikipedia Note that 1 is the unity (identity) of $\mathbb{Z}[i]$. The units of $\mathbb{Z}[i]$ are precisely the Gaussian integers with norm 1, that is, 1, -1, i and $-i$, because

$$\begin{aligned} 1 \cdot 1 &= 1 & \qquad i \cdot (-i) &= 1 \\ (-1) \cdot (-1) &= 1 & \qquad (-i) \cdot i &= 1 \end{aligned}$$

(b) **Definition** A ring R is a set with two binary operations $+$ and $-$ such that for all $a, b, c \in R$ holds

1. $a + b = b + a$
2. $(a + b) + c = a + (b + c)$
3. There is an additive identity 0. That is, there is an element 0 in R s.t. $a + 0 = a \forall a \in R$.
4. There is $-a$ in R s.t. $a + (-a) = 0$
5. $a(bc) = (ab)c$
6. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

> A ring is an Abelian group under addition, also having an associative multiplication that is left and right distributive over addition.
>
> **Definition** A zero-divisor is a nonzero element of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.
>
> **Definition** An integral domain is a commutative ring with unity and no zero-divisors.

Note that where the ring definition is quoted from [1] , the closure property of Abelian group is not mentioned. But it was not mentioned in the ring definition in the lecture either. Nevertheless, here it is for $\mathbb{Z}[i]$:

Using the identity $i^2 = -1$ we get

$$\begin{aligned}(a + bi) + (c + di) &= (a + c) + (b + d)i \\ (a + bi) \cdot (c + di) &= (ac - bd) + (ad + bc)i\end{aligned}$$

so if $(a + bi) \in \mathbb{Z}[i]$ and $(c + di) \in \mathbb{Z}[i]$ then their sum and product are also in $\mathbb{Z}[i]$.

In the lecture the conclusion that $\mathbb{Z}$ is an integral domain followed directly here.

Note that $\mathbb{Z}$ is an integral domain. So the remaining properties follow directly. For example, associativity over multiplication

$$\begin{aligned}((a + bi)(c + di))\,(e + fi) &= (ac + adi + bci + bdi^2)(e + fi) \\ &= ace + acfi + adei + adfi^2 + bcei + bcfi^2 + bdei^2 + bdfi^3 \\ &= (a + bi)\left((cd + cfi + dei + dfi^2)\right) \\ &= (a + bi)\,((c + di)(e + fi))\end{aligned}$$

Consequently, this is an integral domain.

[1] Gallian, Abstract Algebra

Exercise 106

Task description Show that the set $S = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ with the usual addition and multiplication is a field. Compute $(3 - 5\sqrt{2})^{-1}$.

Solution

> **Definition** A unity (or identity) in a ring is a nonzero element that is an identity under multiplication. It need not exist.
>
> **Definition** A nonzero element of a commutative ring with unity need not have a multiplicate inverse. When it does, it is called a unit of the ring. Thus, a is a unit if a^{-1} exists.
>
> **Definition** A field is a commutative ring with unity in which every nonzero element is a unit.

S is certainly a substructure of the real numbers $S \subseteq \mathbb{R}$. Consequently all properties like the associative law and the distributive law are certainly satisfied. We only have to show that if $a + b\sqrt{2} \neq 0$ then there exists an element of this form that is the reciprocal of that.

First of all,

$$a + b\sqrt{2} \neq 0 \Leftrightarrow (a, b) \neq (0, 0) \tag{1}$$

(a and b are not both 0). Proof:

$\Rightarrow$ If $a + b\sqrt{2} \neq 0$ then one of a or b has to be non-zero. Otherwise $0 + 0\sqrt{2} = 0$.

$\Leftarrow$ Suppose not both a and b are 0. Suppose that $a + b\sqrt{2} = 0$. Then $b \neq 0$ because if b were 0 then a would be 0, too. Consequently, $\sqrt{2} = -\frac{a}{b} \in \mathbb{Q}$ which is impossible because it is known that $\sqrt{2} \notin \mathbb{Q}$. Contradiction. It follows $a + b\sqrt{2} \neq 0$.

