Problemes d'Estructures algebraiques

Aleix Torres i Camps

Jordi Guardia (jordi.guardia-rubies@upc.edu), Anna Rio i Santi Molina
(Martí Oller)

Problema 1. Sigui $d \in \mathbb{Z}$ un enter $d \cong 1 \pmod 4$. Sigui $w = \frac{1}{2}(1+\sqrt{d}) \in \mathbb{C}$. Demostreu que el conjunt $\mathbb{Z}[w] = \{a + bw : a, b \in \mathbb{Z}\}$ és un subanell de $\mathbb{C}$.

Solució. Per demostrar el que ens demanen cal comprovar tres propietats. Veure que conté $1_{\mathbf{C}}$ i que és tancat per la resta surt de la PC, PA i PD. Per comprovar que és tancat per la multiplicació, veiem que $w^2 = \frac{1}{4}(1+\sqrt{d})^2 = [d = 4k+1] = k + \frac{1}{2}(1+\sqrt{4k+1}) = k + w$. Llavors quan multipliquem dos elements de $\mathbb{Z}[w]$ ens queda una part entera i un enter multiplicat per w, així que acaba sent un element de $\mathbb{Z}[w]$. □

Problema 2. Sigui $\zeta = e^{2\pi i/5}$ i considereu el conjunt $\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 : a_i \in \mathbb{Z}\}$. Demostreu que és un subanell de $\mathbb{C}$.

Solució. Està clar que $1_{\mathbb{C}}$ pertany a $\mathbb{Z}[\zeta]$ i que és tancat per la suma. Ara, per veure que és tancat per la suma només cal notar que $\zeta^5 = 1_{\mathbb{C}}$, aleshores quan es multipliquin tots per tots, la màxima potència que surt és 4. □

Problema 3. Demostreu que, donat $\alpha \in \mathbb{Q}$, el conjunt de polinomis que s'anul·len en α és un ideal de $\mathbb{Q}[x]$.

Solució. Sigui A aquest conjunt que volem veure que és un ideal. Els seus elements són multiples de $(x-\alpha)$ o, el que és el mateix, $(x-\alpha)$ els divideix.

Ara, $\forall u, v \in A$ i $\forall \alpha, \beta \in \mathbb{Q}[x]$, tenim que $\alpha u + \beta v$ és divisible per $(x-\alpha)$ perquè tant u com v ho són i tant α com β no afecten. □

Problema 4. Sigui $\mathfrak{a}$ un ideal de l'anell A. Demostreu que $\mathrm{Ann}(\mathfrak{a}) = \{a \in A : ax = 0 \forall x \in \mathfrak{a}\}$ és un ideal d'A. S'anomena *anul·lador* d'$\mathfrak{a}$.

Solució. Ara, $\forall u, v \in \mathrm{Ann}(\mathfrak{a})$ i $\forall \alpha, \beta \in A$, tenim que $\alpha u + \beta v$ quan el multipliquem per qualsevol element de $\mathfrak{a}$, com que la multiplicació és distributiva i commutativa quan fem au i av ens donarà 0_A perquè s'anul·len. Així que la combinació lineal també s'anul·len. □

Problema 5. Un element a d'un anell s'anomena nilpotent si $a^n = 0$ per algun $n \geq 1$. Demostreu que el conjunt de tots els elements nilpotents d'una anell és un ideal. S'anomena *radical* de l'anell.

Solució. Siguin $u, v \in \mathrm{Ann}(\mathfrak{a})$ i $\alpha \in A$. Tenim que $(\alpha u)^n = \alpha^n\, u^n = 0$, per n que fa $u^n = 0$. Ara, si m és l'enter que fa $v^m = 0$, anem a comprovar que $(u+v)^{n+m} = 0$. En efecte:

$$(u+v)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} u^i v^{n+m-i} = \sum_{i=0}^{m} \binom{n+m}{i} u^i v^{n+m-i} + \sum_{i=m}^{m+n} \binom{n+m}{i} u^i v^{n+m-i} =$$

$$= v^m \Big(\sum_{i=0}^{n} \binom{n+m}{i} u^i v^{n-i}\Big) + u^n \sum_{i=n+1}^{m+n} \binom{n+m}{i} u^{i-n} v^{n+m-i} = 0 + 0 = 0$$

□

Problema 6. Demostreu que la suma d'un element nilpotent i una unitat d'una anell és una altra unitat.

