Algebrans fundamentalsats

Benjamin Andersson

December 2024

Vi ämnar visa följande teorem.

Teorem 1.1 (Algebrans fundamentalsats)**.** *Varje polynom $f(x) \in \mathbb{C}[x]$ av grad n, har precis n (ej nödvändigtvis distinkta) rötter i $\mathbb{C}$. Eller ekvivalent, $\mathbb{C}$ är algebraiskt sluten.*

För att bevisa detta, behöver vi följande två lemma.

Lemma

Lemma 1.2. *Om $p(x) \in \mathbb{R}[x]$ är sådant att $\deg(p(x)) = 2n+1$ för $n \geqslant 1$, d.v.s. vi har ett polynom med reella koefficienter av udda grad, så gäller att $\exists \alpha \in \mathbb{R}$ så att $p(\alpha) = 0$, d.v.s. $p(x)$ har en reell rot.*

Bevis. Notera att $p(x)$ är ett polynom, så kontinuerligt, och att för tillräckligt stora värden på $|x|$ kommer $2n+1$-termen (den "ledande termen") i polynomet att dominera, vilket gör att $p(x)$ antar båda negativa och positiva värden. Så för ett lämpligt val av $[a, b] \subseteq \mathbb{R}$ (sådant att $p(a)$ är negativt och $p(b)$ är positivt) så kommer $p(\alpha) = 0$ för något $\alpha \in [a, b]$, via *satsen om mellanliggande värden.* □

Lemma

Lemma 1.3. *Om $f(x) = x^2 + px + q \in \mathbb{C}[x]$ så ligger alla rötter till $f(x)$ i $\mathbb{C}$. Eller ekvivalent: det finns inga kvadratiska kroppsutvidningar över $\mathbb{C}$.*

Bevis. Först visar vi att påståendena är ekvivalenta. Om alla rötter till kvadratiska polynom ligger i $\mathbb{C}$, så betyder det att alla algebraiska element $\alpha \in K/\mathbb{C}$ för någon ändlig (algebraisk) kroppsutvidgning K sådant att α har kvadratiskt minimalt moniskt polynom, är sådant att $\mathbb{C}(\alpha) = \mathbb{C}$. Det betyder precis att det ej kan finnas α i något K sådant att $[\mathbb{C}(\alpha) : \mathbb{C}] = 2$, eftersom det skulle betyda att $\deg m_{\mathbb{C},\alpha}(x) = 2$, men det i sin tur skull betyda att vi hade ett kvadratiskt polynom som var irreducibelt, men då måste det innehålla en rot som ej är i $\mathbb{C}$.

Å andra sidan, om det inte finns några kvadratiska kroppsutvidningar i $\mathbb{C}$, så betyder det att $f(x) = x^2 + px + q \in \mathbb{C}[x]$ ej kan vara irreducibelt, för då skulle $f(x)$ vara minimalt polynom till dess rötter, $-\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right) - q}$, men då har vi funnit en kvadratisk kroppsutvidning, motsägelse!

För att se att detta stämmer, så räcker det att visa att varje komplext tal $\alpha = a + bi$ är sådant att det finns något $c \in \mathbb{C}$ så att $c^2 = \alpha$. Om vi övergår till polära koordinater får vi att $\alpha = re^{i\theta}$ för något $r \geqslant 0$ och $\theta \in [0, 2\pi)$. Då gäller att $\sqrt{r}e^{\frac{\theta i}{2}}$ är ett sådant c. För att vara explicit, så vill vi hitta $c + di$ så att $(c + di)^2 = a + bi$.

Ta $c = \pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}}$ och $d = \pm\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}$, där vi väljer tecken framför c, d så att cd har samma tecken som b. Till exempel, anta att tecknet framför b är *positivt*, så att vi tar de *positiva* rötterna som c, d. Då har vi att

$$\begin{aligned}(c+di)^2 &= \left(\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}\right)^2 \\ &= \frac{a+\sqrt{a^2+b^2}}{2} + i\sqrt{-a^2+a^2+b^2} + \frac{a-\sqrt{a^2+b^2}}{2} \\ &= a+bi.\end{aligned}$$

