EPFL - Printemps 2022	Prof. Z. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 6	

Exercice 1. 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
- Assume that $3 = x \cdot y$, with $x, y \in \mathbb{Z}[i]$. Then by Proposition 3.4.8, it follows that both $N(x)$ and $N(y)$ divide $N(3) = 9$. 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 by Proposition 3.4.8 that $2-3i$ is irreducible in $\mathbb{Z}[i]$.

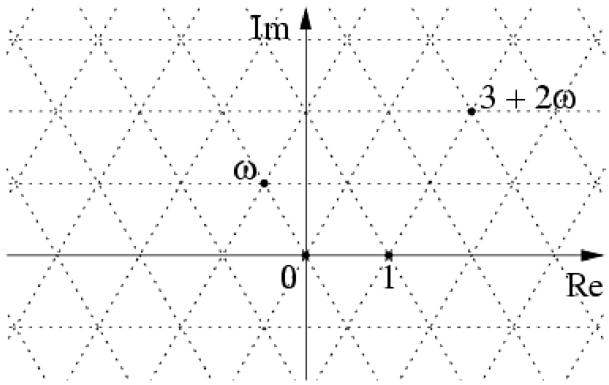
3. We note that $\mathbb{Z}[i]$ is Euclidean by Example 3.2.7, from which it follows by Proposition 3.3.3 that $\mathbb{Z}[i]$ is principal. The Proposition 3.4.13 then states that since 3 is irreducible in $\mathbb{Z}[i]$, the ideal (3) is maximal in $\mathbb{Z}[i]$. It follows that $\mathbb{Z}[i]/(3)$ is a field.

To study its cardinality, we see that the classes modulo 3 are represented by the rest of the division by 3 in $\mathbb{Z}[i]$. The norm of the rest, which we denote by $r_1 + ir_2$ is $N(r_1+ir_2) = r_1^2 + r_2^2$ and is strictly smaller than the norm of 3, which is $N(3) = 9$. This is satisfied for pairs of (r_1, r_2) of the form $(0,0), (1,0), (0,1), (1,1), (2,0), (0,2), (2,1), (1,2), (2,2)$. There are 9 such pairs. (Rmk: for example, the pair $(1,-1)$ satisfies the restrictions as well, but it coincides with the pair $(1,2)$ modulo 3, as $1+2i = 3i + (1-i)$. Hence the pairs above are all.)

An alternative way to count the elements in $\mathbb{Z}[i]/(3)$ is via the isomorphism in Serie 4, Exercies 4.1. We saw that $\mathbb{Z}[i]/(3) \cong \mathbb{F}_3[t]/(t^2 + [1]_3)$. The elements in $\mathbb{F}_3[t]/(t^2 + [1]_3)$ are the following: $0, 1, 2, t, 1+t, 2+t, 2t, 1+2t, 2+2t$, which correspond to the following elements in $\mathbb{Z}[i]/(3) : 0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i$.

Exercice 2. 1. On 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 d 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. 1. We define $\overline{a + b\sqrt{5}} = a - b\sqrt{5}$ and note that for all $z \in \mathbb{Z}[\sqrt{5}]$, the norm $N(z) = z\bar{z}$. The fact that N is a multiplicative function then follows from the fact that $\forall y, z \in \mathbb{Z}[\sqrt{5}]$, it holds that $\overline{yz} = \bar{y}\,\bar{z}$. With this, we get that $N(yz) = yz\overline{yz} = yz\bar{y}\,\bar{z} = y\bar{y}z\bar{z} = N(y)N(z)$.

Furthermore, if $z \in \mathbb{Z}[\sqrt{5}]$ is invertible, then $N(z) = \pm 1$ is necessary. If we denote its inverse by z^{-1}, then $N(z)N(z^{-1}) = N(1) = 1$, and therefore, $N(z) = \pm 1$. On the other hand, if $N(z) = \pm 1$ for some $z \in \mathbb{Z}[\sqrt{5}]$, then $\pm 1 = N(z) = z\overline{z}$ and hence $\pm\overline{z}$ is the inverse of z.

2. We note that $N(9+4\sqrt{5}) = 9^2 - 5 \cdot 4^2 = 1$, and so by the first point, $9+4\sqrt{5}$ is invertible. Furthermore, by the multiplicative property of the norm, the norm of $(9+4\sqrt{5})^n$ is 1 as well, for $n \in \mathbb{N}$. This means that we have created infinitely many invertible elements, and $(\mathbb{Z}[\sqrt{5}])^\times$ is infinite.

