EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 8	

Exercice 1. (a) Let $\phi : A \to B$ be a ring homomorphism and let $a \in A^\times$. Then, there exists $b \in A^\times$ such that $ab = 1$. Then:

$$1 = \phi(1) = \phi(ab) = \phi(a)\phi(b).$$

Hence $\phi(a)$ is an invertible element of B with inverse $\phi(b)$.

(b) Let $a, b \in A$ such that $a \sim b$. Then there exists $u \in A^\times$ such that $a = ub$ and we have:

$$\phi(a) = \phi(ub) = \phi(u)\phi(b).$$

Now by point (a) we have that $\phi(u) \in B^\times$ and we conclude that $\phi(a) \sim \phi(b)$.

(c) Counterexample: Consider the ring homomorphism: $\xi_2 : \mathbb{Z}[x] \to \mathbb{F}_2[x]$ (Example 1.4.36). Now $x^2 + 4x + 2 \in \mathbb{Z}[x]$ is irreducible (one shows this using Eisenstein with $p = 2$), but $\xi_2(x^2 + 4x + 2) = x^2$ and $x^2 \in \mathbb{F}_2[x]$ is reducible.

Exercice 2. (a) Voir corrigé du bonus 3.

(b) Par le théorème des restes chinois

$$\mathbb{Z}/pq\mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Ainsi $(1, 0)$, $(0, 1)$, $(0, 0)$ et $(1, 1)$ sont des racines. Comme les polynômes en jeu sont moniques, on peut voir avec le degré que le produit des $(t - a_i)$ ne peut diviser $t^2 - t$.

(c) As $f|g$ in $\mathbb{Q}[t]$, there exists $h \in \mathbb{Q}[t]$ such that $g(t) = f(t)h(t)$. Now, as $h \in \mathbb{Q}[t|$, we can write $h(t) = c \cdot h_1(t)$, where $h_1(t) \in \mathbb{Z}[t]$ is primitive and $c \in \mathbb{Q}$. Then:

$$g(t) = c \cdot f(t)h_1(t).$$

By Lemma 3.8.9, we have that $f(t)h_1(t)$ is primitive and, since $g(t)$ is also primitive, we use Lemma 3.8.11 to determine that $c \in \mathbb{Z}^\times$, i.e. $c = \pm 1$. Then

$$g(t) = \pm f(t)h_1(t) \text{ in } \mathbb{Z}[t], \text{ therefore } f|g \text{ in } \mathbb{Z}[t].$$

(d) The roots of $x^4 + 1$ over $\mathbb{C}$ are $e^{i(\frac{\pi}{4}+\frac{k\pi}{2})}$, where $0 \leq k \leq 3$, and we have:

$$x^4 + 1 = \prod_{k=0}^{3} (x - e^{i(\frac{\pi}{4}+\frac{k\pi}{2})}).$$

We group the conjugate complex roots and obtain the decomposition over $\mathbb{R}[x]$

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1).$$

By Example 3.9.2 (4), it follows $x^4 + 1$ does not admit roots in $\mathbb{Q}$, as it does not admit roots in $\mathbb{R}$. If $x^4 + 1 = f(x)g(x)$, where $f(x), g(x) \in \mathbb{Q}[x]$ are polynomials of degree 2, then $f(x) = (x-a_1)(x-a_2)$ and $g(x) = (x-a_3)(x-a_4)$, where $a_1, a_2, a_3, a_4 \in \{e^{i(\frac{\pi}{4}+\frac{k\pi}{2})} | \, 0 \leq k \leq 3\}$ are distinct. One checks that for every choice of a_i a_j the polynomial $(x - a_i)(x - a_j)$ does not have coefficients in $\mathbb{Q}$. We conclude that x^4+1 is irreducible in $\mathbb{Q}[x]$. Lastly, we note that, as it is primitive., by Lemma 3.8.13, it is also irreducible in $\mathbb{Z}[x]$.

In $\mathbb{F}_2[x]$ we have $x^4+[1]_2 = (x+[1]_2)^4$.

The squares in $\mathbb{F}_{11}$ are $[0]_{11}, [1]_{11}, [3]_{11}, [4]_{11}, [5]_{11}$ and $[9]_{11}$ and we deduce that $x^4+[1]_{11}$ does not admit roots in $\mathbb{F}_{11}$. Assume that $x^4+[1]_{11}$ admits a decomposition into a product of two polynomials of degree 2. As $\mathbb{F}_{11}$ is a field, we can assume that these polynomials are unitary. We have:

$$x^4+[1]_{11} = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(b+ac+d)x^2+(bc+ad)x+bd$$

and so $d=b^{-1}$ and $c=-a$. We substitute and obtain:

$$x^4+[1]_{11} = x^4+(b-a^2+b^{-1})x^2+a(b^{-1}-b)x+[1]_{11}$$

and so $a(b^{-1}-b)=0$.