Notera nu att för godtyckligt polynom $f(x) = x^2+px+q \in \mathbb{C}[x]$ (eller mer generellt, över karakteristik skild från 2, tror jag) så har vi att

$$\begin{aligned}\left(x+\frac{p}{2}\right)^2 - \left(\frac{p^2}{2}-q\right) &= x^2+px+\frac{p^2}{4}-\frac{p^2}{4}+q \\ &= x^2+px+q \\ &= f(x).\end{aligned}$$

Då $\frac{p^2}{2}-q \in \mathbb{C}[x]$, så finns $\alpha \in \mathbb{C}$ sådant att $\alpha^2 = \frac{p^2}{2}-q$. Men då gäller att $\alpha^2 - \frac{p}{2}$ är sådant att

$$\begin{aligned}f\left(\alpha^2-\frac{p}{2}\right)^2 &= \left(\alpha-\frac{p}{2}+\frac{p}{2}\right) - \left(\frac{p^2}{2}-q\right) \\ &= \alpha^2 - \left(\frac{p^2}{2}-q\right) \\ &= 0.\end{aligned}$$

Men detta visar att för godtyckligt andragradspolynom $f(x) = x^2+px+q \in \mathbb{C}[x]$ så finns ett $\alpha \in \mathbb{C}$ sådant $\alpha^2 - \frac{p}{2} \in \mathbb{C}$ är ett nollställe till $f(x)$. Vi ser då att också $-\alpha - \frac{p}{2} \in \mathbb{C}$ är ett nollställe till $f(x)$, och således följer att alla rötter till ett godtyckligt andragradspolynom över $\mathbb{C}$ är i $\mathbb{C}$, vilket skulle visas. □

Vi återgår nu till 1.1, och ska nu ha de verktygen vi behöver för att kunna visa detta.

Bevis. Vi fortskrider som i [1]. Det räcker att visa att varje polynom $f(x)$ har en rot i $\mathbb{C}[x]$ (eftersom det tillsammans med den euklidiska algoritmen och induktion ger att $f(x)$ måste ha n rötter, givet att $n = \deg f(x)$).

Låt $\tau \in \mathrm{Aut}(\mathbb{C})$ genom komplex konjugering. Om vi antar att $f(x)$ ej har någon rot i $\mathbb{C}$, så påstår vi att inte heller $\overline{f}(x) = \tau f(x)$ kan ha detta (notera här att vi har utökat τ från en automorfi av $\mathbb{C}$ till en ring-isomorfi $\mathbb{C}[x] \to \mathbb{C}[x]$ via linjäritet). För att se detta, låt α vara en rot till $\overline{f}(x)$, så att

$$\begin{aligned}\overline{f}(\alpha) &= \tau f(\alpha) \\ &= 0,\end{aligned}$$

och anta att $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Då gäller att $\alpha^n + \overline{a}_{n-1}\alpha^{n-1} + \ldots + \overline{a}_1\alpha + \overline{a}_0 = 0$. Via grundläggande regler för komplex konjugering ($\overline{a+b} = \overline{a} + \overline{b}$ och $\overline{a^n} = \overline{a}^n$) följer att $\overline{\alpha}$ är en rot till $f(x)$. Notera vidare att $f(x)\overline{f(x)}$ är invariant under komplex konjugering, eftersom

$$\begin{aligned}\tau(f(x)\overline{f}(x)) &= \tau(f(x))\tau(\overline{f}(x)) \\ &= \overline{f(x)}\tau(\tau(f(x))) \\ &= \overline{f(x)}f(x) \\ &= f(x)\overline{f(x)},\end{aligned}$$

där vi använt att $\tau^2 = \mathrm{id}$ och att $\mathbb{C}[x]$ är en kommutativ ring. Det betyder i sin tur att $f(x)\overline{f(x)}$ har reella koefficienter (använd att x^i är en bas för det oändlig-dimensionella $\mathbb{C}$-vektorrummet $\mathbb{C}[x]$), och vidare, notera att om $f(x)\overline{f(x)}$ har en rot så är det antingen en rot av $f(x)$ eller $\overline{f(x)}$; om det förra så är vi klara, om det senare så är det komplexa konjugatet av den roten en rot till $f(x)$. Det ger oss att det räcker att visa att $f(x)\overline{f(x)}$ har en rot i $\mathbb{C}$, men det betyder i sin tur att det räcker att visa att alla *polynom med koefficienter från* $\mathbb{R}$ har en rot i $\mathbb{C}$.