3. We first show that no elements of norm 2 exist. For this, we note that $N(a+\sqrt{5}b) = a^2 - 5b^2$, which is equal to a^2 modulo 5, a square. But all squares in $\mathbb{Z}/5\mathbb{Z}$ are either 0,1 or 4, as one checks by taking the square of all elements in $\mathbb{Z}/5\mathbb{Z}$.

   Now let $z \in \mathbb{Z}[\sqrt{5}]$ be of norm 4, and we assume that $z = v \cdot w$ for $v, w \in \mathbb{Z}[\sqrt{5}]$. Then $4 = N(z) = N(v)N(w)$. But as there are no elements of norm 2, we have that either $N(v) = \pm 1, N(w) = \pm 4$ or $N(v) = \pm 4, N(w) = \pm 1$. In either cases one of the two elements is of norm ± 1, which means that that element is invertible. Hence z is irreducible.

4. We have

   - $4 = 2 \cdot 2$ and $N(2) = 4$, hence by the previous part, 2 is irreducible
   - $4 = (1+\sqrt{5})(-1+\sqrt{5})$ and $N(1+\sqrt{5}) = -4, N(-1+\sqrt{5}) = -4$, hence both $1+\sqrt{5}, -1+\sqrt{5}$ are irreducible.
   - $4 = (3+\sqrt{5})(3-\sqrt{5})$ and $N(3+\sqrt{5}) = 4, N(3-\sqrt{5}) = 4$, hence both $3+\sqrt{5}, 3-\sqrt{5}$ are irreducible.

5. As we see from the previous point, $2 \cdot 2 = 4 = (3+\sqrt{5})(3-\sqrt{5})$, from which it follows that $2 \cdot 2 \in (3+\sqrt{5})$. But as $2 \notin (3+\sqrt{5})$, the ideal $(3+\sqrt{5})$ is not prime.

   We remark that irreducible does not imply prime in a ring that is not factorial or principal.

Exercice 4. 1. We calculate the complex roots of the polynomial $3+2t+2t^2$. They are $\dfrac{-2 \pm i\sqrt{20}}{4} = \dfrac{-1 \pm i\sqrt{5}}{2}$. The roots are elements in $\mathbb{Q}[i\sqrt{5}]$ and we have that $3+2t+2t^2 = 2(t+\dfrac{1+i\sqrt{5}}{2})(t+\dfrac{1-i\sqrt{5}}{2})$. 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 $2(t+\dfrac{1+i\sqrt{5}}{2})$ and $(t+\dfrac{1-i\sqrt{5}}{2})$, 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 $\mathbb{Z}$, (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 integral by Proposition 3.2.3. Since furthermore, it is principal by Corollary 3.3.5, it holds that every irreducible element is prime by Proposition 3.4.13. Then by Proposition 3.5.4, if an 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 $\alpha, \dots, \delta \in A$. 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. By divide $-2 + i\sqrt{5}$ by $1 + i\sqrt{5}$ with rest, and then calculate the norm of the rest. 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 5.

For any field K, we know that by Corollary 3.3.5, $K[t]$ is a principal ideal domain. By Proposition 3.4.13, in a PID, the following are equivalent, for q in the PID:

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

1. For $\mathbb{C}[t]$, we know by Example 2.3.7(c) 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 $(ct+d)$.

For $\mathbb{R}[t]$, we know by Example 3.4.7 that the ideal $(t-d)$ is prime=maximal for all $d \in \mathbb{R}$. Furtermore, by Example 3.4.7, we know that if $f \in \mathbb{R}[t], \deg(f) \leq 3$, then

$$f(t) \in \mathbb{R}[t] \text{ irreducible} \Leftrightarrow \forall c \in \mathbb{R} : f(c) \neq 0$$

Let $f(t) = at^2 + bt + c = a\left(t^2 + \frac{b}{a}t + \frac{c}{a}\right)$, with $a \in \mathbb{R}$ invertible. It suffices therefore to study $f(t) = x^2 + bx + c$. The complex roots of f are $\frac{-b \pm \sqrt{b^2-4c}}{2}$. Both roots are not in $\mathbb{R}$ if $b^2 - 4c < 0$. Hence f is irreducible if $b^2 - 4c < 0$. The ideals $(x^2 + bx + c)$ are prime=maximal for $b^2 - 4c < 0$.