Solució. Sigui n l'element nilpotent i k el primer enter positiu tal que $n^k = 0$ i sigui u una unitat de l'anell. Aleshores, considrem la següent equació, la qual simplement prové de les propietats PD, PA, PC per tant, es compleix per tot anell:

$$x^k - 1 = (1 + x)(1 - x + x^2 - \cdots + (-1)^{k-1}x^{k-1})$$

Ara, a la part dreta de l'equació, multipliquem el terme petit per u i el terme gran per u^-1 (es pot fer per associativitat i la propietat distributiva), a més, considerem els seus inversos per la suma, és a dir, canviem de signe tot:

$$1 - x^k = (u + ux)\left(\sum_{i=0}^{k-1}(-1)^{i+1}u^{-1}x^i\right)$$

Ara substituim $x = u^{-1}n$ i ens queda:

$$1 = 1 - u^{-k}n^k = (u + n)(\sum_{i=0}^{k-1}(-1)^{i+1}u^{-i-1}n^i$$

I, per tant, hem trobat que existeix un element tal que multiplicat a $(u + n)$ dona 1. Llavors, $u + n$ és una altra unitat, que és el que volíem veure. □

Problema 7. Siguin $\zeta = e^{2\pi i/5}$ i $k \in \mathbb{Z}$. Considereu l'apliacació:

$$f : \mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]$$
$$f(\sum_i (a_i\zeta^i)) = \sum_i a_i\zeta^{ki}$$

Demostreu que és un morfisme d'anells.

Solució. Clarament envia 1 a 1, perquè no té potencies (de fet envia qualsevol enter a ell mateix).

La suma es comprova amb fàcilment agrupant i separant termes amb la propietat distributiva, associativa i commutativa.

Pel producte, fem la multiplicacio i factoritzem. □

Problema 8. Siguin K un cos i $\alpha \in K$. Considereu l'aplicació:

$$\varphi_\alpha : K[x] \to K$$
$$f \to \varphi_\alpha(f) = f(\alpha)$$

és un morfisme exhaustiu d'anells. Concloeu que $K[x]/(x - \alpha)$ és isomorf a K.

Solució. Que el φ_α envia 1 a 1 està clar. La suma i producte està clar perquè l'evaliació de suma i producte de polinomis és, per definició, el producte i suma de les evaluacions.

L'exhaustivitat es fàcilment comprovable perquè $\forall a \in K$, el polinomi constant $p(x) = a$ està en la seva antiimatge.

Pel primer teorema d'isomorfisme, tenim que $K[x]/\ker f \cong K$, llavors voolem demostrar que $\ker f = (x - \alpha) = \{p(x)(x - \alpha)\}$. Clarament, l'ideal està dins del nucli perquè evaluant a α dona 0. I tot element del nucli, al ser evaluat a α dona 0, per tant, $p(x)$ té un factor α i llavors es divisible per $(x - \alpha)$ i $p(x)$ estarà en l'ideal de $(x - \alpha)$.

Alternativament, i millor, aquesta última inclusió es pot veure definint $q(x) = q(x + \alpha)$ veien que $q(0) = 0$ i, per tant, que no té coeficient constant, treient-lo per factor comú i tornant a p amb $p(x) = q(x - \alpha)$. □

Problema 9. Volem veure que es pot racionalitzar totes les fraccions de la forma

$$\frac{a+b\sqrt[3]{2}+c\sqrt[3]{4}}{d+e\sqrt[3]{2}+f\sqrt[3]{4}},\ a,b,c,d,e,f\in\mathbb{Q}$$

1. Demostreu que l'ideal de $\mathbb{Q}[x]$ generat pel polinomi x^3-2 és maximal.
2. Definiu un epimorfisme entre $\mathbb{Q}[x]$ i $\mathbb{Q}[\sqrt[3]{2}]=\{a+b\sqrt[3]{2}+c\sqrt[3]{4}:a,b,c\in\mathbb{Q}\}$.
3. Concloeu que $\mathbb{Q}[\sqrt[3]{2}]$ és un cos.