Anta att $\deg(f(x)) = n$ med reella koefficienter, och skriv $n = 2^k m$ för m udda. Vi ämnar visa att $f(x)$ har en rot i $\mathbb{C}$ via induktion över k. Om $k = 0$, så är $f(x)$ *udda*, och då $f(x) \in \mathbb{R}[x]$ följer från 1.2 att $f(x)$ har en rot $\alpha \in \mathbb{R} \subset \mathbb{C}$. Anta nu att $k \geqslant 1$. Låt $\alpha_1, \ldots, \alpha_n$ vara rötter av $f(x)$ (att sådana rötter existerar i någon kroppsutvidgning av $\mathbb{C}$ följer från teorem om existensen av splittringskropp för $f(x)$), och låt $K = \mathbb{R}(\alpha_1, \ldots, \alpha_n, i)$. Vi påstår då att K är en Galois-utvidgning av $\mathbb{R}$ som innehåller $\mathbb{C}$ och rötterna av $f(x)$. Mer precist påstår vi att K är *splittringskroppen* för det reella polynomet $f(x)\overline{f(x)}$. För att se detta, notera att $\mathbb{R}(\alpha_1, \ldots, \alpha_n)$ är splittringskropp för polynomet $f(x)$, och att $\mathbb{R}(i)$ är splitringskropp för $x^2 + 1$, så båda kroppsutvidgningarna är normala, och vidare är alla ändliga kroppsutvidgningar över en kropp av karakteristik 0 (här $\mathbb{R}$) separabla, vilket ger att $\mathbb{R}(\alpha_1, \ldots, \alpha_n)$ och $\mathbb{R}(i)$ är Galois-utvidningar av $\mathbb{R}$. Men det ger att

$$\mathbb{R}(\alpha_1, \ldots, \alpha_n)\mathbb{R}(i) = \mathbb{R}(\alpha_1, \ldots, \alpha_n, i)$$

är Galois.

Det är vidare tydligt att $\mathbb{C} \subseteq K$ och att K innehåller alla rötter till $f(x)$. För godtyckligt $t \in \mathbb{R}$, betrakta nu polynomet

$$L_t(x) = \prod_{1 \leqslant i < j \leqslant n} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)).$$

Om $\sigma \in \mathrm{Gal}(K/\mathbb{R}) = \mathrm{Aut}(K/\mathbb{R})$ är en godtycklig automorfi, notera då att σ måste ta någon rot av α_i till någon annan rot α_ℓ och samma för α_j, så det ger alltså något annat på samma form som en faktor $(x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$, och då alla $1 \leqslant i, j \leqslant n$ är representerade (och σ en automorfi) får vi tillbaka L_t. Notera nu att fixkropp för $\mathrm{Gal}(K/\mathbb{R})$ är precis $\mathbb{R}$, så om vi kan visa att koefficienterna i polynomet $L_t(x)$ fixeras av alla $\sigma \in \mathrm{Gal}(K/\mathbb{R})$ så följer att alla koefficienter är i $\mathbb{R}$, så att $L_t(x) \in \mathbb{R}[x]$. Eftersom vi ser att $\sigma(L_t(x)) = L_t(x)$, så om vi låter $L_t(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ så ger det oss att

$$\begin{aligned}\sigma(L_t(x)) &= x^n + \sigma(a_{n-1})x^{n-1} + \ldots + \sigma(a_1)x + \sigma(a_0) \\ &= x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0,\end{aligned}$$

men då $\{1, x, x^2, \ldots, \}$ är en bas för $K[x]$ sedd som vektorrum följer det att $\sigma(a_i) = a_i$. Då $\mathbb{R}$ är fixkroppen så gäller det att $a_i \in \mathbb{R}$ för $i = 1, \ldots, n$, d.v.s. $L_t(x) \in \mathbb{R}[x]$. För att bestämma *graden* för $L_t(x)$, behöver vi titta på hur många sätt det finns att välja $i, j \in \{1, \ldots, n\}$ så att $i < j$. Men detta är detsamma som att välja ut 2 saker utan ordning från n (eftersom ordningen entydigt bestäms av

