Math 422 Homework List

§23 #'s ~~6~~, ~~7~~, ~~9~~, ~~14~~, ~~16~~, ~~18~~, ~~19~~, ~~28~~, ~~34~~, ~~36~~

pg. 175 #20 (§18), also ~~§18 #'s 15, 19, 23, 24,~~

§18 #'s ~~15~~, ~~19~~, ~~20a~~, ~~23~~, ~~24~~, ~~35~~, ~~46~~, ~~49a~~, ~~49~~, ~~53~~

§22 # ~~22~~, ~~24~~, ~~25~~, ~~27~~, ~~29~~, ~~30~~

Lemma 21.3b # ~~1~~, ~~6~~, ~~7~~

§21 proofs for fields of quotients (distributivity of addition, commutative addition & multiplication

~~§22.4~~ Th^{m} 22.4 Proof.

Th^{m} 23.20 Proof.

§24 # ~~16~~, ~~17~~

§18 Selected Problems from Fraleigh's Abstract Algebra

§18 #15 Describe all units in $\mathbb{Z}\times\mathbb{Z}$.

A "unit" in $\mathbb{Z}\times\mathbb{Z}$ is an element (a,b) s.t. $\exists (c,d)$ with $(a,b)\cdot(c,d) = (1,1)$. We need to solve in $\mathbb{Z}$,

$$(ac, bd) = (1,1) \iff \left\{\begin{matrix} ac = 1 \\ bd = 1 \end{matrix}\right\} \iff \left\{\begin{matrix} a = c = \pm 1 \\ b = d = \pm 1 \end{matrix}\right\}$$

thus the units are $\boxed{(1,1), (1,-1), (-1,1), (-1,-1)}$

§18 #19 Find units in $\mathbb{Z}_4$

$U(4) = \{1,3\}$. Notice $3\cdot 3 = 9 = 1 \mod(4)$. In contrast 2 not a unit since $\nexists m \in \mathbb{Z}_4$ s.t. $2m = 1 \mod(4)$.

Units are $\boxed{1 \text{ and } 3}$

§18 #20a Consider matrix ring $M_2(\mathbb{Z}_2)$, find its order

$$M_2(\mathbb{Z}_2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle/ a,b,c,d \in \mathbb{Z}_2 \right\} \text{ has order } 2^4 = 16.$$

$$= \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \right.$$
$$\left. \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

By the way, you can prove $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ makes sense if we interpret the formula correctly in the context of $\mathbb{Z}_2$.

§18 #23 Describe all ring homomorphisms of $\mathbb{Z}$ into $\mathbb{Z}$.

Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be a homomorphism. Then $\phi(1) = \phi(1\cdot 1) = \phi(1)\phi(1)$ thus $\phi(1) = x$ satisfies $x = x^2 \Rightarrow x^2 - x = x(x-1) = 0 \therefore \phi_0(1) = 0$ or $\phi_1(1) = 1$.

Then if $\phi_0(1) = 0$ we find $\phi_0(n) = \phi_0\left(\sum_{k=1}^{n} 1\right) = \sum_{k=1}^{n} \phi_0(1) = 0$.

Whereas $\phi_1(n) = \phi_1\left(\sum_{k=1}^{n} 1\right) = \sum_{k=1}^{n} \phi_1(1) = \sum_{k=1}^{n} 1 = n$. Since ring homomorphisms have $\phi(-x) = -\phi(x)$ it follows that $\forall z \in \mathbb{Z}$ $\phi_0(z) = 0$ or $\phi_1(z) = z$. Hence $\boxed{\phi_0 = 0 \text{ or } \phi_1 = id}$

§18#24 Describe all ring homomorphisms from $\mathbb{Z}$ into $\mathbb{Z}\times\mathbb{Z}$.

