Äärellisulotteinen lineaarialgebra, kevät 2015.
Harjoitus 10.

1. a) Käy läpi kaikki polynomialgebran $\mathbb{Z}_2[\mathbf{X}]$ 2- ja 3-asteiset polynomit ja esitä jokainen niistä (polynomialgebran $\mathbb{Z}_2[\mathbf{X}]$) jaottomien polynomien tulona.
   b) Anna esimerkki sellaisista polynomialgebran $\mathbb{Z}_2[\mathbf{X}]$ 4-asteisista polynomeista $\mathbf{p}_1, \mathbf{p}_2$, joille pätee seuraava.

   (i) Polynomilla $\mathbf{p}_1$ ei ole juuria kunnassa $\mathbb{Z}_2$, mutta se ei ole jaoton.

   (ii) Polynomi $\mathbf{p}_2$ on jaoton.

   c) Sama kuin b)-kohta, mutta 5-asteisille polynomeille.

   Ratkaisu: Kunnassa $\mathbb{Z}_2$ on vain kaksi alkiota, $0 = 0_2$ ja $1 = 1_2$, joten jokainen (nollasta eroava) polynomi $\mathbf{p} \in \mathbb{Z}_2[\mathbf{X}]$ on muotoa

   $$X^{n_1} + X^{n_2} + \ldots + X^{n_l}, \tag{1}$$

   missä $n_1 > n_2 > \ldots n_l \geq 0$ ja $n_1 = \deg \mathbf{p}$. Selvästi 0 on tämän polynomin juuri jos ja vain jos $n_l > 0$ (eli polynomi ei sisällä vakiotermiä). Polynomin (1) arvo toisessa kunnan alkiossa 1 on taas selvästi $l \cdot 1 = l_2$, mistä nähdään, että 1 on polynomin (1) juuri jos ja vain jos l on parillinen luku eli jos ja vain jos polynomi sisältää tasan parillisen määrän nollasta eroavia termejä.

   a) Käytetään hyväksi sitä, että 2-tai 3-asteinen polynomi on jaoton jos ja vain jos sillä on juuri. Tämä johtuu siitä, että ainoa tapa jakaa tällainen polynomi kahden ei-vakio polynomin tuloksi on kun ainakin yksi näistä polynomeista on 1-asteinen. Tämän avulla nähdään, että toisen asteen polynomit (jaettuna jaottomiin tekijöihin) ovat

   $$\mathbf{X}^2 = \mathbf{X}\mathbf{X}, \mathbf{X}^2 + \mathbf{X} = \mathbf{X}(\mathbf{X} + 1),$$
   $$\mathbf{X}^2 + 1 = (\mathbf{X} + 1)(\mathbf{X} + 1), \mathbf{X}^2 + \mathbf{X} + 1,$$

   missä viimeksi mainittu on ainoa jaoton 2-asteinen polynomi (koska sillä ei ole juuria $\mathbb{Z}_2$:ssä). Jako $\mathbf{X}^2 + 1 = (\mathbf{X} + 1)(\mathbf{X} + 1) = (\mathbf{X} + 1)^2$ voidaan helposti päätellä esimerkiksi siitä, että 1 on tämän polynomin juuri kun taas 0 ei ole. Edellinen fakta tarkoittaa sitä, että $\mathbf{X}^2 + 1 = (\mathbf{X} + 1)\mathbf{q}$, missä $\deg \mathbf{q} = 1$, jolloin polynomilla $\mathbf{q}$ täytyy olla juuri, joka on myös polynomin $\mathbf{X}^2 + 1$ juuri. Tällöin ainoaksi mahdollisuudeksi jää $\mathbf{q} = \mathbf{X} + 1$.

   Toinen, ehkä yksinkertaisempi, ainakin mekaanisempi tapa olisi käydä läpi kaikki mahdolliset tulot $\mathbf{pq}$, missä $\mathbf{p}, \mathbf{q}$ ovat 1-asteisia polynomeja eli polynomeja $\mathbf{X}, \mathbf{X}+1$. Näiden tuloina saadaan polynomit $\mathbf{X}^2$, $\mathbf{X}^2 + \mathbf{X}$, $\mathbf{X}^2 + 1$, joten ainoan jäljellä olevan toisen asteen polynomin $\mathbf{X}^2 + \mathbf{X} + 1$ täytyy olla jaoton.

Samantyyppisillä tarkasteluilla nähdään 3-asteisista polynomeista seuraavat jaot,

$$\mathbf{X}^3 = \mathbf{X}\mathbf{X}\mathbf{X}, \mathbf{X}^3 + \mathbf{X}^2 = \mathbf{X}\mathbf{X}(\mathbf{X}+1),$$

$$\mathbf{X}^3 + \mathbf{X} = \mathbf{X}(\mathbf{X}+1)(\mathbf{X}+1), \mathbf{X}^3 + 1 = (\mathbf{X}+1)(\mathbf{X}^2+\mathbf{X}+1),$$
$$\mathbf{X}^3 + \mathbf{X}^2 + \mathbf{X} = \mathbf{X}(\mathbf{X}^2+\mathbf{X}+1), \mathbf{X}^3 + \mathbf{X}^2 + 1,$$
$$\mathbf{X}^3 + \mathbf{X} + 1, \mathbf{X}^3 + \mathbf{X}^2 + \mathbf{X} + 1 = (\mathbf{X}+1)(\mathbf{X}+1)(\mathbf{X}+1).$$

Tässäkin ehkä nopein tapa on ensin laskea kaikki tulot $\mathbf{pq}$, missä $\deg \mathbf{p} = 1$, $\deg \mathbf{q} = 2$, jolloin saadaan kaikki jaolliset 3-asteiset polynomit (ja myös jaot niille). Jäljellä olevat ovat sitten jaottomia.

b) Ainoa tapa saada 4-asteinen polynomi $\mathbf{p}$, joka ei ole jaoton, mutta jolla ei ole juuria, on ottaa polynomi muotoa $\mathbf{p} = \mathbf{q}_1\mathbf{q}_2$, missä $\mathbf{q}_1, \mathbf{q}_2$ ovat jaottomia 2-asteisia polynomeja. Mutta a)-kohdan perusteella ainoa jaoton 2-asteinen polynomi on $\mathbf{X}^2 + \mathbf{X} + 1$, joten, itse asiassa, ainoa polynomi, joka kelpaa b)-kohdan (i)-osaan onpolynomi

$$(\mathbf{X}^2 + \mathbf{X} + 1)(\mathbf{X}^2 + \mathbf{X} + 1) = \mathbf{X}^4 + \mathbf{X}^2 + 1.$$

Tällöin jaottomaksi 4-asteiseksi polynomiksi kelpaa mikä tahansa toinen 4-asteinen polynomi, jolla ei ole juuria. Edellisen nojalla tällaisella polynomilla täytyy olla vakiotermi 1 ja lisäksi sillä täytyy olla pariton määrä nollasta eroavia termejä, eli, neljännen asteen polynomin kohdalla viisi tai kolme. Näin ollen b)-ii) kohdan vastaukseksi kelpaavat polynomit $\mathbf{X}^4 + \mathbf{X}^3 + \mathbf{X}^2 + \mathbf{X} + 1$, $\mathbf{X}^4 + \mathbf{X}^3 + 1$, $\mathbf{X}^4 + \mathbf{X} + 1$ (yksikin esimerkki riittää, tietysti).

c) Ainoa tapa saada 5-asteinen polynomi $\mathbf{p}$, joka ei ole jaoton, mutta jolla ei ole juuria, on ottaa polynomi muotoa $\mathbf{p} = \mathbf{q}_1\mathbf{q}_2$, missä $\deg \mathbf{q}_1 = 3$, $\deg \mathbf{q}_2$ ja kumpikin polynomi $\mathbf{q}_1, \mathbf{q}_2$ on jaoton. Koska nämä on selvitetty a)-kohdassa, ainoat vaihtoehdot ovat polynomit

$$(\mathbf{X}^2 + \mathbf{X} + 1)(\mathbf{X}^3 + \mathbf{X}^2 + 1) = \mathbf{X}^5 + \mathbf{X} + 1,$$

$$(\mathbf{X}^2 + \mathbf{X} + 1)(\mathbf{X}^3 + \mathbf{X} + 1) = \mathbf{X}^5 + \mathbf{X}^4 + 1$$

(yksi esimerkki riittää). Tällöin jaoton polynomi on mikä tahansa toinen 5-asteinen polynomi, jolla ei ole juuria. Edellisen nojalla tällaisella polynomilla täytyy olla vakiotermi 1 ja lisäksi sillä täytyy olla pariton määrä nollasta eroavia termejä, esimerkiksi $\mathbf{X}^5 + \mathbf{X}^3 + 1$ käy vastaukseksi(paljon muitakin on).

2. Kompleksiluvun $z = x + iy \in \mathbb{C}$ *konjugaatti* $\bar{z}$ on kompleksiluku $\bar{z} = x - iy$.
a) Osoita, että kuvaus $\phi\colon \mathbb{C} \to \mathbb{C}$, $\phi(z) = \bar{z}$ on $\mathbb{R}$-algebrojen välinen isomorfismi. Mikä on sen käänteiskuvaus? Onko ϕ myös $\mathbb{C}$-algebrojen välinen homomorfismi?
b) Osoita, että kaikilla $z \in \mathbb{C}$ kompleksiluvut $z\bar{z}$, $z + \bar{z}$ ovat reaalilukuja.

