EPFL - Printemps 2025 | Prof. Zs. Patakfalvi
Anneaux et Corps | **Exercices**
Solutions 5

Exercice 1.
Entiers de Gauss.

1. Comme vu en cours, l'anneau $\mathbb{Z}[i]$ est euclidien avec $N(a+ib) = |a+ib|^2$. Pour $a, b \in \mathbb{Z}[i], a \neq 0$ on appelle une égalité de la forme $b = aq + r$, avec $q, r \in \mathbb{Z}[i]$ et $N(r) < N(a)$ une division avec reste. Effectuer la division avec reste de $5 + 5i$ par $4 + 2i$ et montrer que les quotients et restes de la division dans $\mathbb{Z}[i]$ ne sont pas uniques.

2. Les entiers de Gauss $2, 3$ et 5 sont-ils irréductibles dans $\mathbb{Z}[i]$? Et $2i$ et $2 - 3i$?

3. Montrer que le quotient $\mathbb{Z}[i]/(3)$ est un corps de cardinalité 9.

4. Soit p un nombre premier. Montrer que les énoncés suivants sont équivalents.

   (a) L'entier p n'est pas irréductible dans $\mathbb{Z}[i]$.
   (b) Il existe $a, b \in \mathbb{Z}$ avec $p = a^2 + b^2$.
   (c) ($\star$) $p = 2$ ou alors $p \equiv 1 \mod 4$.

Solution.

1. We first do this division in $\mathbb{C}$. There, we obtain that

$$\frac{(5+5i)}{(4+2i)} = \frac{(5+5i)(-4+2i)}{(4+2i)(-4+2i)} = \frac{3}{2} + \frac{1}{2}i.$$

   By either rounding up or down both the real and imaginary part, we find the closest elements in $\mathbb{Z}[i]$ to be the quotients $1, 2, 1+i, 2+i$. The division by these with rest are

   - $(5+5i) = 1 \cdot (4+2i) + (1+3i)$
   - $(5+5i) = 2 \cdot (4+2i) + (-3+i)$
   - $(5+5i) = (1+i) \cdot (4+2i) + (3-i)$
   - $(5+5i) = (2+i) \cdot (4+2i) + (-1-3i)$

   Remark that we need to take the closest elements in $\mathbb{Z}[i]$ to $\frac{3}{2} + \frac{1}{2}i \in \mathbb{C}$ as otherwise the norm of the rest would exceed the norm of $4+2i$, which is a contradiction. In all of the above cases, this is satisfied. This also shows that the quotent and rest of the euclidean division are not unique.

2. We have

   - $2 = (1+i)(1-i)$ and since $1+i, 1-i \notin (\mathbb{Z}[i])^\times$ it follows that 2 is not irreducible. On note que *en tant qu'idéaux* $(2) = (1+i)^2$.
   - Assume that $3 = x \cdot y$, with $x, y \in \mathbb{Z}[i]$. Then $9 = N(xy) = N(x)N(y)$, so both $N(x)$ and $N(y)$ divide 9. This is possible if $N(x), N(y) \in \{1, 3, 9\}$. If $N(x) = 1$, then x is a unit. If $N(x) = 9$, then $N(y) = 1$ and y is a unit. If $N(x) = 3$, with $x = a + ib$ for $a, b \in \mathbb{Z}$, then $N(x) = a^2 + b^2$, but for natural numbers a and b this is impossible. So $N(x) \neq 3$, and the only way to write 3 as a product of two elements x, y in $\mathbb{Z}[i]$ is if either of them is a unit, which means that 3 is irreducible.
   - $5 = (2+i)(2-i)$ is not irreducible, as both factors are not units.

- $2i = (1+i)^2$ is not irreducible, as $1+i$ is not a unit.
- Since $N(2-3i) = 13$ is irreducible in $\mathbb{Z}$, it follows that $2-3i$ is irreducible in $\mathbb{Z}[i]$.

  Remarque. Comme $\mathbb{Z}[i]$ est euclidien, donc principal, donc *factoriel*, un élément est irréductible si et seulement si l'idéal associé est premier. Ainsi pour $a+bi \in \mathbb{Z}[i]$ le quotient

  $$\mathbb{Z}[t]/(t^2+1, a+bt)$$

  est intègre si et seulement si $a+bi$ est irréductible.

3. We note that $\mathbb{Z}[i]$ is Euclidean by Example 3.7.4, from which it follows that $\mathbb{Z}[i]$ is principal. The Proposition 3.6.3 then states that since 3 is irreducible in $\mathbb{Z}[i]$, the ideal (3) is maximal in $\mathbb{Z}[i]$. It follows that $\mathbb{Z}[i]/(3)$ is a field.