Same trick as # 23. If $\phi: \mathbb{Z} \longrightarrow \mathbb{Z}\times\mathbb{Z}$ a homomorphism then $\phi(1) = \phi(1\cdot 1) = \phi(1)\,\phi(1) = \phi(1)^2$. Suppose $\phi(1)=(a,b)$.

We need

$$(a,b)^2 = (a,b)$$

$$(a^2, b^2) = (a,b)$$

$$\left\{\begin{matrix} a^2 = a \\ b^2 = b \end{matrix}\right\}$$

In $\mathbb{Z}$ this has sol^n's $(a,b) = (0,0), (0,1), (1,0), (1,1)$.

These correspond to the zero map, π_1, π_2, id.

$$0(n) = 0$$
$$\pi_1(z) = (z,0)$$
$$\pi_2(z) = (0,z)$$
$$id(z) = (z,z).$$

§18#35 Show that ϕ_a of Ex 18.10 satisfies $\phi_a(zw) = \phi_a(z)\phi_a(w)$

$\phi_a : \mathbb{R}^{\mathbb{R}} \longrightarrow \mathbb{R}$ defined by $f \in \mathbb{R}^{\mathbb{R}}$ has $\phi_a(f) = f(a)$.

Let $f, g \in \mathbb{R}^{\mathbb{R}}$ then $\phi_a(fg) = (fg)(a) = f(a)g(a) = \phi_a(f)\phi_a(g)$.

§18#40 Show that $2\mathbb{Z}$ and $3\mathbb{Z}$ are <u>not</u> isomorphic as rings. Also show the fields $\mathbb{R}$ and $\mathbb{C}$ are <u>not</u> isomorphic

- Usually these sort of questions are resolved by exhibiting a property which holds for one item but is <u>impossible</u> for the other.
- $2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$ whereas $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \dots\}$

neither of these has 1 this time, I'll need something else...

$$2+2 = 4 \qquad 3+3 = 6$$
$$2\cdot 2 = 4 \qquad 3\cdot 3 = 9$$

If $\phi(2) = 3$ then $\phi(2\cdot 2) = \phi(2+2) \Rightarrow 9 = 6$ oops.

§18#40 We can argue that $\phi : 2\mathbb{Z} \longrightarrow 3\mathbb{Z}$ must map $\phi(2) = \pm 3$. Otherwise the map will not be onto $3\mathbb{Z}$. Then since

$$2+2=4 \qquad 3+3=6$$
$$2\cdot 2=4 \qquad 3\cdot 3=9$$

It follows $\phi(2)=3$ get's us into trouble as we need

$$\phi(2^2) = \phi(2)\phi(2) = 3\cdot 3 = 9$$
$$\phi(2^2) = \phi(2+2) = \phi(2)+\phi(2) = 6$$

$\therefore$ no isomorphism from $2\mathbb{Z}$ to $3\mathbb{Z}$ exists. $2\mathbb{Z} \not\cong 3\mathbb{Z}$.

(Remark: there are a few holes in this sol^n.) I half-stole it from answer key.

Alternatively: (probably using things we shouldn't know yet)

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\gamma_2"] \arrow[dr, "\pi_2"'] & 2\mathbb{Z} \arrow[r, "\phi"] & 3\mathbb{Z} & \mathbb{Z} \arrow[l, "\gamma_3"'] \arrow[dl, "\pi_3"] \\
& \mathbb{Z}/\ker\gamma_2 \arrow[u, dashed, "\psi_2"'] \arrow[rr, "\psi_1^{-1}\circ\phi\circ\psi_2"'] & & \mathbb{Z}/\ker\gamma_3 \arrow[u, dashed, "\psi_1"]
\end{tikzcd}$$

Recall that
$\mathbb{Z}/\ker\gamma_2 = \mathbb{Z}_2$
$\mathbb{Z}/\ker\gamma_3 = \mathbb{Z}_3$.

