Álxebra Linear e Multilineal. Grao en Matemáticas. USC.
Lista de exercicios, tema 1. Polinomios.

Problema 1. Determinar un polinomio $p(x) \in \mathbb{C}[x]$ de grao mínimo tal que $x^2+1 \mid p(x)$ e $x^3+1 \mid p(x)-1$.

Solución. Da primeira condición temos que $p(x) = (x^2+1)q(x)$. Da segunda, temos que x^3+1 divide $(x^2+1)q(x)-1$. Polo tanto,

$$(x^2+1)q(x) - 1 = (x^3+1)r(x).$$

Imos amosar agora tres maneiras distintas de resolver o problema a partir de aquí.

(a) A partir da igualdade anterior, podemos aplicar a identidade de Bézout (algoritmo de Euclides xeneralizado), dado que o problema consiste en encontrar polinomios $q(x)$ e $r(x)$ tales que

$$(x^2+1)q(x) - (x^3+1)r(x) = 1,$$

o cal vai ser posible dado que x^2+1 e x^3+1 non teñen ningún factor irredutible en común. Realizando a división euclidiana temos que

$$x^3+1 = (x^2+1)x + (1-x), \quad x^2+1 = (1-x)(-x-1)+2,$$

co cal

$$\begin{aligned} 2 &= x^2+1+(1-x)(x+1) \\ &= x^2+1+((x^3+1)-x(x^2+1))(x+1) \\ &= (x^3+1)(x+1)+(x^2+1)(-x^2-x+1). \end{aligned}$$

Dividindo por 2 e reordeando os termos quédanos que

$$(x^2+1)\cdot\frac{-x^2-x+1}{2} - 1 = (x^3+1)\cdot\frac{-x-1}{2}.$$

Polo tanto, o polinomio buscado é

$$p(x) = \frac{-x^4-x^3-x+1}{2}.$$

Observamos tamén que $q(x)$ (e polo tanto $p(x)$) non pode ter grao menor, dado que calquera outro que cumpra a ecuación sería da forma $\frac{-x^2-x+1}{2} + a(x)\cdot(x^3+1)$, con $a(x) \in K[x]$, e se $a(x) \neq 0$ o polinomio sempre será de grao polo menos 3. Isto proba ademais que o polinomio que achamos é o único de grao 4 que cumpre a condición.

(b) Na ecuación $(x^2+1)q(x) - 1 = (x^3+1)r(x)$, o lado esquerdo ten que se anular nas raíces de $x^3+1 = (x+1)(x^2-x+1) = (x+1)(x+\xi)(x+\bar{\xi})$, con $\xi = \frac{1+\sqrt{-3}}{2}$. Impondo estas condicións, e usando que $\xi^2 = \xi - 1$, resulta que $2q(-1) = 1$, $\xi q(\xi) = 1$ e $\bar{\xi}q(\bar{\xi}) = 1$.

Dado que temos tres condicións, imos comezar buscando un polinomio de grao 2 (tres graos de liberdade). Pomos $q(x) = ax^2+bx+c$. Impondo a condición en ξ e $\bar{\xi}$, temos

$$\xi(b+c) - (a+b) = 1, \quad \bar{\xi}(b+c) - (a+b) = 1.$$

Restando as dúas ecuacións, $(b+c)(\xi-\bar{\xi})=0$, co cal vemos que $b+c=0$, e polo tanto $a+b=-1$. A condición en -1, á súa vez, dinos que $2a-2b+2c=1$. Polo tanto,

$$\begin{aligned} 2a-2b+2c &= 1 \\ b+c &= 0 \\ a+b &= -1. \end{aligned}$$

Isto dinos que $(a,b,c)=(-1/2,-1/2,1/2)$. Polo tanto, $q(x)=\frac{-x^2-x+1}{2}$ e

$$p(x)=\frac{-x^4-x^3-x+1}{2}.$$

Resulta doado comprobar que non existe ningún $q(x)$ de grao 1 que cumpra a condición.