   Comme

   $$\mathbb{Z}[i]/(3) \cong \mathbb{F}_3[t](t^2+1)$$

   c'est un $\mathbb{F}_3$-espace vectoriel de dimension 2, donc de cardinalité 9.

4. - On montre que $(a) \implies (b)$. Vu que p n'est pas irréductible, on peut écrire $p = xy$ avec x et y non-inversibles (en donc pas de norme 1). On a alors que $p^2 = N(p) = N(x)N(y)$ et donc $N(x), N(y) \in \{1, p, p^2\}$. Vu que $N(x)$ et $N(y)$ ne valent pas 1, ils ne peuvent pas valoir p^2 non plus, et donc $N(x) = N(y) = p$. Si l'on écrit $x = a+bi$, alors $p = a^2+b^2$.
   - On montre que $(b) \implies (a)$. Si $p = a^2+b^2$, alors $p = (a+bi)(a-bi)$. Vu que $a \pm bi$ n'est pas inversible (sa norme vaut p), on en déduit que p n'est pas irreductible dans $\mathbb{Z}[i]$.
   - On montre que $(a) \implies (c)$. Supposons $p \neq 2$, et montrons que 4 divise $p-1$. Vu que p n'est pas irréductible dans $\mathbb{Z}[i]$, l'ideal (p) ne peut pas être intègre. Ainsi,

     $$\mathbb{F}_p[t]/(t^2+1) \cong \mathbb{Z}[i]/(p)$$

     n'est pas intègre, et donc en particulier t^2+1 n'est pas premier dans $\mathbb{F}_p[t]$ (et donc pas irreductible, vu que $\mathbb{F}_p[t]$ est factoriel). Ainsi, il existe une race $a \in \mathbb{F}_p$ de t^2+1, et donc $a^4 = 1$. Comme $p \neq 2$, on a que $a^2 \neq 1$, et donc a est d'ordre 4 dans le groupe multiplicatif $\mathbb{F}_p^\times$, qui est d'ordre $p-1$. Par le théorpme de Lagrange, on en déduit que 4 divise $p-1$.
   - On montre que $(c) \implies (a)$. Par le même argument que précédemment, il suffit de montrer que t^2+1 n'est pas irréductible dans $\mathbb{F}_[t]$ (et donc que t^2+1 admet une racine dans $\mathbb{F}_p$). Si $p = 2$, c'est immédiat ($1^2+1 = 2 = 0$). Supposons donc que 4 divise $p-1$. Vu que $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, il existe un élément a d'ordre 4 dans $\mathbb{F}_p^\times$. Vu que $a^2 \neq 1$, on a forcément que $a^2 = -1$, et donc a et bel et bien une racine de t^2+1.

Exercice 2.
Entiers d'Eisenstein. Soit $\omega = e^{\frac{2\pi i}{3}}$ et $\mathbb{Z}[\omega]$ l'anneau des entiers d'Eisenstein.

1. Montrer que $N(a+b\omega) = a^2-ab+b^2$ coïncide avec le module au carré dans le plan complexe de $a+b\omega$.

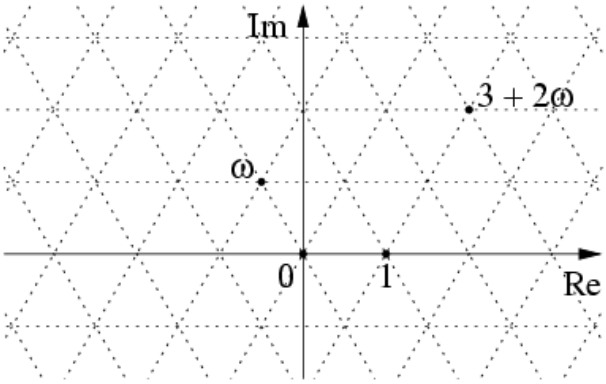
2. Montrer que $N(a+b\omega) = a^2-ab+b^2$ munit $\mathbb{Z}[\omega]$ d'une fonction euclidienne. On pourra par exemple montrer que le point milieu d'une maille du réseau $(a+b\omega)$ se trouve à une distance strictement plus petite que $\sqrt{N(a+b\omega)}$ de chacun des quatre sommets de cette maille.

3. Trouver les éléments inversibles de $\mathbb{Z}[\omega]$ (quelle est leur norme?).

Solution.