Solució.

1. Si volem veure que (x^3-2) és maximal, cal veure que no existeix un polinomi p tal que $(x^3-2)\subsetneq(p)\subsetneq\mathbb{Q}[x]$, perquè tots els ideals de l'anell de polinomis són generats per un element (perquè és principal). Ara bé, com que $(x^3-2)\subsetneq(p)$ implica que $p|x^3-2$ perquè (p) ha de contenir x^3-2. Però com que x^3-2 és irreductible això és impossible i hem acabat. En general, en els anells principals, els ideals generats per elements irreductibles són maximals.
2. Primer de tot, està clar que $\mathbb{Q}[\sqrt[3]{2}]$ és un anell, hereda les operacions típiques tot i que quan es fan potencies terceres torna a 2. Després, que el morfisme φ que agafa un polinimi $p(x)$ de $\mathbb{Q}[x]$ i l'evalua a $\sqrt[3]{2}$ és realment un morfisme (perquè l'1 va a l'1, la suma i el producte es comporten bé). I és exhaustiu perquè amb els polinomis $a+bx+cx^2$ en fem prou. El nucli de φ és $\ker\varphi=(x^3-2)$, perquè el polinomi més petit que conté l'arrel $\sqrt[3]{2}$ és aquest. Llavors, existeix un epimorfisme entre $\mathbb{Q}[x]$ i $\mathbb{Q}[\sqrt[3]{2}]$ tal que el nucle és l'ideal generat per x^3-2.
3. Pel primer teorema d'isomorfisme, tenim que $\mathbb{Q}[\sqrt[3]{2}]\cong\mathbb{Q}/(x^3-2)$, i com que (x^3-2) és maximal implica que el quocient és un cos i per tant, que $\mathbb{Q}[\sqrt[3]{2}]$ és un cos.

Extra: les fraccions de la forma descrita es poden racionalitzar perquè hem vist que tot element de la forma del polinomi de baix té un invers de la mateixa forma, per tant, multiplicant a dalt i a baix per aquest invers tenim que el denominador queda 1. □

Problema 10. *Teorema xinès dels residus.* Dos ideals I,J d'un anell $\mathbb{A}$ es diuen *coprimers* (o *comaximals*) si $I+J=\mathbb{A}$. Sigui $\varphi:\mathbb{A}\to\mathbb{A}/I\times\mathbb{A}/J$ el morfisme que té per components les projeccions canòniques: $\varphi(x)=([x]_I,[x]_J)$. Demostreu que:

1. Si I i J són coprimers aleshores $IJ{=}I\cap J$;

   INDICACIÓ: Existeixen $u\in I$ i $v\in J$ amb $u+v=1$.
2. Si I i J són coprimers aleshores per a tot parell d'elements $a,b\in\mathbb{A}$ existeix un element $x\in\mathbb{A}$ tal que $x\equiv a\pmod I$ i $x\equiv b\pmod J$, i la classe d'aquest element mòdul IJ queda unívocament determinada.
3. φ és exhaustiu si, i només si, I i J són coprimers.
4. Si I i J són coprimers aleshores $\mathbb{A}/IJ\cong\mathbb{A}/I\times\mathbb{A}/J$.

Solució.

1. $\subseteq$) Si tenim una combinació del producte $\sum u_iv_j$ com que, les u_i pertanyen a I, llavors u_iv_j segueix en I i fent la suma segueix en I. Simétricament també pertany a J.

   $\supseteq$) Primer veiem que $\exists u\in I,v\in J$ tal que $u+v=1$, que vé del fet que són coprimers. De fet, és un sí i només sí. Sigui $x\in I\cap J$, llavors $x=x(u+v)=xu+xv$, pel fet de $x\in J$, $u\in I$ i que $x\in I$, $v\in J$, tenim que $xu,xv\in I\cdot J$, llavors la suma també pertany al producte així que x pertany al producte.
2. $x=a+\alpha=b+\beta$, on $\alpha\in I$ i $\beta\in J$, llavors volem $a-b=\beta-\alpha$ que és la resta d'un element de J i un de I, que al ser I i J coprimers es pot fer. Més concretament, utilitzant u i v d'abans. $a-b=(a-b)u+(a-b)v$, per tant, $x=a-(a-b)u=b+(a-b)v$.