Secondly, we have to check that there is an inverse (reciprocal) element of this form. To do so, consider $\frac{1}{a+b\sqrt{2}}$ where we multiply numerator and denominator by $a - b\sqrt{2}$

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \underbrace{\frac{a}{a^2 - 2b^2}}_{\in\mathbb{Q}} - \underbrace{\frac{b}{a^2 - 2b^2}}_{\in\mathbb{Q}} \sqrt{2} \tag{2}$$

Note that we can replace b by $-b$ in both sides of equation 1. From this follows that if $(a, b) \neq (0, 0)$ then $a - b\sqrt{2} \neq 0$. As a consequence $(a + b\sqrt{2})(a - b\sqrt{2})$ in equation 2 is a product of two non-zero numbers. Then $a^2 - 2b^2 \neq 0$.

So finally $(S, +, \cdot)$ is a field.

Using equation 2 we get

$$(3 - 5\sqrt{2})^{-1} = \frac{1}{3 - 5\sqrt{2}} = \frac{3}{3^2 - 2 \cdot 5^2} - \frac{5}{3^2 - 2 \cdot 5^2} \cdot \sqrt{2} = \frac{3}{-41} - \frac{5}{-41} \cdot \sqrt{2}$$

Exercise 107

Some interesting definitions **Task description** Determine whether the set $T = \{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbb{Q}\}$ with the usual addition and multiplication is a field. If yes, prove it. If not, describe the smallest field (a subfield of $\mathbb{R}$) that contains T.

Solution

> **Definition** A field is a commutative ring with unity in which every nonzero element is a unit.

Nice hint

For the sake of a contradiction, suppose T is a field. Let

- $a, c = 0$ and $b = 1$ to get $\sqrt{2} \in T$
- $a, b = 0$ and $c = 1$ to get $\sqrt{3} \in T$

Then$\sqrt{2} \cdot \sqrt{3} \in T$. However, $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$ is an irrational number. So there is no way to set $a, b, c \in \mathbb{Q}$ such that $\sqrt{6}$ is in T. Consequently, T is not closed under multiplication. Hence T is **not** a field.

By multiplying two arbitrary elements of T and using $\sqrt{2}^2 = 2$ and $\sqrt{3}^2 = 3$

$$\begin{aligned}&(a_1 + b_1\sqrt{2} + c_1\sqrt{3})(a_2 + b_2\sqrt{2} + c_2\sqrt{3})\\ =&\underbrace{a_1a_2 + 2b_1b_2 + 3c_1c_2}_{u\in\mathbb{Q}} + \underbrace{(a_1b_1 + a_2b_1)}_{v\in\mathbb{Q}}\sqrt{2} + \underbrace{(a_1c_1 + a_2c_1)}_{w\in\mathbb{Q}}\sqrt{3} + \underbrace{(b_1c_2 + b_2c_1)}_{x\in\mathbb{Q}}\sqrt{6}\end{aligned}$$

we get a term of the form $u + v\sqrt{2} + w\sqrt{3} + x\sqrt{6}$.

By multiplying two arbitrary elements of that new form and using the identity $\sqrt{6} = \sqrt{2}\sqrt{3}$

$$\begin{aligned}&(a_1 + b_1\sqrt{2} + c_1\sqrt{3} + d_1\sqrt{6})(a_2 + b_2\sqrt{2} + c_2\sqrt{3} + d_2\sqrt{6})\\ =&a_1a_2 + 2b_1b_2 + 3c_1c_2 + 6d_1d_2 + (a_1b_2 + b_1a_2 + 3c_1d_2 + 3d_1c_2)\sqrt{2}+\\ &(a_1c_3 + 2b_1d_2 + c_1a_2 + 2d_1b_2)\sqrt{3} + (a_1d_2 + b_1c_2 + c_1b_2 + d_1a_1)\sqrt{6}\end{aligned}$$

we get a term of the new form again. This means that, in contrast to the first one, the new form is closed under multiplication.

- StackExchange

- StackExchange

In fact, we can show that $T' = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.

> **Definition (Subfield test)** Let F be a field and let K be a subset of F with at least two elements. K is a subfield of F if, for any $a, b (b \neq 0)$ in K, $a - b$ and ab^{-1} belong to K.