1. On the one hand, we have $\mid a+b\omega \mid^2 = (a+b\omega)(a+b\bar{\omega}) = a^2 + ab(\omega+\bar{\omega}) + b^2\omega\bar{\omega}$. On the other hand, we see that both $\omega = e^{\frac{2\pi i}{3}}$ and its complex conjugate $\bar{\omega} = e^{-\frac{2\pi i}{3}}$ are roots of the polynomial $z^3 - 1 = 0$. Since $z^3 - 1 = (z-1)(z^2+z+1)$, both ω and $\bar{\omega}$ are roots of the polynomial (z^2+z+1) and therefore $(z^2+z+1) = (z-\omega)(z-\bar{\omega}) = z^2 - (\omega+\bar{\omega})z + \omega\bar{\omega}$, from which it follows by comparing coefficients that $\omega + \bar{\omega} = -1$ and $\omega\bar{\omega} = 1$. Therefore, $\mid a+b\omega \mid^2 = a^2 - ab + b^2 = N(a+b\omega)$.

2. La norme au carré étant toujours positive, la formule définissant N montre que cette norme prend des valeurs entières. Pour montrer qu'il s'agit d'une fonction euclidienne on procède comme pour les entiers de Gauss. Soit $a+b\omega$ un entier d'Eisenstein et $(a+b\omega)$ l'idéal principal correspondant. Cet idéal est un réseau dans $\mathbb{Z}[\omega]$. Voici une illustration tirée de Wikipedia de $\mathbb{Z}[\omega]$:



   La maille fondamentale de ce réseau est un losange de côté 1 dont les sommets sont par exemples $0, 1, \omega$ et $1+\omega$, ce dernier étant aussi de norme $1 - 1 + 1 = 1$. Ainsi la petite diagonale est de longueur 1 et la grande est de longueur $\sqrt{3} = \sqrt{N(1-\omega)}$.

   L'idéal $(a+b\omega)$ est donc obtenu à partir du réseau ci-dessus par une dilatation d'un facteur $\sqrt{N(a+b\omega)}$ et rotation d'angle l'argument de $a+b\omega$. Pour nos considérations il suffira de considérer la taille d'un losange de ce réseau homothétique, choisissons le losange de sommets $0, a+b\omega, \omega(a+b\omega)$ et $(1+\omega)(a+b\omega)$ (que l'on pourra dessiner sur l'illustration précédente pour $3+2\omega$ par exemple.) La petite diagonale est de longueur $\mid a+b\omega \mid$ et la grande de longueur $\sqrt{3}\cdot \mid a+b\omega \mid$. Par conséquent le cercle dont le centre est le milieu du losange (point d'intersection des diagonales) et dont le rayon vaut $\sqrt{3}/2\cdot \mid a+b\omega \mid$ contient toute la maille. Ceci démontre que tout point de $\mathbb{Z}[\omega]$ se trouve à une distance d'au plus $\sqrt{3}/2\cdot \mid a+b\omega \mid$ d'un point de ce réseau $(a+b\omega)$.

   Autrement dit, pour tout entier d'Eisenstein $c+d\omega$, il existe un entier $q = q_0 + q_1\omega$ tel que $r = c+d\omega - q(a+b\omega)$ est de norme plus petite ou égale à $3/4 \cdot N(a+b\omega) < N(a+b\omega)$. On choisira alors q pour quotient et r comme reste de la division.

3. Let $z \in \mathbb{Z}[\omega]$ be invertible, with inverse element denoted by z^{-1}. Then by the multiplicative properties of the norm, we have that $1 = N(1) = N(z)\cdot N(z^{-1})$, and therefore, $N(z) \in \mathbb{N}$ needs to be equal to 1. This is obtained for the elements $z = \pm 1, \pm\omega, \pm(1+\omega)$. One checks that these are indeed units: ± 1 is clearly a unit, and by the first point, we have that $\omega + \bar{\omega} = -1$. From this, it follows with $\omega^2 = \bar{\omega}$ that $\omega(1+\omega) = \omega + \omega^2 = \omega + \bar{\omega} = -1$. Hence the inverse of $\pm\omega$ is $\mp(1+\omega)$.

Exercice 3.
L'anneau $\mathbb{Z}[i\sqrt{5}]$.

1. Montrer que le polynôme $3 + 2t + 2t^2$ est irréductible sur $\mathbb{Z}[i\sqrt{5}]$, mais pas sur le corps des fractions de $\mathbb{Z}[i\sqrt{5}]$

2. **Généralisation.** Soient a, b, c, d des éléments irréductibles non associés d'un anneau commutatif et intègre A tels que $ab = cd$. Calculer $(a + ct)(b + ct)$ et conclure que le polynôme $d + (a + b)t + ct^2$ est irréductible sur A, mais pas sur son corps des fractions K.