   Sigui x' un altre element amb les mateixes congruencies que x, llavors, $x-x'\in I,J$ i, per tant, $x-x'\in I\bigcap J=IJ$, aleshores tenen el mateix módul.

3. $\Longrightarrow$) Com que tot element té antiimatge, fem l'antiimatge de $([0],[1])$ que és un element $\alpha \in \mathbb{A}$ tal que α pertany a I perquè la seva clase és el 0 i existeix un element de J β tal que $\alpha = 1 + \beta$, per tant, l'1 es pot escriure com suma d'un element d'I i un element de J. Això és suficient per veure que I i J són coprimers (com hem dit a l'apartat 1), perquè $\forall x \in \mathbb{A}$ complex que $x\alpha - x\beta = x$ i el primer element és de I i el segon de J. Així que hem vist que I i J són comprimers.

   $\Longleftarrow$) Suposem que I i J són coprimers i agafem un element (a, b) qualsevol de l'espai de sortida de φ, ara busquem un element $x \in \mathbb{A}$ tal que $x \equiv a \pmod{I}$ i $x \equiv b \pmod{J}$ que és exactament l'apartat anterior, per tant, φ és exhaustiva.

4. Anem a veure que $\ker \varphi = IJ$, si un element té per imatge $([0]_I, [0]_J)$ vol dir que pertany a I i a J a la vegada. Per tant, $\ker I \cap J = IJ$ per l'apartat 1. Ara, pel primer teorema d'isomorfisme tenim el que ens demanen: $\mathbb{A}/IJ \cong \mathbb{A}/I \times \mathbb{A}/J$.

□

Problema 11. Demostreu que un ideal $\mathfrak{p}$ és primer si, i només si, $IJ \subseteq \mathfrak{p} \iff I$ o $J \subseteq \mathfrak{p}$, per a tot parell d'ideals I, J.

Solució. Suposem $\mathfrak{p}$ és primer.
$\Longleftarrow$) Si $I \subset \mathfrak{p} \implies IJ \subset \mathfrak{p}$, amb J igual.

$\Longrightarrow$) Suposem que $IJ \subseteq \mathfrak{p}$ i suposem que ni I ni J estan dintre de $\mathfrak{p}$. Llavors existeix $a \in I \setminus \mathfrak{p}$ i $b \in I \setminus \mathfrak{p}$. Però llavors, $ab \in IJ \subseteq \mathfrak{p}$, però per $\mathfrak{p}$ primer tenim que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, que contradiu la primera suposició, per tant, o $I \subseteq \mathfrak{p}$ o $j \subseteq \mathfrak{p}$.

Ara suposem que tenim un ideal $\mathfrak{p}$ tal que compleix la segona condició. Aleshores $\forall ab \in \mathfrak{p}$ com que alemenys $a \in (a)$ i $b \in (b)$ es compleix que $(a)(b) \subseteq \mathfrak{p}$ per tant, o bé $(a) \subset \mathfrak{p}$, o bé $(b) \subseteq \mathfrak{p}$. Llavors, com son els principals, això es pot traduir com: o bé a, o bé b pertanyen a $\mathfrak{p}$. □

Problema 12. Sigui $I \subset \mathbb{A}$ un ideal d'una anell $\mathbb{A}$.

1. Comproveu que $I[X] = \{\sum a_i X^i : a_i \in I\}$ és un ideal de l'anell de polinomis $\mathbb{A}[X]$.
2. Demostreu que I és primer si, i només si, $I[X]$ també ho és, però que tant si I és maximal com si no, $I[X]$ no ho és mai.
3. Demostreu que $\mathbb{A}[X]/I[X] \simeq (\mathbb{A}/I)[X]$.

Solució.