Where $\gamma_2(n) = 2n$ and $\gamma_3(n) = 3n$ are clearly onto $2\mathbb{Z}$ and $3\mathbb{Z}$ respective. If ϕ we an isomorphism then $\psi_1^{-1}\circ\phi\circ\psi_2 : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_3$ would be an isomorphism from $\mathbb{Z}_2$ to $\mathbb{Z}_3$. This is impossible since $|\mathbb{Z}_2| = 2$ whereas $|\mathbb{Z}_3| = 3$.

What about $\mathbb{R}$ and $\mathbb{C}$? Clearly the thing that makes $\mathbb{C}$ different is $i = \sqrt{-1}$ with $i^2 = -1$. Suppose $\mathbb{C} \cong \mathbb{R}$ as fields then $\exists\, \varphi : \mathbb{C} \longrightarrow \mathbb{R}$

$$\varphi(1) = \varphi(1)\varphi(1) = \varphi(-i^2) = -\varphi(i)\varphi(i)$$

We know $\varphi(1) = 1$ since $\varphi(1) = 0$ does not give isomorphism. Then $-\varphi(i)\varphi(i) = 1 \Rightarrow (\varphi(i))^2 = -1$ for some $\varphi(i) \in \mathbb{R}$. Of course this has no sol^n's. Thus $\mathbb{C} \not\cong \mathbb{R}$.

§18 # 44a) An element a of a ring R is idempotent if $a^2 = a$. Show that $\mathcal{I} = \{r \in R \mid r^2 = r\}$ has $\mathcal{I}\mathcal{I} \subseteq \mathcal{I}$. given R is a commutative ring

Let $a, b \in \mathcal{I}$ then $(ab)^2 = (ab)(ab) = aa\,bb = a^2 b^2 = ab$

using R commutative.

Thus $a, b \in \mathcal{I} \Rightarrow (ab) \in \mathcal{I}$ $\therefore$ $\mathcal{I}\mathcal{I} \subseteq \mathcal{I}$.

Remark: $\mathcal{I}$ not a subring. $\mathcal{I}(\mathbb{Z}) = \{1, -1\}$ yet $1+1 \notin \mathcal{I}(\mathbb{Z})$.

§18 # 49) We did this in lecture.

§18 # 53) We did this in lecture also. (do # 52 to warm up to it).

What about § 19, 20, 21 homeworks?

§19 # 10) Find $\text{char}(\mathbb{Z}_6 \times \mathbb{Z}_{15})$. Observe $(1,1)$ is the identity element in $\mathbb{Z}_6 \times \mathbb{Z}_{15}$. We want smallest $n \in \mathbb{Z}$ such that $n \cdot (1,1) = 0$. This means we want to solve $(n, n) = (0, 0)$ in $\mathbb{Z}_6 \times \mathbb{Z}_{15}$ hence solve $n = 0 \bmod (6)$ <u>and</u> $n = 0 \bmod (15)$. The $\text{lcm}(6, 15) = 30$. This is the smallest sol$^{\underline{n}}$ to the system of congruences.

---

§21 #1 Describe the field of quotients F for the integral subdomain $D = \{n + mi \mid n, m \in \mathbb{Z}\}$ of $\mathbb{C}$.

In the obtuse langauge of §22 an element of F looks like $(n+mi, a+bi)$ for $a, b, m, n \in \mathbb{Z}$ such that $a+bi \neq 0$. A more traditional notation will serve us better,

$$(n+mi, a+bi) = \frac{n+mi}{a+bi}$$

Moreover, we can multiply by $\frac{a-bi}{a-bi}$ to see,

$$\left(\frac{n+mi}{a+bi}\right)\left(\frac{a-bi}{a-bi}\right) = \frac{an + i(am-bn)}{a^2+b^2}$$