Ratkaisu: a) ϕ on bijektio, sillä on itse asiassa itsensä käänteiskuvaus, $\phi \circ \phi = \mathrm{id}$. Tämä johtuu siitä, että $\overline{\bar{z}} = \overline{x - iy} = x - (-iy) = x + y = z$ kaikilla $z = x + iy \in \mathbb{C}$.

Osoitetaan, että ϕ on rengashomomorfismi. Olkoot $z = x + iy$, $z' = x' + iy' \in \mathbb{C}$. Tällöin

$$\phi(z+z') = \phi((x+x')+i(y-y')) = (x+x')-(y-y')i = (x-yi)+(x'-y'i) = \phi(z)+\phi(z'),$$

$$\phi(zz') = \phi((xx' - yy') + i(xy' + x'y)) = (xx - yy') - i(xy' + x'y) =$$
$$(xx' - (-y)(-y')) + i(x(-y') + x'(-y)) = (x - yi)(x' - y'i) = \phi(z)\phi(z').$$

On näytetty, että kaikilla $z, z' \in \mathbb{C}$ pätee

$$\phi(z + z') = \phi(z) + \phi(z'),$$

$$\phi(zz') = \phi(z)\phi(z').$$

Näin ollen $\phi\colon \mathbb{C} \to \mathbb{C}$ on rengashomomorfismi. Näytetään vielä, että ϕ on yhteensopiva $\mathbb{R}$-skalaarikertolaskun suhteen, eli

$$\phi(rz) = r\phi(z)$$

kun $r \in \mathbb{R}, z \in \mathbb{C}$. Kun reaaliluku $r \in \mathbb{R}$ tulkitaan kompleksilukuna $r + i0$, selvästi $\phi(r) = r - i0 = r$. Näin ollen edellisen nojalla

$$\phi(rz) = \phi(r)\phi(z) = r\phi(z).$$

Tämä, edellä osoitetun yhtälön $\phi(z+z') = \phi(z)+\phi(z')$ kera, osoittaa, että $\phi\colon \mathbb{C} \to \mathbb{C}$ on $\mathbb{R}$-lineaarinen, kun $\mathbb{C}$ ajatellaan $\mathbb{R}$-vektoriavaruutena $\mathbb{R}^2$.

ϕ ei ole $\mathbb{C}$-lineaarinen, sillä tämä tarkoittaisi sitä, että

$$\phi(zz') = z\phi(z')$$

kaikilla $z, z' \in \mathbb{C}$. Kuitenkin edellä on jo osoitettu, että kaikilla $z, z' \in \mathbb{C}$ pätee $\phi(zz') = \phi(z)\phi(z')$. Näin ollen jos kumpikin kaava olisi voimassa, olisi myös totta, että $z\phi(z') = \phi(z)\phi(z')$ kaikilla $z, z' \in \mathbb{C}$. Sijoittamalla tässä $z' = 1$ saadaan $z = \phi(z)$ kaikilla $z \in \mathbb{C}$, mikä kuitenkin pitää paikkansa kun $z \in \mathbb{R}$. Voidaan myös antaa konkrettinen vasta-esimerkki: kun $z = i$, $z' = 1$ pätee

$$\phi(zz') = \phi(z) = -i \neq i = z\phi(z').$$

Näin ollen ϕ ei ole $\mathbb{C}$-lineaarinen.

b) Olkoon $z = x + iy \in \mathbb{C}$. Tällöin

$$z + \bar{z} = (x + iy) + (x - iy) = 2x \in \mathbb{R},$$

$$z\bar{z}(x + iy)(x - iy) = x^2 + y^2 \in \mathbb{R}.$$

3. a) Olkoon $\mathbf{p} \in \mathbb{R}[\mathbf{X}]$. Oletetaan, että kompleksiluku $z \in \mathbb{C}$ on tämän polynomin juuri. Osoita, että tällöin myös sen konjugaatti $\bar{z}$ on polynomin $\mathbf{p}$ juuri.
b) Osoita a)-kohdan avulla, että jokainen polynomi $\mathbf{p} \in \mathbb{R}[\mathbf{X}]$ voidaan esittää polynomialgebrassa $\mathbb{R}[\mathbf{X}]$ ensimmäisen ja toisen asteen polynomien tulona. Algebran peruslause saa olettaa tunnetuksi.

Ratkaisu: Olkoon $\mathbf{p} = \sum_{i=0}^{n} a_i \mathbf{X}^i \in \mathbb{R}[\mathbf{X}]$ ja oletetaan, että kompleksiluku $z \in \mathbb{C}$ on tämän polynomin juuri. Tämä tarkoittaa sitä, että

$$\sum_{i=0}^{n} a_i z^i = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n = 0.$$

Ottamalla tämän yhtälön molemmasta puolesta konjugaatti, eli soveltamalla siihen edellisen tehtävän kuvausta ϕ saadaan

$$\sum_{i=0}^{n} a_i \bar{z}^i = a_0 + a_1 \bar{z} + a_2 \bar{z}^2 + \ldots + a_n \bar{z}^n = 0.$$

Näin ollen konjugaatti $\bar{z}$ on myös polynomin $\mathbf{p}$ juuri. Huomaa, että tässä käytetään sitä, että $\overline{a_i} = a_i$ kaikilla $i = 0, \ldots, n$, sillä $a_i \in \mathbb{R}$ kaikilla $i = 0, \ldots, n$.

b) Jokainen algebran $\mathbb{R}[\mathbf{X}]$ polynomi voidaan myös ajatella algebran $\mathbb{C}[\mathbf{X}]$ polynomina, sillä $\mathbb{R} \subset \mathbb{C}$. Täsmällisesti tämä tarkoittaa sitä, että kuvaus $\iota \to \mathbb{R}[\mathbf{X}] \to \mathbb{C}[\mathbf{X}]$, joka kuvaa $\mathbb{R}$-kertoiminen polynomi $\mathbf{p} = \sum_{i=0}^{n} a_i \mathbf{X}^i \in \mathbb{R}[\mathbf{X}]$ samannäköiseksi $\mathbb{C}$-kertoimiseksi polynomiksi $\mathbf{p} = \sum_{i=0}^{n} a_i \mathbf{X}^i \in \mathbb{C}[\mathbf{X}]$, on injektiivinen $\mathbb{R}$-algebrojen välinen isomorfismi, joten $\mathbb{R}[\mathbf{X}]$ voidaan samastaa luonnollisella tavalla algebran $\mathbb{C}[\mathbf{X}]$ osajoukon $\operatorname{Im} \iota$ kanssa.

Olkoon $\mathbf{p} = \sum_{i=0}^{n} a_i \mathbf{X}^i \in \mathbb{R}[\mathbf{X}]$ reaalilukukertoiminen polynomi. Osoitetaan, että se voidaan kirjoittaa ensimmäisen ja toisen asteen reaalilukukertoimisten polynomien tulona. Olkoot $r_1, \ldots, r_k$ kaikki polynomin $\mathbf{p}$ *reaaliset* juuret. Tällöin Seurauksen 3.55 nojalla

$$\mathbf{p} = (\mathbf{X} - r_1)^{l_1} (\mathbf{X} - r_2)^{l_2} \ldots (\mathbf{X} - r_k)^{l_k} \mathbf{q},$$

missä $\mathbf{q}$ on sellainen polynomialgebran $\mathbb{R}[\mathbf{X}]$ polynomi, jolla ei ole lainkaan juuria kunnassa $\mathbb{R}$. Nyt riittää osoittaa, että tämä polynomi $\mathbf{q}$ voidaan kijoittaa toisen asteen (reaalilukukertoimisten) polynomien tulona. Tarkastellaan polynomi $\mathbf{q}$ algebran $\mathbb{C}[\mathbf{X}]$ alkiona. Koska kunta $\mathbb{C}$ on algebrallisesti suljettu (Propositio 3.18), polynomilla $\mathbf{q}$ on kunnassa $\mathbb{C}$ ainakin yksi juuri $z \in \mathbb{C}$, jolloin se on jaollinen polynomilla $(\mathbf{X} - z)$ algebrassa $\mathbb{C}[\mathbf{X}]$ (Propisitio 3.54). Koska $\mathbf{q}$ on $\mathbb{R}$-kertoiminen, a)-kohdan nojalla myös konjugaatti $\bar{z}$ on polynomin $\mathbf{q}$ juuri, joten $\mathbf{q}$ on myös jaollinen polynomilla $(\mathbf{X} - \bar{z})$ algebrassa $\mathbb{C}[\mathbf{X}]$. Lisäksi $z \neq \bar{z}$, sillä muuten z olisi reaaliluku, mikä on vastoin sitä tietoa, että polynomilla $\mathbf{q}$ ei ole juuria kunnassa $\mathbb{R}$. Ensimmäisen asteen polynomeina pääpolynomit $(\mathbf{X} - z)$ ja $(\mathbf{X} - \bar{z})$ ovat jaottomia, joten ne esiintyvät polynomin $\mathbf{q}$ yksikäsitteisessä esityksessä jaottomien pääpolynomien

tulona (Propositio 3.48). Tästä voidaan päätellä, että $\mathbf{q}$ on itse asiassa jaollinen (algebrassa $\mathbb{C}[\mathbf{X}]$!) polynomien $(\mathbf{X} - z)$ ja $(\mathbf{X} - \bar{z})$ tulona eli toisen asteen polynomilla

$$(\mathbf{X} - z)(\mathbf{X} - \bar{z}) = \mathbf{X}^2 - (z + \bar{z})\mathbf{X} + z\bar{z} = \mathbf{X}^2 + a\mathbf{X} + b,$$

missä $a = z + \bar{z}$, $b = z\bar{z}$. Kuitenkin edellisen tehtävän nojalla a ja b ovat kumpikin reaalilukuja, joten polynomi $\mathbf{X}^2 + a\mathbf{X} + b$ on algebran $\mathbb{R}[\mathbf{X}]$ 2-asteinen alkio. On osoitettu, että polynomilla $\mathbf{q}$ on toisen asteen reaalilukukertoiminen tekijä. Jatkamalla induktiivisesti saadaan $\mathbf{q}$ esitettyä toisen asteen reaalilukukertoimisten polynomien tulona, mikä todistaa väitteen.