1. És tancat per la suma perquè es treu factor comú de cada X^i i I és tancap per la suma i si multipliques per un altre polinomi com tots els termes tenen un element de I, cada un d'ells pertany a I i la suma d'ells també i, per tant, $I[X]$ és un ideal.
2. Es pot fer a partir de l'apartat 3, per tant, suposem que l'apartat 3 està demostrat. Ara, per $(x) + I[x]$.
3. Ens definim $\varphi : A[x] \to (A/I)[x]$, que envia $\sum_n a_n X^n$ a $\sum_n \bar{a_n} X^n$. Clarament és exhaustiu perquè recull totes les classes. Ara $\ker \varphi = I[x]$, perquè és la classe del 0. I, pel primer teorema d'isomorfisme, $A[x]/I[x] \simeq (A/I)[x]$.

□

Problema 13. Un anell *local* és un anell que té un únic ideal maximal. Sigui $I \subseteq \mathbb{A}$ un ideal propi. Demostreu que:

1. Si $\mathbb{A} \setminus I \subseteq \mathbb{A}^*$ aleshores $\mathbb{A}$ és local i I és el seu ideal maximal.
2. Si I és maximal i $1 + I = \{1 + x : x \in I\} \subseteq \mathbb{A}^*$ aleshores $\mathbb{A}$ és local.

Solució.

1. Anem a veure que I és maximal. Suposem que existeix J tal que $\mathbb{A} \subsetneq J \subsetneq I$, llavors existeix $x \in J \setminus I \subseteq \mathbb{A} \setminus I \subset \mathbb{A}^*$. Llavors x és ínvertible i per tant, $J = \mathbb{A}$ perquè al multiplicar pel seu invers donaria 1 i a partir de 1, genera tot l'anell.

   Anem a veure que $\mathbb{A}$ és local. Sigui J un altre ideal maximal. Per tant, $x \in J \setminus I \subset \mathbb{A} \setminus I \subset \mathbb{A}^*$ i,igual que abans, $J = \mathbb{A}$, per tant no és maximal sino el total.

2. Suposem I maximal i que $1 + I \subset \mathbb{A}^*$, anem a veure que $\mathbb{A}$ és local fent servir l'apartat anterior. Sigui $x \in \mathbb{A} \setminus I$, llavors l'ideal $I + (x)$ és el total, perquè inclou sense igualtat a I però aquest és maximal. Llavors, qualsevol element d'$\mathbb{A}$ es pot posar com a suma d'un element de I i un de (x), com $1 = v + ux$ llavors, $xu = 1 - v \in 1 + I \subset A^*$, llavors x és invertible i, per tant $A \setminus I \subset \mathbb{A}^*$ i per l'apartat anterior, $\mathbb{A}$ és local.

□

Problema 14. Demostreu que tot domini d'integritat finit és un cos. Deduïu que en un anell finit tot ideal primer és maximal.

Problema 15. Sigui $\mathbb{A}$ un anell factorial. Siguin $u, v \in \mathbb{A}$ amb $\gcd(u, v)$=1. Demostreu que si $uv = a^n$ amb $a \in \mathbb{A}$ aleshores existeixen $\alpha, \beta \in \mathbb{A}$ tals que $u \sim \alpha^n$, $v \sim \beta^n$ i $\alpha^n \beta^n = a^n$.

Problema 16. Sigui d un enter lliure de quadrats amb $d \equiv 2, 3 \pmod 4$. Demostreu que l'anell $\mathbb{Z}[\sqrt{-d}]$ no és factorial.

INDICACIÓ: Demostreu que 2 és irreductible però no és primer.

Problema 17. Demostreu que els anells següents són euclidians amb les normes donades:

1. Els enters $\mathbb{Z}$, on $\delta(n)$ és el nombre de dígits en la representació en base 2 de $|n|$ (per exemple, $\delta(-6) = 3$ ja que 6 és 110 en base binària).
2. L'anell $\mathbb{Q}[X]$, on $\delta(f) = 2^{\deg f}$.
3. L'anell $\mathbb{Q}[[X]]$, on $\delta(\sum_{i=0}^{\infty} a_i X^i)$ és el i més petit tal que $a_i \neq 0$.

Problema 18. *Enters de Gauss.* Comproveu que l'anell $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ és euclidià amb la norma definida com $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$.