First of all,

$$\begin{aligned}&(a_1 + b_1\sqrt{2} + c_1\sqrt{3} + d_1\sqrt{6}) - (a_2 + b_2\sqrt{2} + c_2\sqrt{3} + d_2\sqrt{6})\\ =&(a_1 - a_2) + (b_1 - b_2)\sqrt{2} + (c_1 - c_2)\sqrt{3} + (d_1 - d_2)\sqrt{6}\end{aligned}$$

is in T'. It is sufficient to show that the reciprocal exists. It does not have to be given explicitly.

$$\frac{1}{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}} = \frac{1}{(a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3}} = \frac{(a + b\sqrt{2}) - (c + d\sqrt{2})\sqrt{3}}{(a + b\sqrt{2})^2 - 3(c + d\sqrt{2})^2}$$

The numerator is of the form $a+b\sqrt{3}$ and (by multiplication of) $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$. In other words terms of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ can be arranged into elements of the form $a + b\sqrt{3}$. By multiplication we see that the denominator is of the form $a + b\sqrt{2}$. We already found the reciprocal of $a + b\sqrt{2}$ in the previous exercise.

Exercise 109

It would have been smart to multiply with complex conjugates, apparently

Task description Determine the minimal polynomial of $\sqrt{3}+i$

(a) over $\mathbb{Q}$

(b) over $\mathbb{R}$

(c) over $\mathbb{C}$

Solution

> **Definition** If a is algebraic over a field F, then there is a unique monic irreducible polynomial $p(x)$ in $F[x]$ such that $p(a) = 0$. Such a polynomial is called the minimal polynomial for a over F.
>
> **Definition** $K \subseteq L$ field, $\alpha \in L$ algebraic over K. $M(x) \in K[x] \setminus \{0\}$ is a minimal polynomial of α if
>
> 1. $M(\alpha) = 0$
> 2. $\deg M(x)$ minimal with this property
> 3. $M(x)$ monic (leading coefficient 1)

Let $a = \sqrt{3}+i$. For $p(x) = x$ we get $p(a) = \sqrt{3}+i$. Using $-a$ directly gives

$$p(x) = x - a = x - (\sqrt{3}+i)$$

and then $p(a) = a - a = 0$. Any minimal polynomial must have $\deg p(x)$ at least 1 because otherwise we cannot calculate $p(a)$, so as $\deg p(x) = 1$ it is minimal. Also the coefficients 1 and $\sqrt{3}+i$ are complex, so this is the minimal polynomial over $\mathbb{C}$.

We continue with this polynomial by using the property $i^2 = -1$ and calculating squares to eliminate i.

$$\begin{aligned} p(x) = 0 &= x - \left(\sqrt{3}+i\right) \\ x - \sqrt{3} &= i \\ i^2 &= x^2 - 2x\sqrt{3} + 3 \\ p(x) = 0 &= x^2 - 2x\sqrt{3} + 4 \end{aligned}$$

and verify that $p(a) = 0$. It is minimal because without using x^2 to get $i^2 = -1$ we cannot remove the imaginary part.

> **Theorem** (Reducibility Test for Degrees 2 and 3) Let F be a field. If $f(x) \in F[x]$ and $\deg f(x)$ is 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

The roots of the new $p(x)$ are $\sqrt{3} \pm i$, so they are not in $\mathbb{R}$. Consequently $p(x)$ is irreducible over $\mathbb{R}$. The coefficient $2\sqrt{3}$ is in $\mathbb{R}$ but not $\mathbb{Q}$. The remaining coefficients are also in $\mathbb{R}$. So $x^2 - 2x\sqrt{3} + 4$ is our minimal polynomial over $\mathbb{R}$.

We continue by squaring again to eliminate $\sqrt{3}$.

$$\begin{aligned} 0 &= x^2 - 2x\sqrt{3} + 4 \\ 4x^2 \cdot 3 &= (x^2+4)^2 = x^4 + 8x^2 + 16 \\ 0 &= x^4 + 8x^2 - 12x^2 + 16 \\ p(x) = 0 &= x^4 - 4x^2 + 16 \end{aligned} \tag{3}$$

and verify that $p(a) = 0$. There must be a second square operation because the root and the i are connected by $+$. Hence, $p(x)$ is minimal.