Teknisellä tasolla tässä päättelyssä on pieniä teknisiä ongelmia, jotka pitää hoitaa jotenkin. Nimittäin yllä on osoitettu, että polynomilla $\mathbf{q}$ on toisen asteen realailukukertoiminen tekijä **polynomialgebrassa** $\mathbb{C}[\mathbf{X}]$, ei polynomialgebrassa $\mathbb{R}[\mathbf{X}]$! Tarkemmin sanottuna, on osoitettu, että on olemassa toisen asteen polynomi $\mathbf{q}_1 \in \mathbb{R}[\mathbf{X}]$ ja polynomi $\mathbf{q}_2 \in \mathbb{C}[\mathbf{X}]$ siten, että

$$\mathbf{q} = \mathbf{q}_1\mathbf{q}_2. \tag{2}$$

Pointti on siis siinä, että a priori polynomi $\mathbf{q}_2$ tässä on kompleksiketoiminen, joten kun induktiivisesti siirrytään siihen seuraavasti, ei voida päätellä suoraan a)-kohdan nojalla, että sen juuren z konjugaatti $\bar{z}$ on myös sen juuri. Tämä pieni tekninen ongelma voidaan hoitaa osoitamalla, että polynomilla $\mathbf{q}_2$ on itse asiassa välttämättä reaalilukukertoiminen. Osoitetaan tämä. Proposition 3.48 nojalla reaalilukertoiminen polynomi $\mathbf{q}_1$ voidaan esittää (yksikäsitteisellä tavalla muodossa

$$\mathbf{q}_1 = k \cdot \mathbf{r}_1\mathbf{r}_2 \dots \mathbf{r}_m,$$

missä $k \in \mathbb{R}^*$ ja $\mathbf{r}_i$ on polynomialgebran $\mathbb{R}[\mathbf{X}]$ jaoton *pääpolynomi* jokaisella $i = 1, \dots, m$. Tässä täytyy olla tarkka - polynomit $\mathbf{r}_i$ ovat siis jaottomia $\mathbb{R}[\mathbf{X}]$:ssä, ei välttämättä $\mathbb{C}[\mathbf{X}]$:ssä. Koska $\mathbf{q} = \mathbf{q}_1\mathbf{q}_2$, polynomit $\mathbf{r}_i$ ovat myös polynomin $\mathbf{q}$ tekijöitä. Koska jako jaottomiin tekijöihin on oleellisesti yksikäsitteinen, tästä voidaan päätellä, että jokainen polynomi $\mathbf{r}_i$ esiintyy myös polynomin $\mathbf{q}$ esityksessä jaottomien tekijöiden tulona. Erityisesti

$$\mathbf{q} = \mathbf{r}_1\mathbf{r}_2 \dots \mathbf{r}_m\mathbf{s},$$

missä $\mathbf{s}$ on jokin **reaalilukukertoiminen** polynomi. Sijoittamalla näitä esityksiä yhtälöön 2 ja supistamalla kummastakin puolesta yhteiset tekijät $\mathbf{r}_i$ (mikä onnistuu, sillä $\mathbb{C}[\mathbf{X}]$ on kokonaisalue!), saadaan

$$\mathbf{q}_2 = k^{-1}\mathbf{s} \in \mathbb{R}[\mathbf{X}],$$

mitä pitikin todistaa.

Tämä ratkaisutapa yleistyy yleiseen tilanteeseen, jossa pari $\mathbb{R}, \mathbb{C}$ voidaan korvata millä tahansa kunnilla K, K', joille $K \leq K'$. Toisin sanoen samalla tavalla voidaan osoittaa, että jos

$$\mathbf{q} = \mathbf{q}_1\mathbf{q}_2,$$

missä $\mathbf{q}, \mathbf{q}_1 \in K[\mathbf{X}]$, $\mathbf{q}_1 \neq \mathbf{0}$ ja $\mathbf{q}_2 \in K'[\mathbf{X}]$, missä K on kunnan K' alikunta, niin itse asiassa $\mathbf{q}_2 \in K[\mathbf{X}]$.

Hieman erikoisempi toinen todistustapa, joka toimisi vain reaali-ja kompleksilukujen kuntien tapauksessa olisi käyttää konjugaattioperaattoria. Nimittäin edellisen tehtävän konjugaattikuvaus $z \mapsto \bar{z}$ helposti yleistyy polynomeihin. Toisin sanoen jos $\mathbf{p} = \sum_{i=0}^{n} a_i \mathbf{X}^i \in \mathbb{C}[\mathbf{X}]$, voidaan määritellä sen konjugaatti $\overline{\mathbf{p}} = \in \mathbb{C}[\mathbf{X}]$ kaavalla $\overline{\mathbf{p}} = \sum_{i=0}^{n} \overline{a_i} \mathbf{X}^i$. Helposti nähdään, että vastaavuus $\mathbf{p} \to \overline{\mathbf{p}}$ on injektiivinen ja säilyttää kaikki polynomien laskutoimitukset, toisin sanoen on algebraisomorfismi. Erityisesti yhtälöstä $\mathbf{q} = \mathbf{q}_1 \mathbf{q}_2$ seuraa yhtälö

$$\overline{\mathbf{q}} = \overline{\mathbf{q}_1 \mathbf{q}_2}.$$

Toisaalta helposti nähdään, että polynomi $\mathbf{p} \in \mathbb{C}[\mathbf{X}]$ on reaalilukukertoiminen jos ja vain jos se on itsensä konjugaatti eli $\mathbf{p} = \overline{\mathbf{p}}]$. Näin ollen, jos $\mathbf{q}, \mathbf{q}_1 \in \mathbb{R}[\mathbf{X}]$, saadaan yhtälö $\mathbf{q} = \mathbf{q}_1 \overline{\mathbf{q}_2}$. Jos lisäksi $\mathbf{q}_1 \neq \mathbf{0}$ tästä seuraa yhtälön $\mathbf{q} = \mathbf{q}_1 \mathbf{q}_2$ avulla, että $\mathbf{q}_2 = \overline{\mathbf{q}_2}$, joten $\mathbf{q}_2$ on myös reaalilukukertoiminen.

Kolmas tapa: Suoralla ”laskulla”. Oletetaan, että $\mathbf{q} = \sum_{i=0}^{n+m} a_i \mathbf{X}^i$, $\mathbf{q}_1 = \sum_{j=0}^{n} b_j \mathbf{X}^j$ kumpikin polynomialgebran $K[\mathbf{X}]$ polynomi ja $\mathbf{q}_2 = \sum_{k=0}^{m} c_k \mathbf{X}^k \in K'[\mathbf{X}]$, missä $K \leq K'$. Oletetaan, että $\mathbf{q} = \mathbf{q}_1 \mathbf{q}_2 \neq \mathbf{0}$. Tehtävänä on osoittaa, että tällaisessa tilantessa myös $\mathbf{q}_2 \in K[\mathbf{X}]$. Todistetaan tämä induktiolla polynomin $\mathbf{q}_2$ asteen suhteen. Jos $\mathbf{q}_2 = c_0 \in K'$ on vakiopolynomi, on selvä, että $c_0 b_n = a_n$, mistä seuraa, että $c_0 = a_n / b_n \in K$. Yleisessä tapauksessa yhtälö $\mathbf{q} = \mathbf{q}_1 \mathbf{q}_2$ kirjoitettuna auki on yhtälö muotoa

$$a_{n+m} X^{n+m} + \text{ alempi-asteisia termejä } = b_n c_m X^{n+m} + \text{ alempi-asteisia termejä } .$$

Tästä nähdään, että $a_{n+m} = b_n c_m$, mistä seuraa, että $c_m = a_{n+m} / b_n \in K$. Lisäksi tällöin

$$\mathbf{q} = \mathbf{q}_1 (b_n \mathbf{X}^{\mathbf{m}} + \mathbf{q}_2'),$$

missä $\mathbf{q}_2' = \mathbf{q} - b_n \mathbf{X}^{\mathbf{m}}$ on pienempi asteinen polynomi. Tämä voidaan kirjoittaa muotoon

$$\mathbf{q} - \mathbf{q}_1 b_n \mathbf{X}^{\mathbf{m}} = \mathbf{q}_1 \mathbf{q}_2'.$$

Tässä sekä polynomi $\mathbf{q}_1$, että vasemmanpuoleinen polynomi $\mathbf{q} - \mathbf{q}_1 b_n \mathbf{X}^{\mathbf{m}}$ on algebran $K[\mathbf{X}]$ polynomi. Induktio-oletuksesta seuraa, että $\mathbf{q}_2' \in K[\mathbf{X}]$. Näin ollen myös $\mathbf{q}_2 = b_n \mathbf{X}^{\mathbf{m}} + \mathbf{q}_2' \in K[\mathbf{X}]$, joten haluttu apuväite saadaan todistettua.