- if $a=0$, then $b-a^2+b^{-1}=b+b^{-1}=0$, which is impossible as $[-1]_{11}$ is not a square in $\mathbb{F}_{11}$.
- if $b=b^{-1}$, then $b^2=[1]_{11}$ and so $b\in\{[1]_{11},[10]_{11}\}$.
  - If $b=[1]_{11}$, then $b-a^2+b^{-1}=[2]_{11}-a^2=0$, which is impossible as $[2]_{11}$ is not a square in $\mathbb{F}_{11}$.
  - If $b=[10]_{11}$, then $b-a^2+b^{-1}=[9]_{11}-a^2=0$ and so $a\in\{[3]_{11},[8]_{11}\}$.

We conclude that

$$x^4+[1]_{11} = (x^2+[3]_{11}\cdot x+[10]_{11})(x^2+[8]_{11}\cdot x+[10]_{11}) \text{ in } \mathbb{F}_{11}[x].$$

Since $x^8-1=(x^4+1)(x^4-1)$ it suffices to factor x^4-1:

- in $\mathbb{C}[x]$ we have: $x^4-1=(x+i)(x-i)(x+1)(x-1)$.
- in $\mathbb{R}[x]$, $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$ we have: $x^4-1=(x^2+1)(x+1)(x-1)$.
- in $\mathbb{F}_2[x]$ we have: $x^4-[1]_2=x^4+[1]_2=(x+[1]_2)^4$.
- in $\mathbb{F}_{11}[x]$ we have: $x^4-[1]_{11}=(x^2+[1]_{11})(x+[1]_{11})(x+[10]_{11})$, where we have seen earlier that $x^2+[1]_{11}$ is irreducible.

Exercice 3. (a) We write $\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}=\frac{1}{9}(2x^5+15x^4+9x^3+3)\in\mathbb{Q}[x]$.

Now $\frac{1}{9}\in\mathbb{Q}[x]^\times$, as $\frac{1}{9}\in\mathbb{Q}^\times$. Therefore $\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}$ is irreducible in $\mathbb{Q}[x]$ if and only if $2x^5+15x^4+9x^3+3$ is. As $\gcd(2,15,9,3)=1$, we have that $2x^5+15x^4+9x^3+3$ is primitive, hence it is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Lemma 3.8.13). Using Eisenstein for $p=3$, where $3\in\mathbb{Z}$ is irreducible, we deduce that $2x^5+15x^4+9x^3+3$ is irreducible in $\mathbb{Z}[x]$.

(b) Let $f(x)=x^4+[2]_5\in\mathbb{F}_5[x]$. Note that for all $a\in\mathbb{F}_5$ we have $a^2\in\{[0]_5,[1]_5,[4]_5\}$. Therefore f does not admit roots in $\mathbb{F}_5$. We will now show that f is not a product of two polynomials of degree 2. As $\mathbb{F}_5$ is a field, we can assume that these polynomials are unitary and so assume there exist $a,b,c,d\in\mathbb{F}_5$ such that

$$f(x)=x^4+[2]_5=(x^2+ax+b)(x^2+cx+d)=x^4+(a+c)x^3+(b+ac+d)x^2+(bc+ad)x+bd.$$

Then $c=-a$ and $d=[2]_5b^{-1}$ and substituting in the above gives:

$$x^4+[2]_5=x^4+(b-a^2+[2]_5\cdot b^{-1})x^2+(-ab+[2]_5\cdot ab^{-1})x+[2]_5.$$

Thus $-ab+[2]_5\cdot ab^{-1}=a(-b+[2]_5\cdot b^{-1})=0$ and

- if $a = 0$, then $b^2 = -[2]_5$, a contradiction.
- if $-b + [2]_5 b^{-1} = 0$, then $b^2 = [2]_5$, a contradiction.

We conclude that f is irreducible in $\mathbb{F}_5[x]$.

Lastly, let $x^4 + 15x^3 + 7 \in \mathbb{Q}[x]$. As the dominant coefficient is 1, this polynomial is primitive, hence it is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Lemma 3.8.13). Let $\phi_5 : \mathbb{Z} \to \mathbb{F}_5$ be the quotient homomorphism and let $\pi_5 : \mathbb{Z}[x] \to \mathbb{F}_5[x]$ be its induced homomorphism. We have that:

$$\pi_5(x^4 + 15x^3 + 7) = x^4 + [2]_5$$

and, as $x^4 + [2]_5$ is irreducible in $\mathbb{F}_5[x]$, we use Proposition 3.9.1 to conclude that $x^4 + 15x^3 + 7$ is irreducible in $\mathbb{Z}[x]$.