3. Montrer que la norme n'est pas une fonction euclidienne sur $\mathbb{Z}[i\sqrt{5}]$.

Solution.

1. We calculate the complex roots of the polynomial $3 + 2t + 2t^2$. They are $\frac{-2 \pm i\sqrt{20}}{4} = \frac{-1 \pm i\sqrt{5}}{2}$. The roots are elements in $\mathbb{Q}[i\sqrt{5}]$ and we have that $3+2t+2t^2 = 2(t+\frac{1+i\sqrt{5}}{2})(t+\frac{1-i\sqrt{5}}{2})$. This means that $3 + 2t + 2t^2$ is not irreducible in $\mathbb{Q}[i\sqrt{5}]$, as we can express it as the product of $2(t + \frac{1+i\sqrt{5}}{2})$ and $(t + \frac{1-i\sqrt{5}}{2})$, both of which are not units.

   On the other hand, if we try to decompose $3 + 2t + 2t^2$ into a product of two non-invertible elements in $\mathbb{Z}[i\sqrt{5}]$, then we have two option: we assume that $3 + 2t + 2t^2 = f(t)g(t)$ with f, g polynomials in $\mathbb{Z}[i\sqrt{5}][t]$. Now the sum of the degree of f plus the degree of g is equal to 2, which means that either f is of degree 2, and g of degree 0 (or vice versa), or the degree of both is 1.

   If g is of degree 0, then g is in $\mathbb{Z}[i\sqrt{5}]$, and it holds that g times the leading coefficient of f is equal to 2. But since 2 is irreducible in $\mathbb{Z}[i\sqrt{5}]$, (this can be seen by checking that $N(2) = 4$, and verifying that not element in $\mathbb{Z}[i\sqrt{5}]$ exists with norm 2) it follows that either $g = \pm 1$ or $g = \pm 2$. If $g = \pm 1$, then the decomposition of $3 + 2t + 2t^2$ is the decomposition into a unit multiplied by a non-unit. The other decomposition with $g = \pm 2$ does not exist, since not all coefficients of $3 + 2t + 2t^2$ are divisible by 2.

   Therefore, our only possibility for a decomposition into a product of two non-invertible elements is if both f and g are of degree 1. Let $f(t) = (\alpha t + \beta), g(t) = (\gamma t + \delta)$ with $\alpha, \ldots, \delta \in \mathbb{Z}[i\sqrt{5}]$. Since the leading coefficient of $3+2t+2t^2$ is 2, which is irreducible in $\mathbb{Z}$, it follows that $\alpha = \pm 2, \gamma = \pm 1$ (or vice versa). We now note that the ring $\mathbb{C}[t]$ is Euclidian by Proposition 3.7.1 (hence factorial by Theorem 3.7.7) it holds that every irreducible element is prime by Theorem 3.5.1. Again, since this ring is factorial, if element $c(t) \in \mathbb{C}[t]$ admits a decomposition into irreducible factors, then that decomposition is unique (up to multiplication by units). This means that if a decomposition of $3 + 2t + 2t^2$ in $\mathbb{Z}[i\sqrt{5}]$ exists, then it must agree with the decomposition in $\mathbb{C}[t]$ we have found above. So if $3+2t+2t^2 = (2t+\beta)(t+\delta)$ is a decomposition in $\mathbb{Z}[i\sqrt{5}][t]$, then it needs to agree with the decomposition in $\mathbb{C}[t]$, which would force the decomposition to be of the form $3 + 2t + 2t^2 = (2t + 1 + \sqrt{5}i)(t + \frac{1-i\sqrt{5}}{2})$ or $3 + 2t + 2t^2 = (t + \frac{1+\sqrt{5}i}{2})(2t + 1 - i\sqrt{5})$. But clearly one of the roots is not a root in $\mathbb{Z}[i\sqrt{5}]$, which is a contradiction. We conclude that in $\mathbb{Z}[i\sqrt{5}]$, the polynomial can not be written as a product of non-invertible elements, making it irreducible.

2. **Généralisation.** We calculate

$$(a + ct)(b + ct) = ab + (cb + ac)t + c^2t = cd + (cb + ac)t + c^2t = c(d + (a + b)t + ct^2)$$

   which shows that the roots of $d + (a + b)t + ct^2$ are $-a/c$ and $-b/c$ in K. This shows that in K, we can write the polynomial $d + (a + b)t + ct^2$ as the product $c(t + \frac{a}{c})(t + \frac{b}{c})$, with both terms $c(t + \frac{a}{c})$ and $(t + \frac{b}{c})$, not units. Hence the polynomial is not irreducible in K.