Thus, without loss of generality if $f \in F$ then $\exists\, x, y, z \in \mathbb{Z}$ such that

$$f = \frac{x+iy}{z} = \frac{x}{z} + i\frac{y}{z}$$

Thus $f = p + iq$ for $p, q \in \mathbb{Q}$

§21 #2 Describe field of quotients for integral subdomain $D = \{n + m\sqrt{2} \mid n, m \in \mathbb{Z}\}$ of $\mathbb{C}$

Let $a, b, c, d \in \mathbb{Z}$ then $\frac{a+\sqrt{2}b}{x+\sqrt{2}y} \in F$ but notice that

$$\frac{a+\sqrt{2}b}{x+\sqrt{2}y}\left(\frac{x-y\sqrt{2}}{x-y\sqrt{2}}\right) = \frac{ax - 2by + (bx-ay)\sqrt{2}}{x^2+2y^2} = p + q\sqrt{2}$$

So just like #1, $f \in F \Rightarrow f = p + q\sqrt{2}$ for some $p, q \in \mathbb{Q}$.

Remark: Notice that both i and $\sqrt{2}$ are algebraic over $\mathbb{Q}$. We discover later that

$$D = \mathbb{Q}[x]/\langle x^2+1\rangle \quad \text{(for \#1)} \qquad D = \mathbb{Q}[x]/\langle x^2-2\rangle$$

then the field of quotients is developed as described in §21. Notice that the net-effect is to join an element to $\mathbb{Q}$

$$F = \mathbb{Q} \oplus i\mathbb{Q} \quad \text{(for \#1)} \qquad F = \mathbb{Q} \oplus \sqrt{2}\,\mathbb{Q} \quad \text{(for \#2)}$$

§21#6 Prove part 2 of step 3 in the field of quotients construction.

Show addition is associative where we were working with an integral domain D and a set

$$S = \{(a,b) \mid a,b \in D,\ b \neq 0\}$$

on which we defined an equivalence relation $\sim$

$(a,b),(c,d) \in S$ then $(a,b) \sim (c,d)$ iff $ad = bc$.

Then we defined addition and multiplication on $S/\sim$ for $[(a,b)],[(c,d)] \in S/\sim$

$$[(a,b)] + [(c,d)] = [(ad+bc,\ bd)]$$

$$[(a,b)][(c,d)] = [(ac,\ bd)]$$

We already proved these are well-defined in the sense that these rules are independent of representative in $F \equiv S/\sim$

Let $[(a,b)],[(c,d)],[(x,y)] \in F$,

$$[(a,b)]+[(c,d)] = [(ad+bc,\ bd)]$$

$$[(ad+bc,\ bd)] + [(x,y)] = [((ad+bc)y + (bd)x,\ bdy)]$$

Hence,

$$\big([(a,b)] + [(c,d)]\big) + [(x,y)] = [(ady + bcy + bdx,\ bdy)]$$

Likewise, consider

$$[(c,d)] + [(x,y)] = [(cy+dx,\ dy)]$$

$$[(a,b)] + [(cy+dx,\ dy)] = [(ady + b(cy+dx),\ bdy)]$$

Consequently,

$$[(a,b)] + \big([(c,d)] + [(x,y)]\big) = [(ady + bcy + bdx,\ bdy)]$$

Thus addition in F is associative. We need to use associativity of addition in the additive group $\langle D, + \rangle$ many times throughout the calculation above.

§22 # 22 Find a polynomial of nonzero degree in $\mathbb{Z}_4[x]$ that's a unit

We wish to find $f(x)g(x) = 1$ for some $f(x) \in \mathbb{Z}_4[x]$ with $\deg(f) \geq 1$. Try $f(x) = a + bx$ for $a, b \in \mathbb{Z}_4$ and $g(x) = c$

$$f(x)g(x) = (a+bx)c = ac + (bc)x = 1$$

Need $bc = 0$ while $ac = 1$. If $a = 3$ and $c = 3$ then $ac = 9 = 1$.