vilka två vi väljer ut), d.v.s. vi får att

$$\begin{aligned}\deg(L_t(x)) &= \binom{n}{2} \\ &= \frac{n!}{2!(n-2)!} \\ &= \frac{n(n-1)}{2} \\ &= \frac{2^k m(2^k m-1)}{2} \\ &= 2^{k-1}m(2^k m-1) \\ &= 2^{k-1}(2^k m^2-m) \\ &= 2^{k-1}m'\end{aligned}$$

där nu m' är udda, då $k \geqslant 1$ sådant att $2^k m^2 - m$ är differensen av ett jämnt och ett udda tal, vilket alltid är udda ($2\ell - (2\gamma+1) = 2(\ell-\gamma)-1)$). Vi kan då via induktionsantagandet sluta oss till att $L_t(x)$ har en rot i $\mathbb{C}$. Det ger alltså att för varje $t \in \mathbb{R}$ så måste det finnas $1 \leqslant i < j \leqslant n$ sådant att $\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$. Det finns oändligt många val av t men bara ändligt många i, j, så det medför att det måste (jämför Dirichlets postfacksprincip) finnas något par $i < j$ sådant att det finns *distinkta* $s, t \in \mathbb{R}$ med $s \neq t$ sådant att

$$\alpha_i + \alpha_j + s\alpha_i\alpha_j \in \mathbb{C} \tag{1.1}$$
$$\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}. \tag{1.2}$$

□

Genom att subtrahera 1.1 från 1.2 får vi att $(s-t)\alpha_i\alpha_j \in \mathbb{C}$, och då $\mathbb{C}$ är en kropp är den sluten under kroppsoperationerna addition, subtraktion, multiplikation och division, och eftersom $s - t \neq 0$ så gäller att $\frac{1}{(s-t)} \in \mathbb{C}$ vilket ger att $\frac{1}{(s-t)}(s-t)\alpha_i\alpha_j = \alpha_i\alpha_j \in \mathbb{C}$. Genom att multiplicera 1.2 med $\frac{s}{t}$ och dra bort resultatet från 1.1 får vi att

$$(\alpha_i + \alpha_j) - \frac{s}{t}(\alpha_i + \alpha_j) = \frac{(t-s)(\alpha_i+\alpha_j)}{t} \in \mathbb{C},$$

och om vi då multiplicerar detta med $\frac{t}{(t-s)}$ så får vi att $\alpha_i + \alpha_j \in \mathbb{C}$ (notera att om t eller $s = 0$ så får vi genom att anta [utan förlust av allmängiltighet] att $s = 0$ att dra bort 1.2 från 1.1 $-t\alpha_i\alpha_j \in \mathbb{C} \implies \alpha_i\alpha_j \in \mathbb{C}$, och vi vet då från 1.1 att $\alpha_i + \alpha_j \in \mathbb{C}$).

Om vi då låter $a = \alpha_1 + \alpha_2$ och $b = \alpha_1\alpha_2$ så påstår vi att α_1, α_2 är rötter till $p(x) = x^2 - ax + b$.

För att se detta, notera att

$$\begin{aligned}p(\alpha_1) &= \alpha_1^2 - \alpha_1(\alpha_1+\alpha_2) + \alpha_1\alpha_2 \\ &= 0,\end{aligned}$$

och

$$\begin{aligned}p(\alpha_2) &= \alpha_2^2 - \alpha_2(\alpha_1+\alpha_2) + \alpha_1\alpha_2 \\ &= 0.\end{aligned}$$

Då får vi från 1.3 att $\alpha_i, \alpha_j \in \mathbb{C}$, vilket då α_i för $i = 1, \ldots, n$ var rötter till $f(x)$ medför att $f(x)$ har en komplex rot. Från induktion drar vi slutsatsen att det gäller för $f(x) \in \mathbb{C}[x]$ av godtycklig grad, vilket var vad vi ville visa.

References

[1] David S. Dummit and Richard M. Foote. *Abstract algebra*. 3rd ed. New York: Wiley, 2004.