   On the other hand, over A, the polynomial is irreducible. This we prove as in the exercise above. We assume that the polynomial decoposes into a product of two non-invertible polynomials f and g. There are two options. Firstly, we suppose that g is of degree 0, and f is of degree 2. Then, g multiplied with the leading coefficient of f is equal to c. But since

c is irreducible in A, it follows that $g = u, u \in A^\times$ or $g = uc, u \in A^\times$ If $g = u$, then the decomposition is the decomposition into a unit and non-unit. The other decomposition, with $g = uc$ does not exist, since c does not divide at least one coefficient of our polynomial. In fact, c does not divive d because they are irreducible and not associated.

So we now assume that the degree of f and g is 1. Then, $f(t) = \alpha t + \beta, g(t) = \gamma t + \delta$, with $\alpha, \ldots, \delta \in A$. Since the leading coefficient is c, which is irreducible in A, it follows that $\alpha = uc, u \in A^\times$. The argument above only uses the fact that $\mathbb{C}$ is a field to show that if an element over $\mathbb{C}[t]$ admits a decomposition into irreducible factors, then it is unique. Hence we apply the same propositions to the field K and see that the decomposition of $d+(a+b)t+ct^2$ as the product $c(t+\frac{a}{c})(t+\frac{b}{c})$ is unique. From this, it follows that if there exists a decomposition of the polynomial in A, then it must agree with the decomposition in K, which is of the form $d + (a + b)t + ct^2 = (ct + a)(t + \frac{b}{c})$, or $d + (a + b)t + ct^2 = (t + \frac{a}{c})(ct + b)$. But clearly in both cases, one of the roots is not a root in A, which is a contradiction. Hence the polynomial is irreducible in A.

3. Dividing $-2 + i\sqrt{5}$ by $1 + i\sqrt{5}$ with rest and calculating the norm of the rest, we see that if $\mathbb{Z}[i\sqrt{5}]$ with the norm $N(a + i\sqrt{5}b) = a^2 + 5b^2$ was Euclidean, then the norm of the rest would need to be smaller than the norm of $1 + i\sqrt{5}$, which is 6. We perform the division over $\mathbb{C}$, and obtain $\frac{-2+i\sqrt{5}}{1+i\sqrt{5}} = \frac{1}{2} + i\frac{1}{2}\sqrt{5}$. The closest elements in $\mathbb{Z}[i\sqrt{5}]$ are $0, i\sqrt{5}, 1, 1 + i\sqrt{5}$. It holds that

   - $-2 + i\sqrt{5} = (1 + i\sqrt{5}) \cdot 0 + (-2 + i\sqrt{5}) = 0 + (-2 + i\sqrt{5})$ with $N(-2 + i\sqrt{5}) = 9$
   - $-2 + i\sqrt{5} = (1 + i\sqrt{5}) \cdot i\sqrt{5} + 3 = (-5 + i\sqrt{5}) + 3$ with $N(3) = 9$
   - $-2 + i\sqrt{5} = (1 + i\sqrt{5}) \cdot 1 + (-3) = (1 + i\sqrt{5}) + (-3)$ with $N(-3) = 9$
   - $-2+i\sqrt{5} = (1+i\sqrt{5})\cdot(1+i\sqrt{5})+(2-\sqrt{5}) = (-4+i2\sqrt{5})+(2-\sqrt{5})$ with $N(2-\sqrt{5}) = 9$

   As the norm of every rest is bigger than 6, we can not find $q, r \in \mathbb{Z}[i\sqrt{5}]$ such that $-2+i\sqrt{5} = q(1 + i\sqrt{5}) + r$ with $N(r) < N(1 + i\sqrt{5})$, which means that $\mathbb{Z}[i\sqrt{5}]$ equipped with N is not Euclidean.

   Note that we can also look at the calculations above in a geometric way. The four elements 0, $1 + i\sqrt{5}$, $-5 + i\sqrt{5}$ et $-4 + 2i\sqrt{5}$ are the edges of the rectangle of the lattice spanned by $(1 + i\sqrt{5})$ that contains $-2 + i\sqrt{5}$.

Exercice 4.
En s'inspirant de l'exemple 3.7.4.(3), montrer que $\mathbb{Z}[i\sqrt{2}]$ est Euclidien.