Can we solve $3b = 0$ simultaneously? Check possibilities

$$3(1) = 3, \quad 3(2) = 6 = 2, \quad 3(3) = 9, \quad 0(3) = 0$$

Nope, this isn't going to work. Let's try $g(x) = c + dx$ instead,

$$f(x)g(x) = (a+bx)(c+dx) = ac + (bc+ad)x + bdx^2$$

need $ac = 1 \Rightarrow a = c = 3$ $(a=1, c=1$ no use$)$

$bc + ad = 0 \Rightarrow \boxed{3b + 3d = 0}$

$bd = 0$ $\quad \boxed{bd = 0}$

← think about this. $b = d = 2$ works. $6 + 6 = 12 = 0$, $2 \cdot 2 = 4 = 0$.

$$\boxed{\text{Thus } f(x) = 3 + 2x \text{ has multiplicative inverse of } g(x) = 3 + 2x, \ f(x) \text{ is a unit.}}$$

§22 # 24 Prove that if D is an integral domain then $D[x]$ is also an integral domain.

If D is an integral domain then D is a commutative ring with no zero divisors. Th^{m} 22.2 in the text assures us that $D[x]$ is a commutative ring. We need only to check for zero divisors. Let $f(x), g(x) \in D[x]$ such that $f(x) = \sum_{k=0}^{\infty} a_k x^n$ and $g(x) = \sum_{j=0}^{\infty} b_j x^j$ where at least one (each) $b_j, a_k \neq 0$. Consider then

$$f(x)g(x) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_i b_{n-i} \right) x^n = 0 \text{ iff } \sum_{i=0}^{n} a_i b_{n-i} = 0$$

for each $n \in \mathbb{N} \cup \{0\}$.

But, $\exists k_0, j_0$ such that $b_{j_0} \neq 0$ and $a_{k_0} \neq 0$ consequently the term $a_{k_0} b_{j_0} \neq 0$ since D an integral domain. Hence $f(x)g(x) \neq 0$, and $D(x)$ an integral domain.

§22 # 25 Let D be an integral domain and x an indeterminant describe a.) units in $D[x]$, b.) units in $\mathbb{Z}[x]$, c.) units in $\mathbb{Z}_7[x]$

a.) the units in $D[x]$ are $f(x) = c \neq 0$ such that c is a unit in D.

b.) units in $\mathbb{Z}[x]$ are $f(x) = \pm 1$.

c.) units in $\mathbb{Z}_7[x]$ are $f(x) = 1, 2, 3, 4, 5, 6$.

<u>Remark:</u> $\mathbb{Z}_4$ is not an integral domain and the fact that $2 \cdot 2 = 0$ even though $2 \neq 0$ was what made $f(x) = 3 + 2x$ a unit in $\mathbb{Z}_4[x]$ which was non simply a unit of $\mathbb{Z}_4$. This cannot happen for an integral domain since the coefficients of the terms with x, x^2 etc... will not be zero in the product $f(x)g(x)$ if $\deg(f), \deg(g) \geq 1$.

§22 # 27 Let F be a field with $\text{char}(F) = 0$ and let

$$D(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_1 + 2a_2x + 3a_3x^2 + \cdots + na_nx^{n-1}$$

a.) show $D: F[x] \to F[x]$ is a group homomorphism of $\langle F[x], + \rangle$

b.) find $\text{Ker}(D)$ c.) find image $F[x]$ under D.

