Exercises 23

② $3x^2+2x-3 \overline{)\, x^6+3x^5+4x^2-3x+2}$

$5x^4+5x^2+4$

$-(x^6+3x^5-x^4)$

$x^4+0x^3+4x^2$

$-(x^4+3x^3-x^2)$

$5x^2-3x+2$

$-(5x^2+x-5)$

$3x+3$

$q(x)=5x^4+5x^2+4$, $r(x)=3x+3$

⑨ $(1)^4+4=1+4=0 \Rightarrow x-1$ is a factor
$(2)^4+4=1+4=0 \Rightarrow x-2$ is a factor
$(3)^4+4=1+4=0 \Rightarrow x-3$ is a factor
$(4)^4+4=1+4=0 \Rightarrow x-4$ is a factor

Thus, $x^4+4=(x-1)(x-2)(x-3)(x-4)$

(note: there are many ways to factor this. For ex, $x^2+4=x^2-1$, since $4\equiv -1 \pmod 5$, so it is a difference of perfect squares)

⑪ $2x^3+3x^2-7x-5=(x-3)(x-4)(x-8)$ (method: guess & check zeros to find linear factors)

⑫ No. $2^3+2\cdot 2+3=3+4+3=0 \Rightarrow x-2$ is a factor.
$x^3+2x+1=(x-2)(x^2+2x+1)$ (by polynomial long division).
$=(x-2)(x+1)^2$. [NOTE: This is equal to $(x+3)(x+1)^2$.]

⑭ $f(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's criteria w/ $p=2$. Also, if $f(x)$ has a root in $\mathbb{Q}$ it has a root in $\mathbb{Z}$, which can only be $\pm 1, \pm 2$, & one can check that none of these are zeros.

$f(x)$ is reducible over $\mathbb{R}$: $f(x)=x^2+8x-2=(x+4-3\sqrt{2})(x+4+3\sqrt{2})$
thus $f(x)$ is also reducible over $\mathbb{C}$.

⑰ A root in $\mathbb{Z}$ would have to be ± 1, neither of which work. Since a root in $\mathbb{Q}$ implies a root in $\mathbb{Z}$, it follows that $x^4-22x+1$ has no linear factors.
Suppose $x^4-22x+1=(x^2+bx+c)(x^2+dx+e)$, where $b,c,d,e \in \mathbb{Z}$.
$=x^2+(d+b)x^3+(e+c+bd)x^2+(be+cd)x+ce$
Then $d+b=0$, $e+c+bd=0$, $be+cd=22$, & $ce=1$.
Then $d=-b$ & $c=e=1$ or $c=e=-1$, so $be+cd=e(b+d)=0\neq 22$, which is a contradiction.
Therefore $x^4+22x+1$ does not factor over $\mathbb{Z}$, & thus it does not factor over $\mathbb{Q}$, either, as we proved in class.

⑳ No: the only p s.t. $-9, 24, 18 \equiv 0 \pmod p$ is $p=3$ (b/c this is the only prime dividing 9), & $18\equiv 0 \pmod 9$, so Eisenstein's criteria are not satisfied.

㉑ Yes, Eisenstein's criteria are satisfied with $p=5$.

㉞ Let $a \in \mathbb{Z}_p$. x^p+a is reducible over $\mathbb{Z}_p[x]$ $\Leftrightarrow$ it has a zero. Since $\mathbb{Z}_p$ is a ring, $-a \in \mathbb{Z}_p$, & $(-a)^p+a=-a+a=0$. Therefore x^p+a is reducible for every $a \in \mathbb{Z}_p$.

(35) $a_n + a_{n-1}(\frac{1}{a}) + \cdots + a_0(\frac{1}{a})^n = a_n + \frac{a_{n-1}}{a} + \cdots + \frac{a_0}{a^n}$. Thus,

$a^n\left(a_n + a_{n-1}(\frac{1}{a}) + \cdots + a_0(\frac{1}{a})^n\right) = a_n a^n + a_{n-1}a^{n-1} + \cdots + a_0 = 0$, since a is a zero of $f(x)$. Since $a \neq 0$ & F has no zero divisors, it follows that $a_n + a_{n-1}(\frac{1}{a}) + \cdots + a_0(\frac{1}{a})^n = 0 \Rightarrow 1/a$ is a zero, as desired.

Exercises 22

(5) Let $f(x) \in \mathbb{Z}_2[x]$ be a polynomial of degree ≤ 3. Then $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ where $a_3, a_2, a_1, a_0 \in \mathbb{Z}_2$. Thus we have two choices ($\bar{0}$ or $\bar{1}$) for each a_i. Therefore there are $2^4 = 16$ such polynomials.