Solution.
La technique de l'exemple 3.7.4.(3) s'applique texto car (en reprenant les notations de l'exemple)

$$\left|\Re e\left(\frac{b}{a} - q\right)\right| \leq \frac{1}{2} \qquad \text{et} \qquad \left|\Im m\left(\frac{b}{a} - q\right)\right| \leq \frac{1}{\sqrt{2}}$$

Ceci implique que

$$\left|\frac{b}{a} - q\right|^2 \leq \frac{1}{2^2} + \frac{1}{2} = \frac{3}{4} < 1$$

et on conclut comme dans l'exemple.

Exercice 5.
Idéaux dans un anneau de polynômes.

1. Décrire tous les idéaux premiers et tous les idéaux maximaux de $\mathbb{C}[t]$ et de $\mathbb{R}[t]$.

Pour $\mathbb{R}[t]$, montrez d'abord en utilisant que $\mathbb{C}$ est algébriquement clos et que les racines d'un polynôme réel sont closes par conjugaison, qu'un polynôme de $\mathbb{R}[t]$ se décompose toujours comme produits de polynômes dans $\mathbb{R}[t]$ de degré au plus 2.*

2. Soit K un corps et $a \in K$. Montrer que $(t-a)$ est un idéal premier de $K[s,t]$, mais non maximal. Ainsi $K[s,t]$ est un anneau factoriel mais pas principal.

3. Montrer que l'anneau quotient $\mathbb{C}[s,t]/(s-t^2)$ est principal

4. **Polynôme d'interpolation de Lagrange.** Soit K un corps, $a_1, \ldots, a_n$ des éléments de K distincts et $b_1, \ldots, b_n \in K$. Montrer qu'il existe un polynôme $f \in K[t]$ de degré au plus $n-1$ tel que $f(a_i) = b_i$ pour tout $1 \leq i \leq n$.

Solution.

For any field K, we know that by Propositions 3.7.1 and 3.7.6, $K[t]$ is a principal ideal domain (often denoted PID). By Proposition 3.6.3, the following are equivalent for an element q in a PID:

- q prime
- q irreducible
- (q) prime
- (q) maximal.

1. For $\mathbb{C}[t]$, we know by Example 3.2.10.(3) that

$$f(t) \in \mathbb{C}[t] \text{ irreducible} \Leftrightarrow f(t) = ct + d, c \in \mathbb{C} \setminus \{0\}, d \in \mathbb{C}.$$

   Hence the prime=maximal ideals in $\mathbb{C}[t]$ are of the form $(ct+d)$.

   Pour $\mathbb{R}[t]$: considérons les racines complexes d'un polynôme réel $f(t)$. On les sépare en deux groupes

   (a) les racines dans $\mathbb{R}$
   (b) les racines dans $\mathbb{C} \setminus \mathbb{R}$.

   Comme $\overline{f}(t) = f(t)$ car le polynôme est réel, on voit que les racines du deuxième groupe viennent forcément par paires de conjugués, car si $\lambda \in \mathbb{C} \setminus \mathbb{R}$ est dans ce deuxième groupe, alors $\overline{\lambda} \neq \lambda$ l'est aussi. Mais notons également que $(t-\lambda)(t-\overline{\lambda}) \in \mathbb{R}[t]$, car $\lambda + \overline{\lambda}, \lambda\overline{\lambda} \in \mathbb{R}$. Ainsi on voit que tout polynôme réel se décompose comme produit de polynôme réels de degré au plus 2.

   Dès lors, on conlut que les polynômes irréductibles de $\mathbb{R}[t]$ sont

   (a) Les polynômes de degré 1,
   (b) Les polynômes de degré 2 sans racines.

   En effet tout les polynômes de degré 1 sont irréductibles et un polynôme de degré 2 l'est si et seulement si il n'a pas de racine. En effet s'il n'était pas irréductible il devrait être divisé par un polynôme de degré 1 est donc avoir une racine.

   Attention ce dernier argument ne marche pas pour les polyômes de plus haut degré. Par exemple $(t^2+1)^2$ n'a pas de racine dans $\mathbb{R}$ mais n'est pas irréductible dans $\mathbb{R}[t]$.

2. By example 2.4.10.(1), we know that $K[s,t]/(t-a) \cong K[s]$, which is a domain but not a field. Hence, $(t-a)$ is prime but not maximal.

*En effet si $f(t)$ est à coefficient réels, alors $\overline{f}(t) = f(t)$ et donc si $f(t) = \prod(t-\lambda_i)$ dans $\mathbb{C}[t]$ alors on voit que l'ensemble des racines est stable par conjugaison.