There are no irreducible polynomials of higher degree, since a polynomial in $\mathbb{R}[t]$ of degree 3 or higher has at least one root that is contained in $\mathbb{R}$.

2. We consider the evaluation of $K[s,t]$ at $t = a$, defined as

$$ev_a : K[s,t] \to K[s], \; s \mapsto s, t \mapsto a.$$

Similar to Example 1.4.10, we show that $\ker(ev_a) = (t-a)$. With the first isomorphism theorem (and ev_a being surjective), it follows that $K[s,t]/(t-a) \cong K[s]$. With Proposition 3.2.3, it follows from K being a field, and hence in particular being integral, that $K[s]$ is integral as well. From Proposition 2.5.2 it follows that $(t-a)$ is a prime ideal. On the other hand, it holds that $K[s]$ is not a field, and therefore, with Proposition 2.5.5 it follows that $(t-a)$ is not a maximal ideal.

3. Consider the evaluation of $\mathbb{C}[s,t]$ at $s = t^2$ defined as

$$ev_{s=t^2} : \mathbb{C}[s,t] \to \mathbb{C}[t], \; s \mapsto t^2, t \mapsto t.$$

Again, by the usual argument, $\ker(ev_{s=t^2}) = (s - t^2)$. It follows with surjectivity by the first isomorphism theorem that $\mathbb{C}[s,t]/(s-t^2) \cong \mathbb{C}[t]$. By Corollary 3.3.5, using that $\mathbb{C}$ is a field, it follows that $\mathbb{C}[t]$ is a principal ideal domain.

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.
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.

1. It holds that

   - $(S^{-1}A, +)$ is a subgroup of $(\mathrm{Frac}(A), +)$, since $\frac{0}{1} \in S^{-1}A$, as $0 \in A, 1 \in S$. Furthermore, $\forall \frac{a}{b}, \frac{c}{d} \in S^{-1}A$, we have that $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} \in S^{-1}A$, since $ad + cb \in A$, and $bc \in S$ for $b \in S, c \in S$. Lastly, the additive inverse of $\frac{a}{b} \in S^{-1}A$ is $\frac{-a}{b}$, which is contained in $S^{-1}A$ as well.
   - Since $1_A \in S$, it holds that $\frac{1}{1} \in S^{-1}A$.
   - $\forall \frac{a}{b}, \frac{c}{d} \in S^{-1}A$ we have that $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in S^{-1}A$ since $ac \in A$, and $bd \in S$ for $b \in S, d \in S$.

   This means that $S^{-1}A$ is a ring.

2. We show that $S := A \setminus \mathfrak{p} = \{a \in A \mid a \notin \mathfrak{p}\}$ is closed under multiplication.

   - It holds that $1 \in S$, since if 1 were contained in $\mathfrak{p}$, then $\mathfrak{p}$ would be the whole ring A.
   - For $a, b \in S$, it holds that $a \cdot b \in S$, which means that $a \cdot b \notin \mathfrak{p}$. This holds because if $a \cdot b$ were contained in $\mathfrak{p}$, then since $\mathfrak{p}$ is prime, it would follow that either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, which is not possible due to the assumption that both a and b are contained in S.

For the ring $A = \mathbb{Z}$, you have seen the localization at a prime ideal in Example 2.1.7.

3. We note that the elements in the ring $\mathbb{Z}_{(2)}$ are of the form
$$\mathbb{Z}_{(2)} = \{\frac{a}{b} \in \mathrm{Frac}(\mathbb{Z}) \mid b \in \mathbb{Z} \setminus (2)\} = \{\frac{a}{b} \in \mathbb{Q} \mid 2 \nmid b\}.$$
We remark that the elements $\frac{a}{b} \in \mathbb{Z}_{(2)}$ with $2 \nmid a$ are the units of $\mathbb{Z}_{(2)}$, since the inverse of $\frac{a}{b}$ is $\frac{b}{a}$, which is contained in $\mathbb{Z}_{(2)}$ due to the fact that $2 \nmid a$.