(c) First we note that $x^2 + y^2 + 1 \in \mathbb{R}[x, y]$ is primitive as its dominant coefficient is 1. Secondly, $y^2 + 1 \in \mathbb{R}[y]$ is irreducible. We now apply Eisenstein with $p = y^2 + 1$ to conclude that $x^2 + y^2 + 1$ is irreducible in $\mathbb{R}[x, y]$.

(d) We have $x^2 + y^2 + [1]_2 = (x + y + [1]_2)^2$ in $\mathbb{F}_2[x, y]$.

(e) The evaluation homomorphism $\mathrm{ev}_0 : \mathbb{Q}[y] \to \mathbb{Q}$, $\mathrm{ev}_0(y) = 0$, induces the homomorphism $\xi : \mathbb{Q}[y][x] \to \mathbb{Q}[x]$ with $\xi(y) = 0$ and $\xi(x) = x$. We have that:

$$\xi(y^4 + x^3 + x^2y^2 + xy + 2x^2 - x + 1) = x^3 + 2x^2 - x + 1$$

and, by Proposition 3.9.1, $y^4 + x^3 + x^2y^2 + xy + 2x^2 - x + 1$ is irreducible in $\mathbb{Q}[x, y]$ if $x^3 + 2x^2 - x + 1$ is irreducible in $\mathbb{Q}[x]$. Now $\deg(x^3 + 2x^2 - x + 1) = 3$ and thus $x^3 + 2x^2 - x + 1$ is irreducible in $\mathbb{Q}[x]$ if and only if it does not admit roots in $\mathbb{Q}$. Assume $\frac{p}{r} \in \mathbb{Q}$, where $p, r \in \mathbb{Z}$ and $\gcd(p, r) = 1$, is a root of $x^3 + 2x^2 - x + 1$. Then

$$\left(\frac{p}{r}\right)^3 + 2\left(\frac{p}{r}\right)^2 - \left(\frac{p}{r}\right) + 1 = 0.$$

As $\gcd(p, r) = 1$, it follows that $p|1$, $r|1$ and so $\frac{p}{r} \in \{-1, 1\}$. One checks that neither -1, nor 1 is a root of $x^3 + 2x^2 - x + 1$ and thus $x^3 + 2x^2 - x + 1$ is irreducible in $\mathbb{Q}[x]$.

(f) We have $4x^3 + 120x^2 + 8x - 12 = 4(x^3 + 30x^2 + 2x - 3) \in \mathbb{Q}[x]$. Now $4 \in \mathbb{Q}[x]^\times$ and so $4x^3 + 120x^2 + 8x - 12$ is irreducible in $\mathbb{Q}[x]$ if and only if $x^3 + 30x^2 + 2x - 3$ is. As $\deg(x^3 + 30x^2 + 2x - 3) = 3$ it follows that $x^3 + 30x^2 + 2x - 3$ is irreducible in $\mathbb{Q}[x]$ if and only if it does not admit roots in $\mathbb{Q}$. Assume there exist $\frac{p}{r} \in \mathbb{Q}$, where $p, r \in \mathbb{Z}$ and $\gcd(p, r) = 1$, such that:

$$\left(\frac{p}{r}\right)^3 + 30\left(\frac{p}{r}\right)^2 + 2\left(\frac{p}{r}\right) - 3 = 0.$$

As $\gcd(p, r) = 1$, it follows that $p|3$ and $r|1$. Therefore $\frac{p}{r} \in \{-3, -1, 1, 3\}$. One checks that none of the elements in $\{-3, -1, 1, 3\}$ is a root of $x^3 + 30x^2 + 2x - 3$. We conclude that $x^3 + 30x^2 + 2x - 3$ is irreducible in $\mathbb{Q}[x]$. .

(g) As the polynomial $t^6 + t^3 + 1$ is primitive, it follows that it is irreducible in $\mathbb{Q}[t]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Lemma 3.8.13). We consider the quotient homomorphism $\phi_2 : \mathbb{Z} \to \mathbb{F}_2$ and its induced homomorphism $\pi_2 : \mathbb{Z}[t] \to \mathbb{F}_2[t]$ under which

$$\pi_2(t^6 + t^3 + 1) = t^6 + t^3 + [1]_2.$$

By Proposition 3.9.1, $t^6 + t^3 + 1$ is irreducible in $\mathbb{Z}[t]$ if $t^6 + t^3 + [1]_2$ is irreducible in $\mathbb{F}_2[t]$.