Solució. Que és un anell es pot veure comprovant que és un subanell de $\mathbb{C}$, ja que conté l'1, si restem dos element de $\mathbb{Z}[i]$ agrupant termes ens quedem en el mateix conjunt i quan multipliquem dos element, com que $i^2 = -1$ ens quedem a l'anell $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

Comencem reduint-nos al cas que volguem dividir $y = a + bi \in \mathbb{Z}[i]$ amb un $x \in \mathbb{N}$, utilitzant la divisió en els enters. Llavors, fem la divisió d'a i b entre x, però volem la condició que els residus en valor absolut siguin menors que $\frac{x}{2}$. Això es pot fer perquè en el cas que el residu fos entre $\frac{x}{2}$ i x el que podem fer és restar x. Aleshores, podem escriure $a = q_1 x + r_1$ i $b = q_2 x + r_2$, amb $|r_1||r_2| \leq \frac{x}{2}$. Llavors ens queda: $a + bi = (q_1 + q_2 i)x + (r_1 + r_2 i) = qx + r$, i tenim que $N(r) = r_1^2 + r_2^2 \leq \frac{x^2}{4} + \frac{x^2}{4} < x^2 = N(x)$.

En el cas general, volem dividir y entre x, però en comtes d'això dividim $y\bar{x}$ per $x\bar{x} = N(x)$, llavors és un natural. Pel cas anterior podem fer-ho: $y\bar{x} = qN(x) + r$, $N(r) < N(x)^2 = x^2\bar{x}^2$, llavors fem $r = y\bar{x} - qx\bar{x} = (y - qx)\bar{x} = r_0\bar{x}$, per tant $N(r_0) = N(r)N(\bar{x})^{-1} < N(x)^2 N(\bar{x})^{-1} = N(x)N(\bar{x})N(\bar{x})^{-1} = N(x)$. Retornant, $y = qx + r_0$, perquè $r_0 = y - qx$, i, per tant, hem dividit y entre x. □

Problema 19. Siguin $p \equiv 3 \pmod 4$ un nombre primer. Demostreu que no existeix un enter de Gauss de norma p.

Solució. Normalment, el 2 es deixa de banda. Llavors, anem a veure que si un primer compleix que existeix x tal que $p = N(x)$ aleshores $p \equiv 1(4)$ i per tant, per contrarecíproc, si tenim un $p' \equiv 3(4)$ no pot existir un x tal que $p = N(x)$. Ara, com p és la norma d'un cert enter de Gauss $x = a + bi$, tenim: $p = a^2 + b^2$, sense perdua

de generalitat, suposem $a = 2n$ i $b = 2m + 1$ (al revés també funciona), llavors $p = 4n^2 + 4m^2 + 4m + 1 \equiv 1(4)$. □

Problema 20. Sigui $p \equiv 1 \pmod 4$ un nombre primer. Demostreu que existeix un enter de Gauss de norma p.

INDICACIÓ: Sigui $u \in \mathbb{Z}$ un enter tal que $u^2 \equiv -1 \pmod p$ (per què existeix?). Agafeu tots els enters de la forma $a + bu$ amb $0 \leq a, b < \sqrt{p}$, demostreu que n'hi ha dos que són congruents mòdul p i considereu la seva diferència.

ALTERNATIVA: amb el mateix u d'abans considereu $\gcd(u + i, p)$ a $\mathbb{Z}[i]$.

Solució. Anem a veure que si $p \equiv 1(4)$ llavors existeix un x tal que $p = N(x)$.

Primer fet $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} =< \alpha >$, perquè és un cos cíclic (amb ordre $p-1$), per tant, podem trobar un generador les potencies del qual donen tots els elements. Llavors sigui $u = \alpha^{\frac{p-1}{4}}$, si l'elevem a la quarta tenim $\alpha^{p-1} \equiv 1(p)$ (per ser $p-1$ l'ordre del cos). Llavors si només l'elevem al quadrat, tenim que $u^2 \equiv 1, -1(p)$, però pel fet que l'ordre és p només pot ser -1, llavors, existeix un $u \leq p-1$ tal que $u^2 \equiv -1(p)$.