(iii) Por último, podemos escribir

$$(ax^2+bx+c)(x^2+1)-1=(x^3+1)(ax+d)$$

e resolver o sistema de catro ecuacións, obtendo o mesmo resultado e sen usar explicitamente nin a identidade de Bézout nin propiedades sobre os números complexos. Neste caso, observamos tamén que non é posible que $q(x)$ teña grao 1. De ser así,

$$(ax+b)(x^2+1)-1=c(x^3+1).$$

De aquí, $c=a$, $b=0$, $a=0$ e $b-1=c$, que é un sistema incompatible. Polo tanto, o menor polinomio ten grao 4 e é o presentado nos parágrafos anteriores.

Problema 2. Se $p(x)\in\mathbb{Z}[x]$ e $p(r/s)=0$, con $(r,s)=1$, demostrar que $r-s \mid p(1)$ e $r+s \mid p(-1)$.

Solución. Da condición do enunciado, podemos escribir

$$p(x)=\Big(x-\frac{r}{s}\Big)q(x)=\frac{(sx-r)q(x)}{s},$$

onde $q(x)\in\mathbb{Q}[x]$ (só podemos aplicar os resultados de división sobre polinomios en $\mathbb{Q}$, non en $\mathbb{Z}$). Sexa $M\geq 1$ o menor enteiro positivo tal que $Mq(x)\in\mathbb{Z}[x]$, e poñamos $Mq(x)=b_nx^n+b_{n-1}x^{n-1}+\ldots+b_1x+b_0$. Entón,

$$Msp(x)=(sx-r)(b_nx^n+\ldots+b_0),$$

onde tódolos b_i son enteiros. Imos supoñer que $M>1$ e chegar a unha contradición; para iso, consideremos que ten un divisor primo p. Observemos que se p divide a tódolos b_i, entón poderiamos cambiar M por M/p, o cal contradiciría a condición de minimalidade sobre M. Do mesmo xeito p non pode dividir simultaneamente r e s, dado que son coprimos. Supoñamos que $p\nmid s$, sendo o caso no que $p\nmid r$ completamente análogo. Sexa $0\leq k\leq n$ o maior enteiro tal que $p\nmid b_k$. Se $k=n$, entón teriamos que o coeficiente en x^{n+1} é sb_n, que non é múltiplo de p, unha contradición. Máis en xeral, o coeficiente con x^{k+1} é sb_k-rb_{k+1}. Pola definición de k, temos que b_{k+1} é múltiplo de p, e como o coeficiente en x^{k+1} tamén o debe ser, sb_k ten que ser múltiplo de p. Iso, porén, non é posible, dado que por construción tanto s como b_k son relativamente primos con p. Polo tanto, $M=1$ e $q(x)\in\mathbb{Z}[x]$.

Agora as preguntas do enunciado son sinxelas. Avaliando en $x = 1$, temos que $s \cdot p(1) = (s - r)q(1)$, que como $q(1)$ é enteiro, é unha igualdade de números enteiros. Temos que $r - s$ divide $s \cdot p(1)$, pero polo algoritmo de Euclides $(s, r - s) = (r, s) = 1$, o cal $r - s$ divide $p(1)$. Do mesmo xeito, avaliando en $x = -1$, temos que $s \cdot p(-1) = (-s - r)q(-1)$, e novamente temos que $r + s$ divide $s \cdot p(-1)$; como $(s, r + s) = (r, s) = 1$, $r + s$ divide $p(-1)$.

Problema 3. Os seguintes apartados son independentes entre si.

(a) Descompoñer $x^4 + a^2 \in \mathbb{R}[x]$ en factores irredutibles.

(b) Descompoñer $(x + 1)^n + (x - 1)^n \in \mathbb{C}[x]$ en factores lineares.

(c) Demostrar que o polinomio $x^4 - 9x^2 - 18x - 3 \in \mathbb{Q}[x]$ é irredutible. Podemos dicir o mesmo do polinomio $x^4 - 9x^2 - 18x - 9 \in \mathbb{Q}[x]$?

(d) Demostrar que o polinomio $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 \in \mathbb{Q}[x]$ é irredutible.