Tavalla tai toisella, on kuitenkin näytetty, että jokainen reaalilukukertoiminen polynomi $\mathbf{q}$, jolla ei ole reaalijuuria, on esitettävissä muodossa

$$\mathbf{q} = \mathbf{q}_1 \mathbf{q}_2,$$

missä $\mathbf{q}_1$ ja $\mathbf{q}_2$ ovat *reaalilukkertoimisia* ja $\deg \mathbf{q}_1 = 2$. Haluttu väite seuraa tämän jäkeen helpolla iunduktiolla polynomin $\mathbf{q}$ asteen suhteen.

Vielä yksi ratkaisutapa: Yksi suosittu hieman vaihtoehtoinen ratkaisutapa on seuraava - a)-kohdan perusteella tiedetään, että jokaista reaalikertoimisen polynomin ensimmäisen asteen tekijää $(\mathbf{X} - z)$, missä $z \in \mathbb{C}$ on kompleksiluku, vastaa tekijä $(\mathbf{X} - \bar{z})$. Joz z ei ole reaaliluku, tekijät $(\mathbf{X} - z)$ ja $(\mathbf{X} - \bar{z})$ ovat eri tekijöitä. Koska $\mathbb{C}$ on algebrallisesti suljettu, jokainen reaalilukukertoiminen polynomin $\mathbf{p} \in \mathbb{R}[\mathbf{X}]$ voidaan esittää ensimmäisen asteen tekijöiden tulona algebrassa $\mathbb{C}[\mathbf{X}]$. Edellisen nojalla jokaista aitoa kompleksilukujuurta z vastaa sen "pari" $\bar{z}$. Yhdistämällä aidosti kompleksiset ratkaisut konjugaattipareiksi saadaan polynomille esitys muodossa

$$\mathbf{p} = (\mathbf{X} - r_1) \dots (\mathbf{X} - r_n)(\mathbf{X} - z_1)(\mathbf{X} - \bar{z}_1) \dots (\mathbf{X} - z_m)(\mathbf{X} - \bar{z}_m),$$

jossa $r_1, \dots, r_n$ ovat kaikki polynomit reaaliset juuret ja muut kompleksiset juuret kootu pareissa konjugaattiensa kera. Koska $(\mathbf{X} - z_i)(\mathbf{X} - \bar{z}_i)$ on reaalikertoiminen polynomi, väite seuraa tästä.

Valitettavasti tässäkin yksinkertaisessa ratkaisussa on teknisiä ongelmia, jotka pitää hoitaa. Nimittäin edellä esitettynä se toimii sellaisenaan ilman lisätarkasteluja vain kun polynomin $\mathbf{p}$ aidosti kompleksiset juuret ovat kaikki *yksinkertaisia*. Jos taas jokin juuri on monikertainen ei ole itsestään selvä, että kaikille sen "esiintymisille" löytyy konjugaattipari. Tarkemmin sanottuna oletetaan, että juuri $z \in \mathbb{C}$, $z \notin \mathbb{R}$ on monikertainen, jolloin polynomin $\mathbf{p}$ jaossa ensimmäisen asteen tekijöihin tekijä $(\mathbf{X} - z)$ esiintyy ainakin kaksi kertaa. Toisin sanoen $\mathbf{p}$ on jaollinen ainakin polynomilla $(\mathbf{X} - z)^2$. Nyt a)-kohdan perusteella myös konjugaatti $\bar{z}$ on polynomin $\mathbf{p}$ juuri, jolloin sillä on myös ainakin tekijä $(\mathbf{X} - \bar{z})$. Tämä tekijä voidaan "yhdistää" toisen tekijän muotoa $(\mathbf{X} - z)$ kanssa, jolloin syntyy reaalilukukertoiminen toisen asteen polynomi, mutta esitykseen jää kuitenkin roikkumaan vielä ainakin yksi termi $(\mathbf{X} - z)$. Voidaanko olla varmoja siitä, että sillekin löytyy pari? Tämä vaatii lisää selvittelyjä. Pari löytyy, jos löytyy toinenkin muotoa $(\mathbf{X} - \bar{z})$ oleva tekijä. Itse asiassa niitä täytyy olla saman verran kuin tekijöitä muotoa $(\mathbf{X} - z)$, jotta jokaiselle niistä löytyisi sopiva "pari". Näin ollen, jotta tämä ratkaisutapa toimisi pitää itse asiassa todistaa todeksi vielä seuraava väite:

Väite: Olkoon $\mathbf{p} \in \mathbb{R}[\mathbf{X}]$ polynomi. Olkoon $z \in \mathbb{C}$ sen juuri. Tällöin juuren $\bar{z}$ *kertaluku* on sama kuin juuren z kertaluku.
Väitteen todistus: Symmetrian vuoksi (koska konjugaatin konjugaatti on luku itse) riittää osoittaa seuraava. Oletetaan, että $(\mathbf{X} - z)^l$ on polynomin $\mathbf{p}$ tekijä (algebrassa $\mathbb{C}[\mathbf{X}]$) jollakin $l \in \mathbb{N}$. Tällöin $(\mathbf{X} - \bar{z})^l$ on myös polynomin $\mathbf{p}$ tekijä.

Tämän osoittamiseksi käytetään konjugaatti-operaattorin laajennusta polynomialgebraan $\mathbb{C}[\mathbf{X}]$, josta oli jo puhe edellä. Jos $\mathbf{p}$ on jaollinen algebrassa $\mathbb{C}[\mathbf{X}]$ polynomilla $(\mathbf{X} - z)^l$, on olemassa polynomi $\mathbf{q} \in \mathbb{C}[\mathbf{X}]$ siten, että

$$\mathbf{p} = (\mathbf{X} - z)^l \mathbf{q}.$$

Ottamalla tämän yhtälön kummastakin puolesta konjugaatit saadaan

$$\mathbf{p} = \overline{\mathbf{p}} = (\mathbf{X} - \bar{z})^l \overline{\mathbf{q}}.$$

Näin ollen $(\mathbf{X} - \bar{z})^l$ on myös polynomin $\mathbf{p}$ tekijä. Edellisen nojalla, tämä riittää meitä kiinnostavan väitteen todistamiseksi.

4. Olkoon $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Polynomia $\mathbf{p} = \sum_{i=0}^{n} a_i \mathbf{X}^i \in K[\mathbf{X}]$ sanotaan *kokonaislukukertoimiseksi* jos sen kertoimet $a_0, \ldots, a_n$ ovat kokonaislukuja. Oletetaan, että $m \in \mathbb{Z}$ on kokonaislukukertoimisen polynomin $\mathbf{p} = \sum_{i=0}^{n} a_i \mathbf{X}^i$ juuri. Osoita, että tällöin m on luvun a_0 tekijä. Tutki tämän tuloksen avulla polynomien $\mathbf{X}^3 - 2\mathbf{X} + 4$ ja $\mathbf{X}^4 - 2\mathbf{X}^3 - 4\mathbf{X}^2 + 10\mathbf{X} - 5$ juuria kunnassa K. Jaa nämä polynomit jaottomiin tekijöihin (polynomialgebrassa $K[\mathbf{X}]$).

Ratkaisu: Oletetaan, että kokonaisluku $m \in \mathbb{Z}$ on kokonaislukukertoimisen polynomin $\mathbf{p} = \sum_{i=0}^{n} a_i \mathbf{X}^i$ juuri. Tämä tarkoittaa sitä, että

$$a_n m^n + a_{n-1} m^{n-1} + \ldots + a_1 m + a_0 = 0,$$

mikä voidaan kirjoittaa myös muotoon

$$a_0 = m(-a_n m^{n-1} - a_{n-1} m^{n-2} - \ldots - a_1).$$

Koska luku $-a_n m^{n-1} - a_{n-1} m^{n-2} - \ldots - a_1$ suluissa on nyt kokonaisluku, tästä seuraa, että m on luvun a_0 tekijä.