Agafem $u + i \in \mathbb{Z}[i]$ i llavors $N(u+i)u^2 + 1 \equiv 0(p)$. Notem que $u^2 + 1 \leq (p-1)^2 + 1 = p^2 - 2p < p^2$. Ara fem $(p) + (u + i)$ això és un ideal i com és principal, la suma és un generador (γ). Llavors $\gamma | p, u + 1$, llavors $N(\gamma)|N(p) = p^2$ i $N(\gamma)|N(u+1) < p^2$. □

Problema 21. Comproveu que els elements de $\mathbb{Z}[i]$ següents són primers:

1. $\pi_2 = 1 + i$ és un primer de norma 2.
2. Per a cada primer enter $p \equiv 1 \pmod 4$ hi ha dos primers diferents (no associats) conjugats: $\pi_p = a + bi$ i $\bar{\pi_p} = a - bi$, que tenen norma p;
3. Tot primer enter $q \equiv 1 \pmod 4$ és també un primer a $\mathbb{Z}[i]$, de norma q^2,

i que tot primer de $\mathbb{Z}[i]$ és associat d'algun d'ells.

Problema 22. Trobeu la factorització en primers de $2067 + 312i$ a $\mathbb{Z}[i]$.

Problemes complementaris

Problema 23. Comproveu que el conjunt $\mathcal{P}(X)$ de les parts d'un conjunt X, amb la "suma"definida com la *diferència simètrica* $A + B := A \triangle B = (A \bigcup B)$ i el "producte"definit com la intersecció $A \cdot B = A \bigcap B$ és un anell commutatiu.

Problema 24. Siguin I, J dos ideals d'un anell A. Demostreu que els conjunts:

$$I + J = \{a + b : a \in I, b \in J\}$$
$$IJ = A\langle ab : a \in I, b \in J\rangle$$

són ideals d'A. Doneu un exemple en el qual $I \bigcup J$ no sigui un ideal.

Problema 25. Els ideals $I_1, \cdots, I_k$ d'un anell $\mathbb{A}$ es diuen coprimers si $\sum I_i = \mathbb{A}$ i coprimers dos a dos si $I_i + I_j = \mathbb{A}$ per a tot $i \neq j$. Sigui $\varphi : \mathbb{A} \to \prod \mathbb{A}/I_i$ l'homeomorfisme que té per components les proheccions canòniques. Demostreu que:

1. si $I_1, \ldots, I_k$ són coprimers dos a dos aleshores cada I_i és coprimer amb $\prod_{j \neq i} I_j$;
2. si $I_1, \ldots, I_k$ són coprimers dos a dos aleshores $\prod I_i = \bigcap I_i$;
3. si els I_i són coprimers dos a dos alehsores, donats elements $a_i \in \mathbb{A}$ existeix un element $x \in \mathbb{A}$ tal que $x \equiv a_i \pmod{I_i}$ per a tot i, i aquest element queda unívocament determinat llevat elements de $\prod I_i$.
4. φ és exhaustiu si, i només si, els I_i són coprimers dos a dos;

5. si els I_i són coprimers dos a dos aleshores $\mathbb{A}/\prod I_i \simeq \prod \mathbb{A}/I_i$.

Enuncieu i demostreu un resultat anàleg al del punt 2 que valgui per a ideals I_i, arbitraris.

Problema 26. *Teorema xinès a* $\mathbb{Z}$. Siguin $n_1, \cdots, n_k$ enteres positius coprimers dos a dos; o sigui $\gcd(n_1, n_2)=1$ per a tot $i \neq j$. Donats k enters $a_1, \cdots, a_k$, demostreu que existeix un enter $x \in \mathbb{Z}$ tal que $x \equiv a_i \pmod{n_i}$ per a tot i, i que aquest enter està unívocament determinat mòdul el producte $n_1 n_2 \cdots n_k$. Proveu que aquest x es pot expressar com

$$x = \sum_{i=1}^{k} a_i M_i N_i$$

on $N_i = N/n_i$ i M_i és un enter tal que $M_i N_i + m_i n_i = 1$, amb $m_i \in \mathbb{Z}$.