(7) $\phi_2(x^2+3) = (2)^2 + 3 = 4 + 3 = 7$

(8) $\phi_i(2x^3 - x^2 + 3x + 2) = 2(i)^3 - (i)^2 + 3(i) + 2 = -2i + 1 + 3i + 2 = i + 3$.

(12) $f(x) = x^2 + 1$ in $\mathbb{Z}_2$.
$f(0) = 0^2 + 1 = 1$
$f(1) = 1^2 + 1 = 1 + 1 = 0$
$\Rightarrow$ the only zero is 1.

(15) $f(x)g(x)$, $f(x) = x^3 + 2x^2 + 5$, $g(x) = 3x^2 + 2x$ in $\mathbb{Z}_7$.

a is a zero of $f(x)g(x) \Leftrightarrow a$ is a zero of $f(x)$ or of $g(x)$
zeros of $f(x)$: $f(0) \neq 0$, $f(1) \neq 0$, $f(2) = 1 + 1 + 5 = 0$, $f(3) = 6 + 4 + 5 \neq 0$,
$f(4) = 1 + 4 + 5 \neq 0$, $f(5) = 6 + 1 + 5 \neq 0$, $f(6) = 6 + 2 + 5 \neq 0$
$\Rightarrow$ zero of $f(x)$ is 2.
zeros of $g(x)$: $g(x) = x(3x + 2)$ $g(0) = 0$, $g(1) = 3 + 2 \neq 0$, $g(2) = 2 \cdot 1 \neq 0$, $g(3) = 3 \cdot 4 \neq 0$
$g(4) = 4 \cdot 0 = 0$, $g(5) = 5 \cdot 3 \neq 0$, $g(6) = 6 \cdot 6 \neq 0$
$\Rightarrow$ zero of $g(x)$ are 0 & 4
So the zeros of $f(x)g(x)$ are 0, 2, & 4.

(24) Suppose D is an integral domain. Let $f(x), g(x) \in D[x]$ be such that $f(x) \neq 0$, and $g(x) \neq 0$. We will show $f(x)g(x) \neq 0$, which proves the result.
Let $f(x) = a_nx^n + \cdots + a_1x + a_0$ & $g(x) = b_mx^m + \cdots + b_1x + b_0$, $b_i, a_i \in D$, $a_n \neq 0$ & $b_m \neq 0$.
Then $f(x)g(x) = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right)$

$$= \sum_{k=0}^{n+m}\left(\sum_{l=0}^{k} a_l\, b_{k-l}\right) x^k$$

So the coefficient of x^{n+m} in $f(x)g(x)$ is a_nb_m. Since $a_n \neq 0$ & $b_m \neq 0$, the fact that D is an integral domain implies that $a_nb_m \neq 0$. Therefore, $f(x)g(x) \neq 0$.

(25) (a) Units in $D[x]$ are units in D: if the degree of $f(x) \in D[x]$ is ≥ 1, then for any $g(x) \in D[x] \setminus \{0\}$, the degree of $f(x)g(x) \geq \deg(f(x)) \geq 1$, so $f(x)g(x) \neq 1$. Thus if $f(x)$ is a unit in $D[x]$, we must have $f(x) \in D \Rightarrow f(x)$ is a unit in D. Conversely, if $a \in D$ is a unit, then $\exists b \in D$ s.t. $ab = 1_D$. Since $1_{D[x]} = 1_D$, a is a unit in $D[x]$.

(b) Units in $\mathbb{Z}[x]$ are ± 1

(c) Units in $\mathbb{Z}_7[x]$ are $1, 2, 3, 4, 5, 6$ (since 7 is prime, $\mathbb{Z}_7$ is a field, so every non-zero elt is a unit).

(29) It is clear that R^R is closed under both $+$ & $\cdot$.

- $(R^R, +)$ is an abelian gp:
  - assoc: Let $\varphi, \psi, \theta : R \to R$. Then for any $r \in R$,
    $$[(\varphi + \psi) + \theta](r) = (\varphi+\psi)(r) + \theta(r) = (\varphi(r) + \psi(r)) + \theta(r)$$
    $$= \varphi(r) + (\psi(r) + \theta(r)) \text{ because } (R,+) \text{ is a gp}$$
    $$= \varphi(r) + (\psi+\theta)(r) = [\varphi + (\psi+\theta)](r). \checkmark$$
  - $+$ is commutative: Let $\varphi, \psi : R \to R$. Then $\forall r \in R$,
    $$(\varphi+\psi)(r) = \varphi(r) + \psi(r) = \psi(r) + \varphi(r) = (\psi+\varphi)(r) \checkmark$$
    (b/c $(R,+)$ abel. gp)
  - identity: Let $0 : R \to R$ be defined by $0(r) = 0$ $\forall r \in R$. Then for any $\psi : R \to R$, $(0+\psi)(r) = 0(r) + \psi(r) = 0 + \psi(r) = \psi(r)$, so 0 is the identity.
  - inverses: Let $\varphi \in R^R$, & define $(-\varphi) : R \to R$ by $(-\varphi)(r) = -\varphi(r)$. Then $(\varphi + (-\varphi))(r) = \varphi(r) + (-\varphi)(r) = \varphi(r) - \varphi(r) = 0$ $\forall r \in R$, so $\varphi + (-\varphi) = 0$ & $-\varphi$ is the inverse of φ.