Solución. (a) Supoñamos sen perda de xeralidade que $a > 0$ (senón, cambiámolo por $-a$), e sexa $\sqrt{a}$ a raíz cadrada positiva de a. Sobre os complexos, as raíces do polinomio son $\zeta_8\sqrt{a}$, $\zeta_8^3\sqrt{a}$, $\zeta_8^5\sqrt{a}$ e $\zeta_8^7\sqrt{a}$, onde ζ_8 é unha raíz oitava primitiva da unidade. En concreto, $\zeta_8 = \frac{\sqrt{2}+i\sqrt{2}}{2}$. Agrupando os factores conxugados, resulta que

$$(x - \zeta_8\sqrt{a})(x - \zeta_8^7\sqrt{a}) = x^2 - \sqrt{2a}x + a$$

e

$$(x - \zeta_8^3\sqrt{a})(x - \zeta_8^5\sqrt{a}) = x^2 + \sqrt{2a}x + a.$$

Polo tanto, para un a xenérico,

$$x^4 + a^2 = (x^2 + \sqrt{|2a|}x + a)(x^2 - \sqrt{|2a|}x + a).$$

(b) Pondo

$$(x + 1)^n = -(x - 1)^n = (e^{\pi i/n})^n(x - 1)^n = (e^{\pi i/n}x - e^{\pi i/n})^n,$$

temos dous números que ao elevalos a n dan o mesmo. Polo tanto, a súa diferenza é unha raíz n-ésima da unidade, é dicir,

$$x + 1 = e^{2\pi ik/n}(e^{\pi i/n}x - e^{\pi i/n}), \quad k = 0, 1, \ldots, n - 1.$$

Illando x, resulta

$$x = \frac{1 + e^{\pi i(2k+1)/n}}{e^{\pi i(2k+1)/n} - 1}, \quad k = 0, 1, \ldots, n - 1.$$

Entón,

$$(x + 1)^n + (x - 1)^n = \prod_{k=0}^{n-1} \Big(x - \frac{1 + e^{\pi i(2k+1)/n}}{e^{\pi i(2k+1)/n} - 1}\Big).$$

(c) Para a primeira parte, a observación clave baséase en que un polinomio con coeficientes enteiros e relativamente primos entre si en $\mathbb{Q}[x]$ é irredutible se e soamente

se é irredutible en $\mathbb{Z}[x]$. Por outro lado, se $f(x) = g(x)h(x)$, podemos escribir $\overline{f(x)}$ para a redución módulo 3, e temos que

$$\overline{f(x)} = \overline{g(x)} \cdot \overline{h(x)}.$$

Neste caso, a redución do polinomio módulo 3 é simplemente x^4, co que de existir unha factorización as correspondentes reducións serían da forma x^i, e en particular o termo independente sería 0. Iso quere dicir que o termo independente de $g(x)$ e de $h(x)$ é múltiplo de 3, e o termo independente do polinomio orixinal sería entón múltiplo de 9, que non é posible.

Para a segunda parte, é suficiente con obxervar que

$$x^4 - 9x^2 - 18x - 9 = (x^2 + 3x + 3)(x^2 - 3x - 3).$$

(d) Como no apartado anterior, é suficiente demostrar que $f(X)$ é irredutible sobre $\mathbb{Z}[x]$. Para iso, basta con encontrar un primo p de maneira que $\bar{f}(x)$ sexa irredutible en $\mathbb{F}_p[x]$. Imos considerar $p = 2$. Como $f(x)$ é de grao 5, se fose reducible necesariamente a súa descomposición ten que contar un factor de grao 1 ou de grao 2. É inmediato comprobar que o polinomio non é divisible nin por x nin por $x + 1$, dado que $\bar{f}(0) = \bar{f}(1) = 1$. Imos comprobar que $\bar{f}(x)$ tampouco é divisible polo único polinomio irredutible de grao 2, $x^2 + x + 1$; se o fose,

$$x^5 + x^4 + x^2 + x + 1 = (x^2 + x + 1)(x^3 + ax^2 + bx + c).$$

Igualando termos, vemos que $a = 0$, $b = 1$ e $c = 0$, pero iso é incompatible coa igualdade de termos independentes. Por tanto, $\bar{f}$ é irredutible en $\mathbb{F}_2[X]$ e tamén en $\mathbb{Q}[x]$.