Problema 27. Determineu les unitats de l'anell $K[[x]]$ de sèries de potències amb coeficients en un cos K. Descriviu el cos de fraccions d'aquest anell.

Problema 28. Sigui $\mathbb{A}$ un anell commutatiu. Un element $e \in \mathbb{A}$ es *idempotent* si $e^2 = e$. Dos idempotents e_1, e_2 es diuen *ortogonals* si $e_1 e_2 = 0$.

1. Demostreu que si e és un idempotent aleshores $1 - e$ també ho ésm i tots dos són ortogonals.
2. Sigui e un idempotent. Demostreu que l'ideal principal $\langle e \rangle = e\mathbb{A}$ és un anell amb les mateixes operacions de $\mathbb{A}$ està generat per algun idempotent.
3. Demostreu que tot ideal principal de $\mathbb{A}$ que sigui també un anell amb les operacions de $\mathbb{A}$ està generat per algun idempotent.
4. Comproveu que, al producte cartesià $\mathbb{A}_1 \times \mathbb{A}_2$ de dos anells, els elements (1,0) i (0,1) són idempotents ortogonals.
5. Demostreu que dos idempotents e_1, e_2 amb $e_1 + e_2 = 1$ indueixen un isomorfisme d'anells $\mathbb{A} \simeq e_1\mathbb{A} \times e_2\mathbb{A}$.
6. Trobeu tots els idempotents de $\mathbb{Z}/60\mathbb{Z}$ i doneu totes les descomposicions d'aquest anell com a producte cartesià de dos anells, llevat d'isomorfisme.
7. Enuncieu un resultat que relacioni les descomposicipns $\simeq \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$ d'un anell com a producte cartesià d'anells amb idempotents ortogonals de l'anell.

Problema 29. Demostreu que el radical d'un anell és la intersecció de tots els ideals primers de l'anell.

Problema 30. *Radical d'un ideal.* Sigui $I \subseteq \mathbb{A}$ un ideal. El seu radical es defineix com

$$\mathrm{Rad}(I) = \{a \in \mathbb{A} : \exists n \geq 1, a^n \in I\}$$

1. Comproveu que $\mathrm{Rad}(I)$ és un ideal.
2. Calculeu $\mathrm{Rad}(n\mathbb{Z})$ a l'anell $\mathbb{Z}$.
3. Demostreu que:
   (a) $I \subseteq R(I)$;
   (b) $\mathrm{Rad}(\mathrm{Rad}(I))=\mathrm{Rad}(I)$;
   (c) $\mathrm{Rad}(I \bigcap J)=\mathrm{Rad}(I) \bigcap \mathrm{Rad}(J)$;
   (d) $\mathrm{Rad}(I + J)=\mathrm{Rad}(\mathrm{Rad}(I)+\mathrm{Rad}(J))$;
   (e) $\mathrm{Rad}(I^n)=\mathrm{Rad}(I)$;
   (f) $\mathrm{Rad}(I)=\mathbb{A} \iff I = \mathbb{A}$;
   (g) si $\mathfrak{p}$ és primer, $\mathrm{Rad}(\mathfrak{p}) = \mathfrak{p}$.

Problema 31. Sigui $\mathbb{A}$ un anell íntegre i $\mathbb{K}$ el seu cos de fraccions. Sigui $\mathfrak{p} \subset \mathbb{A}$ un ideal primer.
Demostreu que:

1. $\mathbb{A}_\mathfrak{p} := \{\frac{a}{b} : a, b \in \mathbb{A}, b \notin \mathfrak{p}\} \subseteq K$ és un subanell de $\mathbb{K}$ que conté a $\mathbb{A}$;
2. $\mathfrak{m}_\mathfrak{p} := \{\frac{a}{b} \in \mathbb{A}_\mathfrak{p} : a \in \mathfrak{p}\} \subseteq \mathbb{A}_\mathfrak{p}$ és l'ideal maximal de $\mathbb{A}_\mathfrak{p}$;
3. $\mathbb{A} = \bigcap_\mathfrak{m} \mathbb{A}_\mathfrak{m}$ on la intersecció es fa sobre tots els ideals maximals $\mathfrak{m}$ de $\mathbb{A}$.