Tutkitaan polynomin $\mathbf{X}^3 - 2\mathbf{X} + 4$ kompleksisia juuria. Koska emme osaa ratkaista kolmen asteen yhtälöitä suoraan (on kyllä olemassa kaava, mutta se on melko monimutkainen eikä ole yleensä käyttökelpoinen käytännössä), etsitään ensin kokonaislukujuria (jos niitä on ylipäätän olemassa). Koska polynomi on kokonaislukukertoiminen, tehtävän ensimmäisen osan nojalla jos kokonaisluku $m \in \mathbb{Z}$ on tämän polynomin juuri, niin se on vakiotermin 4 tekijä. Tämän tekijät ovat $\pm 1, \pm 2, \pm 4$ (muista negatiivisia lukuja!). Sijoittamalla näitä polynomiin nähdään suoraan, että niistä vain (-2) on polynomin juuri. Proposition 3.54 nojalla polynomi $\mathbf{X}^3 - 2\mathbf{X} + 4$ on jaollinen polynomilla $X + 2$ missä tahansa kunnassa $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (sillä 2 kuuluu jokaiseen näistä). Jakamalla jakokulmassa (algoritmi esitetty Proposition 3.35 todistuksen yhteydessä) saadaan $\mathbf{X}^3 - 2\mathbf{X} + 4 = (\mathbf{X} + 2)(\mathbf{X}^2 - 2\mathbf{X} + 2)$:

$$\begin{array}{rl}
 & X^2 - 2X + 2 \\
\cline{2-2}
X + 2 \big) & X^3 \quad - 2X + 4 \\
 & -X^3 - 2X^2 \\
\cline{2-2}
 & \quad -2X^2 - 2X \\
 & \quad 2X^2 + 4X \\
\cline{2-2}
 & \quad 2X + 4 \\
 & \quad -2X - 4 \\
\cline{2-2}
 & \quad 0
\end{array}$$

Nyt riittää ratkaista vain toisen asteen polynomit $\mathbf{X}^2 - 2\mathbf{X} + 2$ juuria kompleksilukujen kunnassa. Tämä osataan - kyse on toisen asteen yhtälön ratkaisemista, joka onnistuu $\mathbb{C}$:ssä periatateessa samalla koulusta tutulla ratkaisukaavalla kuin $\mathbb{R}$:ssä (kts. Harj. 9.2 ratksaisu). Yhtälön $x^2 - 2x + 2 = 0$ ratkaisut ovat

$$x_{1,2} = \frac{2 \pm \sqrt{4 - 2 \cdot 4}}{2} = 1 \pm i.$$

Kumpikin juurista on kompleksiluku, mutta ei ole reaali tai rationaaliluku. Koska toisen asteen polynomi on jaoton täsmälleen silloin, kun sillä ei ole juuria, nähdään, että polynomirenkaissa $\mathbb{Q}[\mathbf{X}]$, $\mathbb{R}[\mathbf{X}]$ polynomi $\mathbf{X}^2 - 2\mathbf{X} + 2$ on jaoton. Kunnassa $\mathbb{C}$ taas pätee edellisen nojalla yhtälö

$$\mathbf{X}^2 - 2\mathbf{X} + 2 = (\mathbf{X}1 + i)(\mathbf{X} + 1 - i).$$

Näin ollen kunnissa $\mathbb{Q}[\mathbf{X}]$, $\mathbb{R}[\mathbf{X}]$ polynomi $\mathbf{X}^3 - 2\mathbf{X} + 4$ jakautuu jaottomiin polynomeihin seuraavasti:

$$\mathbf{X}^3 - 2\mathbf{X} + 4 = (\mathbf{X} + 2)(\mathbf{X}^2 - 2\mathbf{X} + 2).$$

Kunnassa $\mathbb{C}[\mathbf{X}]$ taas jako on

$$\mathbf{X}^3 - 2\mathbf{X} + 4 = (\mathbf{X} + 2)(\mathbf{X}1 + i)(\mathbf{X} + 1 - i).$$

Seuraavasti tarkastellaan samalla tavalla polynomia $\mathbf{X}^4 - 2\mathbf{X}^3 - 4\mathbf{X}^2 + 10\mathbf{X} - 5$. Aloitetaan kokonaislukujuurista. Tehtävän alkuosan nojalla kokonaislukujuuret sijaitsevat joukossa $\{\pm 1, \pm 5\}$. Kokoilemalla nähdään heti, että 1 on juuri. Jakamalla polynomi jakokulmassa polynomilla $\mathbf{X} - 1$ saadaan

$$\mathbf{X}^4 - 2\mathbf{X}^3 - 4\mathbf{X}^2 + 10\mathbf{X} - 5 = (\mathbf{X} - 1)(\mathbf{X}^3 - \mathbf{X}^2 - 5\mathbf{X} + 5).$$

$$\begin{array}{r|l}
 & X^3 - X^2 - 5X + 5 \\
\hline
X - 1 & X^4 - 2X^3 - 4X^2 + 10X - 5 \\
 & \underline{-X^4 + X^3} \\
 & \quad -X^3 - 4X^2 \\
 & \quad \underline{X^3 - X^2} \\
 & \quad\quad -5X^2 + 10X \\
 & \quad\quad \underline{5X^2 - 5X} \\
 & \quad\quad\quad 5X - 5 \\
 & \quad\quad\quad \underline{-5X + 5} \\
 & \quad\quad\quad\quad 0
\end{array}$$

Soveltamalla sama testi polynomiin $\mathbf{X}^3 - \mathbf{X}^2 - 5\mathbf{X} + 5$ nähdään, että luku 1 on myös tämän polynomin juuri. Jaetaan siis taas jakokulmassa, jolloin saadaan

$$\mathbf{X}^3 - \mathbf{X}^2 - 5\mathbf{X} + 5 = (\mathbf{X} - 1)(\mathbf{X}^2 - 5)$$

(nähdään myös helpommin ryhmittämällä).

$$\begin{array}{r|l}
 & X^2 - 5 \\
\hline
X - 1 & X^3 - X^2 - 5X + 5 \\
 & \underline{-X^3 + X^2} \\
 & \quad -5X + 5 \\
 & \quad \underline{5X - 5} \\
 & \quad\quad 0
\end{array}$$

Yhtälön $x^2 - 5 = 0$ ratkaisut ovat $\pm\sqrt{5}$. Kumpikin on reaaliluku, mutta ei rationaaliluku. Näin ollen algebrassa $\mathbb{Q}[\mathbf{X}]$ polynomin $\mathbf{X}^4 - 2\mathbf{X}^3 - 4\mathbf{X}^2 + 10\mathbf{X} - 5$ jako jaottomiin polynomeihin on

$$\mathbf{X}^4 - 2\mathbf{X}^3 - 4\mathbf{X}^2 + 10\mathbf{X} - 5 = (\mathbf{X} - 1)^2(\mathbf{X}^2 - 5).$$

Algebroissa $\mathbb{R}[\mathbf{X}]$ ja $\mathbb{C}[\mathbf{X}]$ taas jako on

$$\mathbf{X}^4 - 2\mathbf{X}^3 - 4\mathbf{X}^2 + 10\mathbf{X} - 5 = (\mathbf{X} - 1)^2(\mathbf{X} + \sqrt{5})(\mathbf{X} - \sqrt{5}).$$

5. Olkoon K ääretön kunta. Osoita, että kuvaus $F\colon K[\mathbf{X}] \to K^K$, joka kuvaa polynomin $\mathbf{p} \in K[\mathbf{X}]$ vastaavaksi polynomifunktioksi $p\colon K \to K$, on *injektiivinen* K-algebrahomomorfismi. Huom., tämä erityisesti todistaa sen, että äärettömän kunnan tapauksessa polynomifunktion kertoimet määräävät sen yksikäsiteisesti.

Ratkaisu: Kuvaus F säilyttää kaikki laskutoimitukset, sillä polynomifunktioilla lasketaan samalla tavalla kuin abstrakteilla algebrallisilla polynomeilla.

Koska homomorfismi on injektiivinen jos ja vain jos sen ydin on triviaali, joten riittää todistaa, että $F(\mathbf{p}) = 0$ ainoastaan jos $\mathbf{p}$ on nolla-polynomi. Oletetaan, että algebrallisen polynomin $\mathbf{p}$ määrämä polynomi funktio $p\colon K \to K$ on identtisesti nolla-funktio. Tämä tarkoittaa täsmälleen sitä, että kunnan K jokainen alkio $k \in K$ on tämän polynomin juuri. Kuitenkin Proposition 3.54 nojalla ei-nolla polynomilla $\mathbf{p} \in K[\mathbf{X}]$ voi olla vain äärellinen määrä (itse asiassa korkeintaan polynomin $\mathbf{p}$ asteen verran) juuria kunnassa K. Koska kunta K on ääretön, tästä seuraa, että polynomin $\mathbf{p}$ täytyy olla nolla-polynomi.

6. Tarkastellaan seuraavia $\mathbb{R}$-algebroja A_1, A_2, A_3,

$$A_1 = \mathbb{R}[\mathbf{X}]/(\mathbf{X}^2),$$

$$A_2 = \mathbb{R}[\mathbf{X}]/(\mathbf{X}^2 - 1),$$

$$A_3 = \mathbb{R}[\mathbf{X}]/(\mathbf{X}^2 + 1).$$

a) Osoita, että $\dim_{\mathbb{R}} A_i = 2$ kaikilla $i = 1, 2, 3$. Osoita, että näistä kolmesta algebrasta A_1 on ainoa, jossa on olemassa alkio $\mathbf{x} \neq \mathbf{0}$, jolle pätee $\mathbf{x}^2 = \mathbf{0}$.
b) Osoita, että algebra A_2 ei ole renkaana kokonaisalue.
c) Osoita, että A_3 on $\mathbb{R}$-algebrana isomorfinen kompleksilukujen $\mathbb{R}$-algebran $\mathbb{C}$ kanssa.
d) Päättele, että näistä kolmesta algebrasta mitkään kaksi eivät ole isomorfisia keskenään.