  Thus $(R,+)$ is an abel. gp
- Associativity of $\cdot$: Let $\varphi, \psi, \theta \in R^R$. Then $\forall r \in R$,
  $$(\varphi(\psi\theta))(r) = \varphi(r)(\psi\theta)(r) = \varphi(r)[\psi(r)\theta(r)]$$
  $$= [\varphi(r)\psi(r)]\theta(r) \quad \text{b/c } (R,+,\cdot) \text{ is a ring.}$$
  $$= (\varphi\psi)(r)\,\theta(r)$$
  $$= ((\varphi\psi)\theta)(r) \checkmark$$
- Left distributivity: Let $\varphi, \psi, \theta \in R^R$. Then $\forall r \in R$,
  $$[\varphi(\psi+\theta)](r) = \varphi(r) \cdot (\psi+\theta)(r)$$
  $$= \varphi(r)(\psi(r) + \theta(r))$$
  $$= \varphi(r)\psi(r) + \varphi(r)\psi(r) \text{ b/c } R \text{ is a ring}$$
- Right dist. is similar

Therefore, $(R^R, +, \cdot)$ is a ring.

(30) (a) We first show P_F is a subgp of F^F:
- closed: Let $\varphi, \psi \in P_F$. Then $\exists f(x), g(x) \in F[x]$ s.t. $\varphi(a) = f(a)$ & $\psi(a) = g(a)$ $\forall a \in F$. Thus $\forall a \in F$,
  $(\varphi+\psi)(a) = \varphi(a) + \psi(a) = f(a) + g(a) = (f+g)(a)$. Since $(f+g)(x) \in F[x]$, $\varphi + \psi \in P_F$.
- identity: The identity (under $+$) of F^F is the zero map $0 : F \to F$, as shown in #29. This map clearly agrees with the zero polynomial, so $0 \in P_F$.
- inverses: Let $\varphi \in P_F$. Then $\exists f(x) \in F[x]$ s.t. $\varphi(a) = f(a)$ $\forall a \in F$. The inverse of φ in F^F is $-\varphi$, as shown in #29. $\forall a \in F$,
  $(-\varphi)(a) = -\varphi(a) = -f(a) = (-f)(a)$. Since $-f(x) \in F[x]$, $-\varphi \in P_F$.

Therefore P_F is a subring of F^F.
To show P_F is a subring, we must show it is closed under $\cdot$.
Let $\varphi, \psi \in P_F$. Then $\exists\, f(x), g(x) \in F[x]$ s.t. $\varphi(a) = f(a)$ & $\psi(a) = g(a)$ $\forall a \in F$. Thus $\forall a \in F$,
$(\varphi\psi)(a) = \varphi(a)\psi(a) = f(a)\,g(a) = (fg)(a)$. Since $fg(x) \in F[x]$, $\varphi\psi \in P_F$.
Therefore, P_F is a subring of F^F.

(51) (a) $\mathbb{Z}_2^{\mathbb{Z}_2}$: $\mathbb{Z}_2$ has 2 elements, $\bar{0}$ & $\bar{1}$. An elt $\varphi \in \mathbb{Z}_2^{\mathbb{Z}_2}$ can map each of $\bar{0}$ & $\bar{1}$ to either $\bar{0}$ or $\bar{1}$. So we have 2 choices for each $\bar{0}$ & $\bar{1}$, which gives 4 total choices for φ. Thus $|\mathbb{Z}_2^{\mathbb{Z}_2}| = 4$
[Note: we do not require φ to be a ring hom. in the definition of F^F.]
$\mathbb{Z}_3^{\mathbb{Z}_3}$: By a similar reasoning, we have 3 choices for where an elt $\psi \in \mathbb{Z}_3^{\mathbb{Z}_3}$ can map each of $\bar{0}, \bar{1}, \& \bar{2}$. Thus $|\mathbb{Z}_3^{\mathbb{Z}_3}| = 9$.