<u>Proof of a.)</u> Note $D\left(\sum_{n=0}^{\infty} a_nx^n\right) = \sum_{n=1}^{\infty} na_nx^{n-1}$. Let $f(x) = \sum_{n=0}^{\infty} a_n$, $g(x) = \sum_{n=0}^{\infty} b_n$

Observe,

$$\begin{aligned} D(f(x) + g(x)) &= D\left(\sum_{n=0}^{\infty} (a_n + b_n)x^n\right) \\ &= \sum_{n=1}^{\infty} n(a_n + b_n)x^{n-1} \\ &= \sum_{n=1}^{\infty} na_nx^{n-1} + \sum_{n=1}^{\infty} nb_nx^{n-1} \\ &= D(f(x)) + D(g(x)). \end{aligned}$$

Also clearly $D(0) = 0$ hence D is an additive group homomorphism of $\langle F[x], + \rangle$. However, $D(1) = 0$ thus it is <u>not</u> a ring homorphism. Rather, $D(fg) = (Df)g + f(Dg)$ this is not the needed property.

b.) $\text{Ker}(D) = \{ f(x) \in F[x] \mid f(x) = c \text{ for some } c \in F \} \cong F$

c.) $D(F[x]) = F[x]$ since $D\left(\frac{1}{n+1} a_nx^{n+1}\right) = a_nx^n$ and $D(1) = 0$ and D is an additive homomorphism.

§22 #29 Let R be a ring and $R^R = \{ f : R \to R \mid f \text{ a function} \}$
For $\phi, \psi \in R^R$ define $\phi + \psi$ and $\phi \cdot \psi$ pointwise. Show that $\langle R^R, +, \cdot \rangle$ is a ring.

+ associative) Let $\phi, \psi, \beta \in R^R$ and let $x \in R$,

$$\begin{aligned}
[(\phi + \psi) + \beta](r) &= (\phi + \psi)(r) + \beta(r) \\
&= (\phi(r) + \psi(r)) + \beta(r) \\
&= \phi(r) + (\psi(r) + \beta(r)) \\
&= \phi(r) + (\psi + \beta)(r) \\
&= [\phi + (\psi + \beta)](r) \quad \therefore (\phi + \psi) + \beta = \phi + (\psi + \beta).
\end{aligned}$$

$\therefore$ (+) associative

Likewise,

$$(\phi + \psi)(r) = \phi(r) + \overbrace{\psi(r) = \psi(r)}^{\text{using } R \text{ has commutative } (+).} + \phi(r) = (\psi + \phi)(r) \quad \forall r \in R$$

Thus $\phi + \psi = \psi + \phi \quad \forall \psi, \phi \in R^R \therefore$ (+) is commutative.

Notice $-1 \cdot \psi$ has $(-1 \cdot \psi)(r) = -\psi(r)$ and clearly
$[\psi + (-1 \cdot \psi)](r) = \psi(r) - \psi(r) = 0 \quad \forall r \in R \therefore R^R$ has additive inverses

Where I just noted $f(r) = 0$ is the additive identity in R^R. Moreover, we knew $\exists (-\psi(r))$ for $\psi(r) \in R$ since R has additive inverses. Finally, it is clear that $(\psi \cdot \phi)(r) = \psi(r)\phi(r)$ does define a function from $R \to R$. Right & Left distributive properties follow from similar arguments.

§22 #30 Let F be a field then $\phi \in F^F$ is a polynomial function on F if $\exists f(x) \in F[x]$ such that $\phi(a) = f(a) \ \forall a \in F$.
a.) show P_F the set of all polynomial functions on F forms subring of F^F
b.) show $P_F \not\cong F[x]$ (for finite field case)

a.) fairly clear. The sum and/or product of polynomials is a polynomial.

b.) Consider $F = \mathbb{Z}_2$. If $f \in P_{\mathbb{Z}_2}$ then $f(x) = mx + b$ because for variables in $\mathbb{Z}_2$ we have $x^2 = x$ thus $f(x) = 1 + x + x^3$ is same as $f(x) = 1 + x + x = 1$.
Note $f(0) = 1$ and $f(1) = 1$ (try any of the formulas)
In contrast, $\mathbb{Z}_2[x]$ is infinite as x and $x + x^3 + x^5$ are distinct.

§23#6 The units of $\mathbb{Z}_7$ are $U(7) = \{1, 2, 3, 4, 5, 6\}$.