Ratkaisu: Proposition 3.63 nojalla algebra A_i on 2-ulotteinen $\mathbb{R}$-vektoriavaruutena suhteen kaikilla $i = 1, 2, 3$, sillä polynomit $\mathbf{X}^2$, $\mathbf{X}^2 \pm 1$ ovat tasan 2-asteiset. Lisäksi saman Propisition nojalla eräs $\mathbb{R}$-vektoriavaruuden A_i kanta on $(1, \bar{\mathbf{X}})$. Vektoriavaruutena siis jokainen algebra A_i on samannäköinen. Jokainen sen alkio voidaan

esittää yksikäsitteisellä tavalla muodossa $a1 + b\bar{\mathbf{X}} = a + b\mathbf{X}$ joillakin $a, b \in \mathbb{R}$. Ainoa missä algebrat eroavat on kertolasku operaatio.

Algebrassa A_1 pätee sen määritelmän nojalla $\bar{\mathbf{X}}^2 = 0$, erityisesti tässä algebrassa on olemassa nollasta eroava alkio, jonka neliö on nolla. Tämän avulla myös nähdään, että kahden alkion $a + b\bar{\mathbf{X}}$ ja $c + d\bar{\mathbf{X}}$, $a, b, c, d \in \mathbb{R}$ tulo on

$$(a + b\bar{\mathbf{X}})(c + d\bar{\mathbf{X}}) = ac + (ad + bc)\bar{\mathbf{X}} + bd\bar{\mathbf{X}}^2 = ac + (ad + bc)\bar{\mathbf{X}}.$$

Emme oikestaan tarvitse tätä kaavaa jatkossa, mutta sen kirjoittaminen auki auttaa ymmärtämään mistä on kyse.

Algebrassa A_2 pätee sen määritelmän nojalla $\bar{\mathbf{X}}^2 = 1$. Tämän avulla nähdään, että kahden alkion $a + b\bar{\mathbf{X}}$ ja $c + d\bar{\mathbf{X}}$, $a, b, c, d \in \mathbb{R}$ tulo on

$$(a + b\bar{\mathbf{X}})(c + d\bar{\mathbf{X}}) = ac + (ad + bc)\bar{\mathbf{X}} + bd\bar{\mathbf{X}}^2 = (ac + bd) + (ad + bc)\bar{\mathbf{X}}.$$

Näytetään tämän avulla, että algebrassa A_2 ei ole olemassa sellaista nollasta eroavaa alkiota $a + b\bar{\mathbf{X}}$, jonka neliö on nolla. Nimittäin jokaisella $a + b\bar{\mathbf{X}} \in A_2$ pätee edellisen nojalla

$$(a + b\bar{\mathbf{X}})^2 = (a^2 + b^2) + 2ab\bar{\mathbf{X}}.$$

Koska jono $(1, \bar{\mathbf{X}})$ on kanta, tästä seuraa $a^2 + b^2 = 0 = 2ab$. Näistä selvästi seuraa, että $a = b = 0$, joten ainoastaan nolla-alkion neliö on nolla.

Algebra A_2 ei kuitenkaan ole kokonaisalue, sillä siinä nollasta eroavien alkioiden $\bar{\mathbf{X}} - 1$, $\bar{\mathbf{X}} + 1$ tulo $\bar{\mathbf{X}}^2 - 1$ on nolla algebrassa A_2. Vaihtoehtoisesti voidaan vedota myös suoraan Propositioon 3.63, jonka mukaan tekijäalgebra $K[\mathbf{X}]/(\mathbf{p})$ on kokonaisalue jos ja vain jos polynomi $\mathbf{p}$ on jaoton. Algebran A_2 kohdalla polynomi $\mathbf{X}^2 - 1 = (\mathbf{X} - 1)(\mathbf{X} + 1)$ ei ole jaoton, joten A_2 ei ole kokonaisalue. b)-kohdan väite on todistettu.

Algebrassa A_3 pätee sen määritelmän nojalla $\bar{\mathbf{X}}^2 = -1$. Tämän avulla nähdään, että kahden alkion $a + b\bar{\mathbf{X}}$ ja $c + d\bar{\mathbf{X}}$, $a, b, c, d \in \mathbb{R}$ tulo on

$$(a + b\bar{\mathbf{X}})(c + d\bar{\mathbf{X}}) = ac + (ad + bc)\bar{\mathbf{X}} + bd\bar{\mathbf{X}}^2 = (ac - bd) + (ad + bc)\bar{\mathbf{X}}.$$

Tästä nähdään suoraan, että kertolasku A_3:ssä ”näyttää samalta” kuin kompleksilukujen kertolasku, jos korvataan $\bar{\mathbf{X}}$ imaginaariyksiköllä i. Määritellään siis kuvaus $f\colon \mathbb{C} \to A_3$ kaavalla $f(a + bi) = a + b\bar{\mathbf{X}}$. Edellisen nojalla tämä säilyttää kertolaskun. Lisäksi kuvaus f on bijektio, sillä $(1, \bar{\mathbf{X}})$ on kanta. Helposti nähdään, että myös yhteen-ja skalaarikertolaskut ($\mathbb{R}$:n alkiolla) säilyvät kuvauksessa f. Tämä todistaa c)-kohdan väitteen. Koska $\mathbb{C}$ on kunta, myös A_3 on renkaana kunta, joten erityisesti se on kokonaisalue ja siinä ei voi olla nollasta eroavaa alkiota, jonka neliö on nolla. Myös a)-kohdan väite on nyt todistettu.

Algebrat A_i eivät ole pareittain isomorfisia. A_1 ei ole isomorfinen muiden kanssa, sillä siinä on nollasta eroava alkio, jonka neliö on nolla, kun taas algebroista A_2, A_3 tällaista ei löydy. A_2 ja A_3 eivät ole isomorfisia, sillä A_2 ei ole kokonaisalue, kun taas A_3 on jopa kunta.

7.* Jatkoa edelliselle tehtävälle. Osoita, että edellisen tehtävän $\mathbb{R}$-algebrat A_1, A_2, A_3 ovat isomorfiaa vaille ainoat 2-ulotteiset $\mathbb{R}$-algebrat.
Ohje: Olkoon A 2-ulotteinen $\mathbb{R}$-algebra. Aloita näyttämällä, että A:llä on kanta muotoa $(\mathbf{1}_A, \mathbf{v})$. Osoita sen jälkeen, että $\mathbf{v}$ voidaan valita siten, että $\mathbf{v}^2 \in \mathrm{Span}(\mathbf{1}_A)$. Näytä vielä sen jälken "normeeramalla", että voidaan olettaa $\mathbf{v}^2 \in \{\mathbf{1}_A, \mathbf{0}_A, -\mathbf{1}_A\}$. Johda väite tästä.

Lisää pohdittavaa: Yksinkertaisin esimerkki 2-ulotteisesta $\mathbb{R}$-algebrasta on "tuloalgebra" $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, jossa kertolasku on määritelty "koordinateittain". Tämän avaruuden standardikannalle $(\mathbf{e}_1, \mathbf{e}_2)$ pätee $\mathbf{e}_i \cdot \mathbf{e}_j = \delta_{ij}$. Tehtävän väitteen nojalla $A = \mathbb{R} \times \mathbb{R}$ on isomorfinen tasan yhden algebroista A_1, A_2, A_3 kanssa. Osoita, että A on itse asiassa isomorfinen algebran A_2 kanssa. Etsi jokin algebran A_2 kanta $(\mathbf{v}_1, \mathbf{v}_2)$, jolle pätee $\mathbf{v}_i \cdot \mathbf{v}_j = \delta_{ij}$.

Ratkaisu: Olkoon A kaksiulotteinen $\mathbb{R}$-algebra. Koska A on algebrana erityisesti rengas, sen kertolasku operaatiolla on neutraalialkio $\mathbf{1}_A$, joka ei ole nolla-vektori $\mathbf{0}_A$ (sillä muuten A olisi renkaana triviaali yhden alkion rengas, mikä on mahdotonta, jos se on kaksiulotteinen $\mathbb{R}$-vektoriavaruus). Näin ollen jono $(\mathbf{1}_A)$ on vapaa vektoriavaruudessa A. Koska $\dim_{\mathbb{R}} A = 2$, tämä jono voidaan laajentaa koko avaruuden A kannaksi $(\mathbf{1}_A, \mathbf{v})$. Tässä vektoriksi $\mathbf{v}$ kelpaa itse asiassa mikä tahansa avaruuden A vektori, joka ei ole 1-ulotteisessa aliavaruudessa $\mathrm{Span}(\mathbf{1}_A)$. Tämän aliavaruuden vektori taas ei kelpaa, sillä sellaiselle vektorille jono $(\mathbf{1}_A, \mathbf{v})$ on sidottu.