3. As above, $\mathbb{C}[s,t]/(s-t^2) \cong \mathbb{C}[t]$, which is a PID.

4. We want to apply the Chinese remainder theorem to the ideals $(t-a_i)$ in $K[t]$. We may do so, since from $a_i \neq a_j$ for all i,j it follows that $(t-a_i)$ is prime to $(t-a_j)$. With the remainder theorem, we get that

$$K[t]/((t-a_1) \cap \ldots \cap (t-a_n)) \cong K[t]/(t-a_1) \times \ldots \times K[t]/(t-a_n).$$

First, we remark that $(t-a_1) \cap \ldots \cap (t-a_n) = ((t-a_1) \cdot \ldots \cdot (t-a_n))$, and we denote $f(t) := (t-a_1) \cdot \ldots \cdot (t-a_n)$. Seondly, the $K[t]/(t-a_i)$ are isomorphic to K, using the evaluation at a_i. It follows that

$$K[t]/(f(t)) \cong K \times \ldots \times K \cong K^n.$$

We now take $(b_1, \ldots, b_n) \in K^n$. Via the isomorphism above, there exists $g(t) \in K[t]$ modulo $f(t)$ that corresponds to $(b_1, \ldots, b_n) \in K^n$. Since the isomorphism above is constructed using the evaluations as a_i, it follows that $g(a_i) = b_i$ for all $i = 1, \ldots, n$. Lastly, since $f(t)$ is of degree n, we may represent a class (modulo f) by a polynomial of degree strictly smaller than n. Hence $g(t)$ is of degree at most $n-1$.

Exercice 6.
Trouver tous les idéaux de $\mathbb{Z}[i]$ qui contiennent l'idéal (5) et tous les idéaux de $\mathbb{Z}[i]$ qui contiennent l'idéal (2).

Solution.

By Example 3.2.7, we have that $\mathbb{Z}[i]$ is euclidean. From Proposition 3.3.3 it follows that $\mathbb{Z}[i]$ is principal. This means that every ideal in $\mathbb{Z}[i]$ is generated by a single element. So let $a \in \mathbb{Z}[i]$ such that $(5) \subsetneq (a) \subsetneq \mathbb{Z}[i]$. From Remark 3.4.5 it follows that $a \mid 5$ and then with Proposition 3.4.8 it follows that $N(a) \mid N(5) = 25$. The only options for $N(a)$ are 1,5, or 25. But since (a) is not equal to both (5) and $\mathbb{Z}[i]$, it follows that $N(a) \neq 25$ and $N(a) \neq 1$. Hence $N(a) = 5$, and we let $a = c+id$ with $c, d \in \mathbb{Z}$. In order for $N(c+id) = 5$ to hold, we have that either $c = \pm 1, d = \pm 2$ or vice versa. The possibilities for a are $a = 1+2i, 1-2i, -1+2i, -1-2i$ and $a = 2+i, 2-i, -2+i, -2-i$. But the elements $-1-2i, 1+2i$ and $-2+i$ are all associated to $2-i$ and the elements $-1+2i, 1-2i$ and $-2-i$ are all associated to $2+i$. We obtain two ideals $(a) = (2-i)$ and $(a) = (2+i)$. Since the elements $2-i$ and $2+i$ are not associated, these ideals are distinct.

We now let $b \in \mathbb{Z}[i]$ such that $(2) \subsetneq (b) \subsetneq \mathbb{Z}[i]$. As above, $b \mid 2$, from which it follows that $N(b) \mid N(2) = 4$. The options for $N(b)$ are 1,2 and 4, but since (b) is not equal to (2) or $\mathbb{Z}[i]$, it follows that $N(b) = 2$. This is satisfied for b of the form $1+i, 1-i, -1+i, -1-i$. As all of these elements are associated, the only ideal we obtain is $(b) = (1+i)$.

Exercice 7.
L'objectif de cet exercice est de trouver toutes les paires $(x,y) \in \mathbb{Z}^2$ telles que $x^2+2 = y^3$. Nous allons procéder ainsi.

Fixons $x, y \in \mathbb{Z}$ tel que $x^2+2 = y^3$.

1. Montrer que 2 ne divise pas x.

2. Montrer que $\text{pgdc}(x+i\sqrt{2}, x-i\sqrt{2}) = 1$ dans l'anneau $\mathbb{Z}[i\sqrt{2}]$.

3. Montrer qu'il existe $z \in \mathbb{Z}[i\sqrt{2}]$ tel que $x+i\sqrt{2} = \pm z^3$.

4. Trouver toutes les solutions de l'équation $x^2+2 = y^3$ à valeur dans $\mathbb{Z}$.

Solution.