Problema 4. Un número $\alpha \in \mathbb{C}$ chámase alxébrico se existe un polinomio mónico $p(x) \in \mathbb{Q}[x]$ de maneira que $p(\alpha) = 0$.

(a) Probar que os números $\sqrt{2}, \sqrt{3} + 1, \sqrt[3]{5} - 3, \sqrt{2} + \sqrt{3}$ son alxébricos e encontrar un polinomio con coeficientes racionais do cal sexan ceros.

(b) Demostrar que para todo número alxébrico α existe un único polinomio mónico de grao mínimo $p(x) \in \mathbb{Q}[x]$ de maneira que $p(\alpha) = 0$. Demostrar que calquera outro polinomio $q(x)$ tal que $q(\alpha) = 0$ cumpre que $q(x) = p(x)a(x)$, para algún $a(x) \in \mathbb{Q}[x]$. Para os números do apartado anterior, cal é ese polinomio $p(x)$?

(c) Demostrar que a suma e o produto de elementos alxébricos é un número alxébrico.

Solución. (a) No caso de $\sqrt{2}$ consideramos x^2-2. Para $\alpha = \sqrt{3}+1$, pomos $\alpha-1 = \sqrt{3}$ e elevamos ao cadrado, obtendo $\alpha^2-2\alpha-2 = 0$, co cal o polinomio é x^2-2x-2. Do mesmo xeito, se $\beta = \sqrt[3]{5}-3$, $\beta+3 = \sqrt[3]{5}$ e elevando ao cubo $\beta^3+9\beta^2+27\beta+22 = 0$, co cal o polinomio é $x^3 + 9x^2 + 27x + 22 = 0$. Por último, se $\gamma = \sqrt{2} + \sqrt{3}$, pomos $\gamma - \sqrt{2} = \sqrt{3}$ e elevando ao cadrado temos $\gamma^2 - 1 = 2\sqrt{2}\gamma$; elevando novamente ao cadrado, $\gamma^4 - 10\gamma^2 + 1$, co cal o polinomio buscado é $x^4 - 10x^2 + 1$.

(b) Sexa α un número alxébrico e $p(x)$ un polinomio de grao mínimo con $p(\alpha) = 0$. Sexa $q(x)$ outro polinomio con $q(\alpha) = 0$. En $\mathbb{Q}[x]$ aplicamos o algoritmo da división, e podemos escribir $q(x) = p(x)a(x) + b(x)$, con $b(x)$ de grao menor ao grao de $p(x)$. Avaliando en $x = \alpha$ temos que $q(\alpha) = p(\alpha)a(\alpha) + b(\alpha)$, e como

$q(\alpha) = p(\alpha) = 0$, ten que ser $b(\alpha) = 0$. Polo tanto, $b(x)$ sería un polinomio de grao menor a $p(x)$ que anula α, o cal non é posible.

No caso do apartado anterior, os polinomios que demos son xa os de menor grao. En case tódolos casos é un comprobación rutineira ver que non hai ningún de grao menor; imos traballar o caso de $x^4 - 10x^2 + 1$, que é o menos sinxelo. Para iso, é suficiente ver que o polinomio é irredutible en $\mathbb{Z}$. Como os únicos divisores do termo independente son ± 1 e ningún é unha raíz, non pode haber factores lineais. De haber factores de grao 2, sucedería que

$$(x^4 - 10x^2 + 1) = (x^2 + ax + b)(x^2 + cx + d),$$

con $a, b, c, d \in \mathbb{Z}$. Polo tanto, ou $b = d = 1$ ou $b = d = -1$. Como o termo en x^3 é 0, $a = -c$; considerando o termo en x^2, temos que $b + d - a^2 = -10$, co cal $a^2 = 10 + b + d$. Se $b = d = 1$, $a^2 = 12$; e se $b = d = -1$, entón $a^2 = 8$. En ningún dos casos é posible por tanto ter unha factorización en $\mathbb{Z}[x]$, e iso conclúe o problema.

(c) Hai varias maneiras de demostrar este feito, pero ningunha é realmente sinxela coa teoría que fixemos ata o de agora. Volveremos a esta cuestión no segundo problema para entregar de avaliación continua.