§23#9 The polynomial x^4+4 can be factored in $\mathbb{Z}_5[x]$.

$$\left.\begin{aligned} x^4+4 &= x^4+5x^2+4 \\ &= (x^2+1)(x^2+4) \\ &= (x^2+5x+6)(x^2-1) \\ &= (x+3)(x+2)(x+1)(x-1) \\ &= \underline{(x+1)(x+2)(x+3)(x+4)} \end{aligned}\right\}$$

Calculation done in $\mathbb{Z}_5$ where we can add zero $= 5$ all we like.

§23#14 Show that $f(x) = x^2+8x-2$ is irreducible over $\mathbb{Q}$. What about $\mathbb{R}$ or $\mathbb{C}$?

Try to use Th^{m} 23.15 the Eisenstein Criterion. Consider $P=2$ note $a_2 = 1 \not\equiv_2 0$ and $a_1 = 8 \equiv_2 0$ and $a_0 = -2 \not\equiv_4 0$ hence by Eisenstein Criterion x^2+8x-2 is irred. over $\mathbb{Q}$. Over $\mathbb{R}$ we can use quadratic formula or complete square

$$\begin{aligned} x^2+8x-2 &= (x+4)^2-18 \\ &= [(x+4)-\sqrt{18}][(x+4)+\sqrt{18}] \\ &= (x+4-\sqrt{18})(x+4+\sqrt{18}) \end{aligned}$$

Yes it factors over $\mathbb{R}$ and $\mathbb{C}$ hence it is reducible over $\mathbb{R}$ or $\mathbb{C}$.

§23#16 Show x^3+3x^2-8 is irred. over $\mathbb{Q}$

Consider $P=3$ for the Eisenstein Criteria. Note $1 \neq 0 \bmod(3)$ and $3 = 0 \bmod(3)$ however $-8 \neq 0 \bmod(9)$ hence x^3+3x^2-8 is irred. over $\mathbb{Q}$ by the Eisenstein Criteria with $P=3$.

§23#18 Is x^2-12 irred. over $\mathbb{Q}$?

Let $P=7$. Clearly $1 \neq 0$ and $-12 \neq 0 \bmod(49)$ $\therefore$ $\underline{x^2-12 \text{ irred by E.C.}}$

§23#19 Is $8x^3+6x^2-9x+24$ irred. over $\mathbb{Q}$?

Yes. Try $P=3$ to see this is irred.

mod (3) we have $6=0$ and $9=0$

mod (9) we have $24 \neq 0$.

$\boxed{\S 23 \# 28}$ Find all irred. polynomials of degree 3 in $\mathbb{Z}_2[x]$.

If $f(x) \in \mathbb{Z}_2[x]$ and $\deg(f) = 3$ then $\exists a,b,c,d \in \mathbb{Z}_2$ such that $f(x) = ax^3 + bx^2 + cx + d$. Need $a = 1$ clearly. (otherwise $\deg(f) \neq 3$)

$$f_1(x) = x^3$$
$$f_2(x) = x^3 + 1$$
$$f_3(x) = x^3 + x$$
$$f_4(x) = x^3 + x + 1$$
$$f_5(x) = x^3 + x^2$$
$$f_6(x) = x^3 + x^2 + 1$$
$$f_7(x) = x^3 + x^2 + x$$
$$f_8(x) = x^3 + x^2 + x + 1$$

If $f(a) \neq 0 \ \forall a \in \mathbb{Z}_2$ then f is irreducible here.

You can verify then $\boxed{x^3+x+1,\ x^3+x^2+1 \text{ are the irred, deg 3 in } \mathbb{Z}_2[x]}$

$\boxed{\S 23 \# 34}$ Show for a prime p the polynomial $x^p + a$ in $\mathbb{Z}_p[x]$ is <u>not</u> irreducible for any $a \in \mathbb{Z}_p$

$x^2+1 = (x+1)(x+1)$ in $\mathbb{Z}_2[x]$. Consider p prime and $p > 2$. Then p must be odd. Notice $(-a)^p = -a^p$ since p odd.