We verify that $x^4 - 4x^2 + 16$ is irreducible. The associated quadratic polynomial $x^2 - 4x + 16$ has roots $2 \pm 2i\sqrt{3} \in \mathbb{C}$. So by the reducibility test there is no root in the real numbers. We can use the previous identity 3 of $p(x)$ and $(a-b)(a+b) = a^2 - b^2$ to get a factorization with real number coefficients

$$\begin{aligned} x^4 - 4x^2 + 16 &= \left(x^2+4\right)^2 - 12x^2 \\ &= \left(x^2+4\right)^2 - \left(\sqrt{12}x\right)^2 \\ &= \left(x^2 - \sqrt{12}x + 4\right)\left(x^2 + \sqrt{12}x + 4\right) \end{aligned}$$

The roots of the quadratic equations are $\sqrt{3} \pm i \in \mathbb{C}$ and $-\sqrt{3} \pm i \in \mathbb{C}$. As no root is a real number, $x^4 - 4x^2 + 16$ consists of two polynomials over the real numbers that are irreducible over the real numbers by the reducibility test. If $x^4 - 4x^2 + 16$ were reducible over the rational numbers, the two factorizations in $\mathbb{Q}[x]$ and $\mathbb{R}[x]$ would coincide. Hence, $x^4 - 4x^2 + 16$ is irreducible over the rational numbers and our minimal polynomial over $\mathbb{Q}$.

Exercise 110

Here also apparently multiplying the conjugates is sufficient for the polynomial **Task description** Same question as exercise 109 but for $\sqrt{2}+\sqrt{3}$.

Solution Let $a=\sqrt{2}+\sqrt{3}$. For $p(x)=x$ we get $p(a)=\sqrt{2}+\sqrt{3}$. Using $-a$ directly gives

$$p(x)=x-a=x-\left(\sqrt{2}+\sqrt{3}\right)$$

and then $p(a)=a-a=0$. Any minimal polynomial must have $\deg p(x)$ at least 1 because otherwise we cannot calculate $p(a)$, so as $\deg p(x)=1$ it is minimal. Also the coefficients $\sqrt{2}$ and $\sqrt{3}$ are real numbers, so this is the minimal polynomial over $\mathbb{R}$. As the real numbers are a subset of the complex numbers, this is also the minimal polynomial over $\mathbb{C}$.

For the rational numbers we calculate

$$\begin{aligned}
0&=x-\left(\sqrt{2}+\sqrt{3}\right)\\
x&=\sqrt{2}+\sqrt{3}\\
x^2&=2+2\sqrt{2}\sqrt{3}+3\\
x^2-5&=2\sqrt{6}\\
x^4-2x^2\cdot 5+5^2&=4\cdot 6\\
p(x)=0&=x^4-10x^2+1
\end{aligned}$$

If I remember correctly, we did not do very much Galois theory or vector space things in the lecture. So a solution without much of it.

The zeros of $p(x)$ are $x_1=\sqrt{2}+\sqrt{3}$, $x_2=\sqrt{2}-\sqrt{3}$, $x_3=-\sqrt{2}+\sqrt{3}$ and $x_4=-\sqrt{2}-\sqrt{3}$. Therefore over the reals we have the factorization

$$p(x)=(x-x_1)(x-x_2)(x-x_3)(x-x_4).$$

It is not sufficient to check that none of the roots are rational, because $p(x)$ could still have quadratic factors with rational coefficients. If $p(x)=f(x)g(x)$ were a factorization as a product of two quadratics with rational coefficients, then x_1 must be a zero of one of the factors. Without loss of generality we can assume that $f(x_1)=0$. This means that the other zero of $f(x)$ must be either x_2, x_3 or x_4. But we can check that none of

$$
\begin{aligned}
(x-x_1)(x-x_2) &= (x-\sqrt{2})^2-(\sqrt{3})^2 = x^2-2\sqrt{2}x-1 \\
(x-x_1)(x-x_3) &= (x-\sqrt{3})^2-(\sqrt{2})^2 = x^2-2\sqrt{3}x+1 \\
(x-x_1)(x-x_4) &= x^2-(\sqrt{2}+\sqrt{3})^2 = x^2-5-2\sqrt{6}
\end{aligned}
$$

have rational coefficients. Therefore $p(x)$ has no quadratic factors with rational coefficients, and hence must be irreducible.

Mathonline

Irreducibility