   We define $m \subseteq \mathbb{Z}_{(2)}$ to be $m := \{\frac{a}{b} \in \mathbb{Z}_{(2)} \mid a \in (2)\}$. This is an ideal, since for $\frac{a}{b} \in m, \frac{c}{d} \in \mathbb{Z}_{(2)}$, it holds that $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in m$, since $a \in (2), c \in \mathbb{Z}$, and hence $ac \in (2)$. Furthermore, it is clearly an additive group. We show that this ideal is maximal. For this, we assume that there exists an ideal I such that $m \subset I$ and $m \neq I$. So there must exist an element $\frac{a}{b} \in I$ which is not contained in m. This means that $a \notin (2)$, and hence $2 \nmid a$. But as we remarked above, then $\frac{a}{b}$ is a unit in $\mathbb{Z}_{(2)}$, and so I is equal to $\mathbb{Z}_{(2)}$.

   Other proper ideals in $\mathbb{Z}_{(2)}$ are of the following form $I = \{\frac{a}{b} \in \mathbb{Z}_{(2)} \mid a \in (n)\}$ where (n) is an ideal such that $(n) \subseteq (2) \Leftrightarrow 2 \mid n$. These are clearly ideals. They are all ideals, since if there was an ideal that contained an element $\frac{a}{b}$ such that a is not a multiple of 2, then $\frac{a}{b}$ is a unit and hence the ideal is the whole ring.

   Lastly, we remark that the only prime ideal is the maximal ideal. The other ideals of the form $I = \{\frac{a}{b} \in \mathbb{Z}_{(2)} \mid a \in (n)\}$ with $(n) \subseteq (2)$ but $n \neq 2$ are not prime, since we have that $\frac{n}{1} \in I$, and we may write $n = 2m$ for some $m \in \mathbb{Z}, m < n$. But then $\frac{n}{1} = \frac{2}{1} \cdot \frac{m}{1}$ and both $\frac{2}{1} \notin I$ and $\frac{m}{1} \notin I$.

4. It holds that $\mathbb{Z}_2 = \{\frac{a}{b} \in \mathbb{Q} \mid b \in \{1, 2, 2^2, 2^3, \ldots\}\} = \{\frac{a}{2^i} \in \mathbb{Q} \mid i \in \mathbb{N}\}$. Hence for $i = 0$, we obtain elements $\frac{a}{2^0} = a \in \mathbb{Z}$, and for $i > 0$, we obtain elements of the form $\frac{a}{2^i}$ with $2 \nmid a$. The units are elements that have an inverse in $\mathbb{Z}_2$. These are the elements of the form $2^i \in \mathbb{Z}$, since their inverse is of the form $\frac{1}{2^i}$, which is contained in $\mathbb{Z}_2$, and elements of the form $\frac{1}{2^i}$, since their inverse is of the form $\frac{2^i}{1}$, which is contained in $\mathbb{Z}_2$. The other elements are not units, since seen as elements in $\mathbb{Q}$ they have an inverse, which is unique, but their inverse in not contained in $\mathbb{Z}_2$ (i.e. the inverse of $\frac{a}{2^i}$ with $2 \nmid a$ in $\mathbb{Q}$ is $\frac{2^i}{a}$, but since $2 \nmid a$, this is not an element of $\mathbb{Z}_2$.)

   The irreducible elements are the elements of the form $\frac{p}{2^i}$ and $2^i \cdot p$ with $p \in \mathbb{Z}$ prime. To prove this, we let $\frac{a}{2^i} \in \mathbb{Z}_2$. Then $a \in \mathbb{Z}$ has a prime decomposition of the following form, $a = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ for some prime numbers $p_i \in \mathbb{Z}$, and $r \geq 1, k_i \geq 1$. There are two cases.

   - If all the prime numbers p_i are odd, then we can write
$$\frac{a}{2^i} = \frac{1}{2^i} \cdot p_1^{k_1} \cdot \ldots \cdot p_r^{k_r},$$
with $\frac{1}{2^i}$ a unit in $\mathbb{Z}_2$. It follows that $\frac{a}{2^i}$ is irreducible if and only if $r = 1$ and $k_1 = 1$. This means that $\frac{a}{2^i}$ is of the form $\frac{p}{2^i}$ with p prime im $\mathbb{Z}$.
   - If the prime number 2 appears in the decomposition of a, then we have the following: We may assume that $p_1 = 2$, and that $i = 0$ (since we assume that the fractions in $\mathbb{Z}_2$ are shortened). We can write
$$\frac{a}{2^0} = a = 2^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r},$$
with 2^{k_1} a unit in $\mathbb{Z}_2$. It follows that a is irreducible if and only if $r = 2$ and $k_2 = 1$. This means that $\frac{a}{2^i}$ is of the form $2^j \cdot p$ with p prime in $\mathbb{Z}$.