Seuraavaksi osoitetaan, että $\mathbf{v}$ voidaan itse asiassa valita sillä tavalla, että $\mathbf{v}^2 \in \mathrm{Span}(\mathbf{1}_A)$. Olkoon $r \in \mathbb{R}$ ja tarkastellaan vektoria $\mathbf{w} = r \cdot 1_A + \mathbf{v}$. Tälle vektorille pätee

$$\mathbf{w}^2 = (r \cdot \mathbf{1}_A + \mathbf{v})(r \cdot \mathbf{1}_A + \mathbf{v}) = r^2 \cdot \mathbf{1}_A + 2r\mathbf{v} + \mathbf{v}^2.$$

Koska $\mathbf{v}^2 \in A$, on olemassa $a, b \in \mathbb{R}$ siten, että

$$\mathbf{v}^2 = a\mathbf{1}_A + b\mathbf{v}.$$

Näin ollen vekrtorille muotoa $\mathbf{w} = r \cdot 1_A + \mathbf{v}$ pätee

$$\mathbf{w}^2 = (r^2 - a) \cdot \mathbf{1}_A + (2r + b)\mathbf{v}.$$

Tästä nähdään, että jos valitaan $r = -b/2$, niin $\mathbf{w}^2 \in \mathrm{Span}(\mathbf{1}_A)$. Lisäksi $\mathbf{w} = r \cdot 1_A + \mathbf{v} \notin \mathrm{Span}(\mathbf{1}_A)$, joten voidaan korvata vektori $\mathbf{v}$ vektorilla $\mathbf{w}$. On siis näytetty, että avaruudella A on olemassa kanta muotoa $(\mathbf{1}_A, \mathbf{w})$, missä $\mathbf{w}^2 = t\mathbf{1}_A$ jollakin $t \in \mathbb{R}$. Seuraavaksi "normeeramalla" $\mathbf{w}$ jakamalla sopivalla luvulla päästään tilanteseen, jossa voidaan olettaa, että $\mathbf{w}^2 \in \{0, 1, -1\}$. Tarkemmin sanottuna, tarkastellaan seuraavaksi erikseen tapauksia $t = 0$, $t < 0$, $t > 0$.

Vaihtoehto 1: $t = 0$. Algebralla A on siis kanta $(\mathbf{1}_A, \mathbf{w})$, jossa $\mathbf{w}^2 = \mathbf{0}_A$. Tästä seuraa, että vektorin $\mathbf{w}$ *minimipolynomi* algebrassa A on polynomi $\mathbf{X}^2$. Koska tämän minimipolynomin virittämä ideaali $(\mathbf{X}^2)$ on sijoitushomomorfismin $S_{\mathbf{w}} \colon \mathbb{R}[\mathbf{X}] \to A$ ydin, isomorfialauseesta (Lause 3.61) seuraa, että tekijäalgebra $A_1 = \mathbb{R}[\mathbf{X}]/(\mathbf{X}^2)$ on

isomorfinen algebran A alialgebran $\operatorname{Im} S_{\mathbf{w}}$ kanssa. Kuitenkin $\operatorname{Im} S_{\mathbf{w}} = A$, sillä A:n kantavektorit $\mathbf{1}_A, \mathbf{w}$ selvästi kuuluvat kuvaan $\operatorname{Im} S_{\mathbf{w}}$. Toisin sanoen tässä tapauksessa A on isomorfinen algebran A_1 kanssa.

Vaihtoehto 2: $t > 0$. Tällöin jakamalla positiivisella reaaliluvulla $r = \sqrt{t}$ saadaan kanta $(\mathbf{1}_A, \mathbf{u})$, jossa $\mathbf{u} = (1/r)\mathbf{w}$. Tällöin $\mathbf{u}^2 = \mathbf{1}_A$, joten vektorin $\mathbf{u}$ minimipolynomi on $\mathbf{X}^2 - 1$ ja samalla tavalla kuin vaihtoehdossa 1 nähdään isomorfialauseen avulla, että A on isomorfinen algebran $A_2 = \mathbb{R}[\mathbf{X}]/(\mathbf{X}^2 - 1)$ kanssa.

Vaihtoehto 3: $t < 0$. Tällöin jakamalla positiivisella reaaliluvulla $r = \sqrt{-t}$ saadaan kanta $(\mathbf{1}_A, \mathbf{u})$, jossa $\mathbf{u} = (1/r)\mathbf{w}$. Tällöin $\mathbf{u}^2 = -\mathbf{1}_A$, joten vektorin $\mathbf{u}$ minimipolynomi on $\mathbf{X}^2 + 1$ ja samalla tavalla kuin yllä nähdään isomorfialauseen avulla, että A on isomorfinen algebran $A_3 = \mathbb{R}[\mathbf{X}]/(\mathbf{X}^2 + 1)$ kanssa.

Mietitään vielä algebraa $A = \mathbb{R} \times \mathbb{R}$, joka on $\mathbb{R}$-vektoriavaruutena $\mathbb{R}^2$ ja renkaana varustettu kertolaskulla "koordinateittain", $(a, b) \cdot (c, d) = (ac, bd)$. 2-ulotteisena $\mathbb{R}$-algebrana A on tämän ja edellisen tehtävän nojalla isomorfinen tasan yhden algebroista A_1, A_2, A_3 kanssa. Kaikilla $(a, b) \in A$ pätee $(a, b)^2 = (a^2, b^2)$, mistä nähdään, että nollasta eroavan vektorin neliö ei ole nolla-alkio. Tästä seuraa, että A ei voi olla isomorfinen A_1:n kanssa. Toisaalta A ei ole kokonaisalue, sillä $(1, 0) \cdot (0, 1) = (0, 0)$. Näin ollen se ei voi olla isomorfinen A_3:n kanssa. Voidaan siis suoraan päätellä, että sen on pakko olla isomorfinen algebran $A_2 = \mathbb{R}[\mathbf{X}]/(\mathbf{X}^2 - 1)$ kanssa. Algebralla A on kanta $((1, 0), (0, 1))$, jonka alkioille $(\mathbf{e}_1, \mathbf{e}_2)$ pätee $\mathbf{e}_i \cdot \mathbf{e}_j = \delta_{ij}$. Etsitään algebrasta A_2 kanta, jolla on sama ominaisuus. Huomataan, että algebrassa A_2 pätee $(\bar{\mathbf{X}} - 1)(\bar{\mathbf{X}} + 1) = \bar{\mathbf{X}}^2 - 1 = \mathbf{0}$, joten ainakin alkioilla $\mathbf{w}_1 = (\bar{\mathbf{X}} - 1)$, $\mathbf{w}_2 = (\bar{\mathbf{X}} + 1)$ on ominaisuus $\mathbf{w}_1\mathbf{w}_2 = \mathbf{0}$. Osoitetaan, että ne muodostavat algebran A_2 kannan. Koska vektoria on kaksi ja A_2 on kaksiulotteinen, riittää näyttää, että jono $(\mathbf{w}_1, \mathbf{w}_2)$ on vapaa. Olkoot $a, b \in \mathbb{R}$. Tällöin

$$a\mathbf{w}_1 + b\mathbf{w}_2 = (a + b)\bar{\mathbf{X}} + (b - a) = \mathbf{0}$$

jos ja vain jos $a+b = b-a = 0$, sillä jono $(1, \bar{\mathbf{X}})$ on algebran A_2 kanta. Näistä helposti saadaan $a = b = 0$, joten jono $(\mathbf{w}_1, \mathbf{w}_2)$ todellakin on vapaa. On siis löydetty kanta $(\mathbf{w}_1, \mathbf{w}_2)$, jonka alkioiden tulo on nolla. Tämä ei kuitenkaan vielä toteuda vaadittuja ominaisuuksia, sillä tämän kannan jokaisen alkion neliö *ei ole* alkio itse, vaan pätee

$$\mathbf{w}_1 = (\bar{\mathbf{X}} - 1)^2 = \bar{\mathbf{X}}^2 - 2\bar{\mathbf{X}} + 1 = 2 - 2\bar{\mathbf{X}} = -2\mathbf{w}_1,$$

$$\mathbf{w}_2 = (\bar{\mathbf{X}} + 1)^2 = \bar{\mathbf{X}}^2 + 2\bar{\mathbf{X}} + 1 = 2\bar{\mathbf{X}} + 2 = 2\mathbf{w}_2.$$

Tästä kuitenkin nähdään, että haluttuun kantaan päästään vain sopivalla normerauksella. Nimittäin valitaan $\mathbf{v}_1 = -(1/\sqrt{2})\mathbf{w}_1 = (1/\sqrt{2})(1-\bar{\mathbf{X}})$, $\mathbf{v}_2 = (1/\sqrt{2})\mathbf{w}_2 = (1/\sqrt{2})(1 + \bar{\mathbf{X}})$. Tällöin kannalla $(\mathbf{v}_1, \ldots, \mathbf{v}_2)$ on vaadittu ominaisuus.