Now, one checks that $t^6 + t^3 + [1]_2$ does not admit roots in $\mathbb{F}_2[t]$. Secondly, the only irreducible polynomial of degree 2 in $\mathbb{F}_2[t]$ is $t^2 + t + [1]_2$ and one checks that this does not divide

$t^6+t^3+[1]_2$. Lastly, we assume that $t^6+t^3+[1]_2$ is a product of two polynomials of degree 3. As $\mathbb{F}_2$ is a field, we can assume that these polynomials are unitary and we have:

$$\begin{aligned} t^6+t^3+[1]_2 &= (t^3+a_2t^2+a_1t+a_0)(t^3+b_2t^2+b_1t+b_0) \\ &= t^6+(a_2+b_2)t^5+(a_1+a_2b_2+b_1)t^4+(a_0+a_1b_2+a_2b_1+b_0)t^3+ \\ &\quad +(a_0b_2+a_1b_1+a_2b_0)t^2+(a_0b_1+a_1b_0)t+a_0b_0. \end{aligned}$$

Then $a_0=b_0=[1]_2$, $a_2=b_2$ and

$$\begin{cases} a_0b_1+a_1b_0=[0]_2 \\ a_0b_2+a_1b_1+a_2b_0=[0]_2 \\ a_0+a_1b_2+a_2b_1+b_0=[1]_2 \\ a_1+a_2b_2+b_1=[0]_2 \end{cases} \to \begin{cases} b_1+a_1=[0]_2 \\ a_1b_1=[0]_2 \\ b_2(a_1+b_1)=[1]_2 \\ a_2b_2=[0]_2 \end{cases} \to [1]_2=[0]_2.$$

We conclude that $t^6+t^3+[1]_2$ is irreducible in $\mathbb{F}_2[t]$.

(h) We first note that the ring $\mathbb{Q}[x]$ is factorial, as $\mathbb{Q}$ is (Theorem 3.8.1), and that $x\in\mathbb{Q}[x]$ is irreducible. Secondly the polynomial $y^4+xy^3+xy^2+x^2y+3x^2-2x\in\mathbb{Q}[x,y]$ is primitive, as its dominant coefficient is 1. We now apply Eisenstein with $p=x$ to conclude that $y^4+xy^3+xy^2+x^2y+3x^2-2x$ is irreducible in $\mathbb{Q}[x,y]$.

Exercice 4.
Let $f(t)=t^4+4t^3+3t^2+7t-4\in\mathbb{Z}[t]$.

(a) We have $\pi_2(f(t))=t^4+t^2+t=t(t^3+t+[1]_2)\in\mathbb{F}_2[t]$. Moreover, we remark that $t^3+t+[1]_2$ is irreducible in $\mathbb{F}_2[t]$, as it does not admit roots in $\mathbb{F}_2$.

(b) We have $\pi_3(f(t))=t^4+t^3+t-[1]_3=(t^2+[1]_3)(t^2+t-[1]_3)\in\mathbb{F}_3[t]$.

(c) Assume that $f(t)$ is reducible in $\mathbb{Z}[t]$. Then either $f(t)=(t-a)g(t)$, where $a\in\mathbb{Z}$ and $g(t)\in\mathbb{Z}[t]$ is a polynomial of degree 3, or $f(t)=f_1(t)f_2(t)$, where $f_1(t),f_2(t)\in\mathbb{Z}[t]$ are two polynomials of degree 2.

In the first case, $a|4$ but none of the elements of $\{\pm1,\pm2,\pm4\}$ are roots of f. Hence, we only need to consider the case when $f(t)=f_1(t)f_2(t)$, where $\deg(f_1(t))=\deg(f_2(t))=2$, and we have:

$$\pi_2(f(t))=\pi_2(f_1(t)f_2(t))=\pi_2(f_1(t))\pi_2(f_2(t).$$

Now, as $\deg(\pi_2(f(t)))=4$ and as $\deg(\pi_2(f_1(t)))=\deg(\pi_2(f_2(t)))\leq 2$, it follows that $\deg(\pi_2(f_1(t)))=2$ and $\deg(\pi_2(f_2(t)))=2$.

On the other hand, we have $\pi_2(f(t))=t^4+t^2+t=t(t^3+t+[1]_2)$, where $t^3+t+[1]_2\in\mathbb{F}_2[t]$ is irreducible. We have arrived at a contradiction. We conclude that $f(t)\in\mathbb{Z}[t]$ is irreducible.