Why is $x^3 + a$ reducible in $\mathbb{Z}_3[x]$?

$$(x+a)^3 = x^3 + 3x^2a + 3xa + a^3 = x^3 + a.$$

Generally then,

$$(x+a)^p = x^p + px^{p-1}a + \cdots + pxa^{p-1} + a^p = x^p + a^p \text{ in } \mathbb{Z}_p[x]$$

For example, $(x+a)^5 = x^5 + 5ax^4 + 10a^2x^3 + 10a^3x^2 + 5a^4x + a^5$, you can see the terms all are multiples of 5 except x^5 and a^5. The Binomial Theorem gives $\binom{p}{k} = \dfrac{p!}{k!\,(p-k)!}$ which always produces a factor of p except in the cases $k = 0, p$. Thus $(x+a)^p = x^p + a^p$

Finally, $a^p = a$ for $a \in \mathbb{Z}_p$ (for example, $2^3 = 8 = 2 \bmod 3$, $4^5 = 1024 = 4$ etc...)

§23 #36 Let $f(x) \in F[x]$ where F is a field, and let $\alpha \in F$. Show that the remainder $r(x)$ when $f(x)$ is divided by $(x-\alpha)$, in accordance with the division algorithm, is $f(\alpha)$

We know $\exists\, q(x)$ and $c \in F$ such that

$$f(x) = q(x)\,(x-\alpha) + c$$

We defined $f(\alpha) = \phi_\alpha(f(x)) = q(\alpha)(\alpha-\alpha) + c = c$. Thus $f(x) = q(x)(x-\alpha) + f(\alpha)$. In other notation,

$$\frac{f(x)}{x-\alpha} = q(x) + \frac{f(\alpha)}{x-\alpha}$$ where $f(\alpha)$ is the remainder

§24 #10 Let $\mathbb{H} = \{a + bi + cj + dk \mid a,b,c,d \in \mathbb{R}$ and $i^2 = j^2 = k^2 = -1$ and $ij = k,\ jk = i,\ ki = j$ and $ji = -k,\ kj = -i,\ ik = -j\}$

Find two subsets of $\mathbb{H}$ different than $\mathbb{C}$ and each other but isomorphic to $\mathbb{C}$...

Let $S = \{a + cj \mid a, c \in \mathbb{R}\}$ or $S = \{a + dk \mid a, d \in \mathbb{R}\}$ these are distinct from $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$. In truth, $S = \{a + bi \mid a, b \in \mathbb{R}\} \subset \mathbb{R}^4$ is not $\mathbb{C}$ but a copy of $\mathbb{C}$ inside $\mathbb{H}$. Sort of like how $a + 0i \in \mathbb{R}$ inside $\mathbb{C}$.

§2.4 #17 Show $\mathbb{Y}\mathbb{X} - \mathbb{X}\mathbb{Y} = 1$. Here $\mathbb{Y}(f(x)) = f'(x)$ while $\mathbb{X}(f(x)) = x f(x)$. Consider then,

$$\begin{aligned}
(\mathbb{Y}\circ\mathbb{X} - \mathbb{X}\circ\mathbb{Y})(f(x)) &= \mathbb{Y}(\mathbb{X}(f(x))) - \mathbb{X}(\mathbb{Y}(f(x))) \\
&= \mathbb{Y}(x f(x)) - \mathbb{X}(f'(x)) \\
&= \frac{d}{dx}(x f(x)) - x f'(x) \\
&= f(x) + x f'(x) - x f'(x) \\
&= f(x) \quad \therefore \quad \underline{\mathbb{Y}\circ\mathbb{X} - \mathbb{X}\circ\mathbb{Y} = 1}
\end{aligned}$$