8.* Olkoon $\mathbb{H}$ kompleksisen matriisialgebran $M(2\times 2; \mathbb{C})$ osajoukko, jonka muodostavat muotoa

$$\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}$$

olevat matriisit, missä $z, w \in \mathbb{C}$. Tässä $\bar{z}$ on kompleksiluvun z konjugaatti kuten tehtävässä 2.
a) Osoita, että $\mathbb{H}$ on $\mathbb{R}$-algebra eli on suljettu matriisien yhteenlaskun, kertolaskun, sekä reaaliluvulla kertomisen suhteen. Onko $\mathbb{H}$ myös $\mathbb{C}$-algebra?
b) Olkoon $A \in \mathbb{H}, A \neq 0$. Osoita, että on kääntyvä ja että $A^{-1} \in \mathbb{H}$.
c) Olkoot

$$\mathbf{i} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \mathbf{j} = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Osoita, että $(I_2, \mathbf{i}, \mathbf{j}, \mathbf{k})$ on $\mathbb{R}$-vektoriavaruuden $\mathbb{H}$ kanta. Laske kaikki tulot xy, missä $x, y \in \{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$.

d) Osoita, että yhtälöllä $x^2 + 1 = 0$ on äärettömän monta ratkaisua renkaassa $\mathbb{H}$.

Algebraa $\mathbb{H}$ sanotaan *kvaternioiden algebraksi.*

Ratkaisu: a) Osoitetaan, että $\mathbb{H}$ on suljettu (matriisien) yhteenlaskun, kertolaskun ja $\mathbb{R}$-skalaarikertolaskun suhteen. Olkoot

$$\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}, \begin{bmatrix} z' & w' \\ -\bar{w'} & \bar{z'} \end{bmatrix} \in h$$

ja olkoon $r \in \mathbb{R}$. Tällöin

$$\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} + \begin{bmatrix} z' & w' \\ -\bar{w'} & \bar{z'} \end{bmatrix} = \begin{bmatrix} z+z' & w+w' \\ -\bar{w} - \bar{w'} & \bar{z} + \bar{z'} \end{bmatrix} \in h,$$

$$r \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} = \begin{bmatrix} rz & rw \\ -r\bar{w} & r\bar{z} \end{bmatrix} \in h.$$

Tässä käytetään hyväksi sitä, että $\bar{r} = r$ kaikilla $r \in \mathbb{R}$. Lopuksi

$$\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \begin{bmatrix} z' & w' \\ -\bar{w'} & \bar{z'} \end{bmatrix} = \begin{bmatrix} zz' - w\bar{w'} & zw' + w\bar{z'} \\ -\bar{w}z' - \bar{z}\bar{w'} & -\bar{w}w' + \bar{z}\bar{z'} \end{bmatrix},$$

joka on muotoa

$$\begin{bmatrix} z'' & w'' \\ -\bar{w''} & \bar{z''} \end{bmatrix}$$

kun asetetaan $z'' = zz' - w\bar{w'}, w'' = zw' + w\bar{z'}$. Lisäksi identtinen matriisi I_2 on joukon $\mathbb{H}$ alkio, mikä nähdään, kun asetetaan määritelmässä $z = 1, w = 0$.

Näin ollen $\mathbb{H}$ on matriisialgebran $M(2 \times 2; \mathbb{C})$ alialgebra, kun jälkimmäinen ajatellaan $\mathbb{R}$-algebrana, erityisesti $\mathbb{H}$ on itse $\mathbb{R}$-algebra. $\mathbb{H}$ ei kuitenkaan ole $\mathbb{C}$-algebra, sillä se ei ole suljettu sklaarikertolaskulla kompleksiluvuilla. Esimerkiksi kun yksikkömatriisi I_2 (joka on $\mathbb{H}$:n alkio) kerrotaan imaginääriyksiköllä i, saadaan matriisi

$$\begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix},$$

joka ei ole joukon $\mathbb{H}$ alkio.

b) Osoitetaan, että jokainen $A \in \mathbb{H}, A \neq 0$ on kääntyvä ja A^{-1} on myös algebran $\mathbb{H}$ alkio. Tiedetään, että (2×2)-matriisin käänteismatriisi saadaan kaavalla

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{\det A} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

joka on voimassa aina kun $\det A \neq 0$. Olkoon

$$A = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \in \mathbb{H}$$

Tällöin $\det A = z\bar{z} + w\bar{w} = |z|^2 + |w|^2$, missä $|z|^2 = x^2 + y^2 \geq 0$ on kompleksiluvun $z = x + iy$ *itseisarvo*. Näin ollen kun $A \neq 0$ pätee myös $\det A \neq 0$, joten A kääntyvä. Itse asiassa edellisestä laskusta seuraa jopa, että $\det A$ *on reaaliluku* kun $A \in \mathbb{H}$ (koska kompleksiluvun itseisarvo on reaaliluku). Käänteismatriisille saadaan tämän nojalla kaava

$$A^{-1} = \frac{1}{\det A} \begin{bmatrix} \bar{z} & -w \\ \bar{w} & z \end{bmatrix},$$

missä matriisi

$$\begin{bmatrix} \bar{z} & -w \\ \bar{w} & z \end{bmatrix}$$

helposti nähdään olevan joukon $\mathbb{H}$ alkio. Koska yllä on osoitettu, että $\mathbb{H}$ on suljettu $\mathbb{R}$-skalaarikertolaskun suhteen, tästä seuraa, että A^{-1} on myös $\mathbb{H}$:n alkio.

c) Tässä vaiheessa on kätevää ottaa käyttöön seuraava notaatio. Jokainen joukon $\mathbb{H}$ alkio

$$A = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}$$

määräytyy yksikäsitteisesti ensimmäisen rivinsa alkioista z ja w, joten se on luonnollista samastaa parin (z, w) kanssa. Tällöin $\mathbb{H}$ voidaan tulkita karteesisena tulona $\mathbb{C} \times \mathbb{C} = \mathbb{C}^2$, jossa yhteenlasku ja $\mathbb{R}$-skalaarikertolasku määritellään komponenteittain,

$$(z, w) + (z', w') = (z + z', w + w'),$$
$$r(z, w) = (rz, rw).$$

Kertolasku on tällä tulkinnalla tällöin määritelty kaavalla

$$(z, w) \cdot (z', w') = (zz' - w\bar{w}', zw' + w\bar{z}').$$

Koska $\mathbb{C} = \mathbb{R}^2$, $\mathbb{R}$-vektoriavaruutena $\mathbb{C}^2$ voidaan tulkita luonnollisella tavalla avaruutena $\mathbb{R}^4$. Tästä nähdään, että se on $\mathbb{R}$-vektoriavaruutena 4-ulotteinen ja eräs sen kanta on standardikanta eli jono $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4)$. Tulkinnassa $\mathbb{R}^4 = \mathbb{C}^2$ nämä ovat vektoreita $((1, 0), (0, 1), (i, 0), (0, i))$. Kun tämän kannan kolmas alkio korvataan sen vastavektorilla $-\mathbf{e}_2 = (-i, 0)$ saadaan $\mathbb{R}$-vektoriavaruudelle $\mathbb{C}^2$ kanta, joka

vastaa tasan c)-kohdassa määriteltyä jonoa $(I_2, \mathbf{i}, \mathbf{j}, \mathbf{k})$.

Seuravassa taulukossa esitetään kaikki mahdolliset tulot xy, missä $x, y \in \{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$, nämä saadaan suorilla laskuilla:

	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	I_2	$\mathbf{k}$	$-\mathbf{j}$
$\mathbf{j}$	$-\mathbf{k}$	I_2	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	I_2

d) Olkoon $(z, w) \in Q$, missä $z = x + iy, w = u + iv \in \mathbb{C}$. Tällöin (käytetään samaa notaatiota kuin yllä)

$$(z, w)^2 = (z^2 - |w|^2, zw + \bar{z}w) = (z^2 - |w|^2, w(z + \bar{z})) = -1 = (-1, 0)$$

jos ja vain jos $z^2 - |w|^2 = -1$ ja lisäksi joko $w = 0$ tai $2x = (z + \bar{z}) = 0$. Tässä $|w|^2 = u^2 + v^2 \in \mathbb{R}$. Jos $w = 0$ ensimmäinen ehto $z^2 - |w|^2 = -1$ yksinkertaistuu muotoon $z^2 = -1$, eli $z = \pm i$. Jos taas $w \neq 0$, toisesta ehdosta seuraa, että $x = 0$, jolloin $z = iy$, joten $z^2 = -y^2$. Tässä tapauksessa pätee

$$z^2 - |w|^2 = -y^2 - |w|^2 = -1$$

jos ja vain jos $y^2 + |w|^2 = 1$. Näin ollen yhtälön

$$(z, w)^2 + 1 = 0$$

ratkaisut algebrassa $\mathbb{H}$ ovat tasan sellaiset parit $(z, w) \in \mathbb{H} = \mathbb{C} \times \mathbb{C}$ joille pätee $z = iy$ ja $y^2 + |w|^2 = 1$. Selvästi tällaisia pareja on ääretön määrä - tässä $y \in \mathbb{R}$ voidaan valita mielivaltaisesti väliltä $[-1, 1]$, jolloin $|w|$ määräytyy yksikäsitteisesti.