1. Si 2 divise x, alors 2 divise y^3, et donc 2 divise y. Posons $x = 2x_0$ et $y = 2y_0$. On a alors que
$$4x_0^2 + 2 = 8y_0^3,$$
ce qui est impossible (4 divise $4x_0^2$ et $8y_0^3$, mais pas 2).

2. Supposons que ce n'est pas le cas, et soit $d \in \mathbb{Z}[i\sqrt{2}]$ un élément irréductible tel que d divise à la fois $x + i\sqrt{2}$ et $x - i\sqrt{2}$. L'élément d divise alors
$$(x + i\sqrt{2}) - (x - i\sqrt{2}) = 2i\sqrt{2} = -(i\sqrt{2})^3.$$
Montrons que $i\sqrt{2}$ est irréductible, et soient donc $a, b \in \mathbb{Z}[i\sqrt{2}]$ tels que $ab = i\sqrt{2}$. On a alors que $N(a)N(b) = N(i\sqrt{2}) = 2$, qui est un nombre premier. Ainsi, $N(a)$ ou $N(b)$ doit valoir 1, i.e. a ou b est inversible. Ainsi, $i\sqrt{2}$ est bel et bien irréductible.

   Comme d divise $(i\sqrt{2})^3$ et que $i\sqrt{2}$ est irréductible, on a nécéssairement que $d = i\sqrt{2}$. En effet, vu que $\mathbb{Z}[i\sqrt{2}]$ est Euclidien par l'exercice 4, on sait par le cours que cet anneau est factoriel, et donc que la décomposition en facteurs irréductibles est unique.

   On a donc prouvé que d est associé à $i\sqrt{2}$, et par hypothèse celui-ci divise $x + i\sqrt{2}$. Ainsi, $i\sqrt{2}$ divise x, et donc $2 = N(i\sqrt{2})$ divise $N(x) = x^2$ (dans $\mathbb{Z}$). Comme 2 est premier dans $\mathbb{Z}$, on en déduit que 2 divise x, ce qui contredit le premier point.

3. Posons $a := x + i\sqrt{2}$ et $b = x - i\sqrt{2}$. On a par hypothèse que $ab = y^3$. Soit p un diviseur premier de y. Comme a et b sont premiers entre eux, p ne peut pas diviser a et b à la fois. Comme y^3 est un produit d'éléments premiers élevés au cube, on en déduit que c'est aussi le cas de a et b par l'unicité de la décomposition en facteurs premiers. En particulier, a est un cube à unité près.

   Or, les seuls éléments inversibles de $\mathbb{Z}[i\sqrt{2}]$ sont ± 1. En effet, ces éléments sont certainement inversibles, et dans l'autre sens si $u \in \mathbb{Z}[i\sqrt{2}]^\times$, alors $N(u) \in \mathbb{Z}^\times = \{\pm 1\}$, ce qui force $u = \pm 1$.

   Ainsi, $a = \pm z^3$ pour un certain $z \in \mathbb{Z}[i\sqrt{2}]$.

4. Remarquons que 1 et -1 sont aussi des cubes, et du coup il existe $w \in \mathbb{Z}[i\sqrt{2}]$ tel que $x + i\sqrt{2} = w^3$. Ecrivons $w = e + fi\sqrt{2}$. Alors on a
$$x + i\sqrt{2} = (e + fi\sqrt{2})^3 = (e^3 - 6ef^2) + (3e^2f - 2f^3)i\sqrt{2},$$
et donc
$$\begin{cases} x = e^3 - 6ef^2; \\ 1 = 3e^2f - 2f^3. \end{cases}$$
La deuxième équation montre que f divise 1, i.e. $f = \pm 1$. Ainsi, on a
$$1 = \pm(3e^2 - 2).$$
Si $f = -1$, on en déduirait que $3e^2 = -1$, ce qui est impossible car 3 ne divise par -1. Ainsi, $f = 1$ et donc
$$3e^2 = 3,$$
i.e. $e = \pm 1$.

   On a donc
$$x = e^3 - 6ef^2 = \pm 5.$$
Cela implique que $y^3 = 27$, et donc $y = 2$. Ainsi, les solutions de l'équation $x^2 + 2 = y^3$ dans $\mathbb{Z}^2$ sont
$$\{(5, 3), (-5, 3)\}.$$