Algebra Notes #6. 24

Exercises:
1. P.3
2. P.11
3. P.11
4. P.11
5. P.12
6. P.12
7. P.12

1° Some Number Theory

Recall $p \in \mathbb{N} = \{1, 2, 3, \ldots\}$ natl nos is prime if the only divisors of p are 1 and p (and $p \neq 1$ by convention). $\mathcal{P}$ = the set of prime nos.

$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots\}$

Theorem. If $n \neq 1 \in \mathbb{N}$ (natl nos), then n is a product of prime numbers.

Proof. By induction. We start at $n = 2$. Since 2 is prime, this verifies the bottom of the induction.

Now assume the theorem is true for all $n \in \mathbb{N}$ $(n \neq 1)$ so that $n < N$ for some $N \in \mathbb{N}$. Then either N is itself a prime, or $N = nm$ where $1 < n < N$ and $1 < m < N$. But then by our induction hypothesis n and m are products of primes. Hence $N = nm$ is a product of primes. This completes the proof of this theorem by induction. //

Theorem. If $n < m$, $n, m \in \mathbb{N}$ then $\exists$ unique $r, s \in \mathbb{N} \cup \{0\}$ such that

$$m = rn + s \text{ and } 0 \leq s < n.$$

Proof. By induction. Omitted. //

e.g. $37 = 9 \times 4 + 1$.

When we write $m = rn + s$, $0 \le s < n$, we call s the "remainder on division of m by n". We can also write this in terms of fractions: $\frac{m}{n} = r + \frac{s}{n}$.

e.g. $\frac{37}{4} = 9 + \frac{1}{4}$ $\Longleftrightarrow$ $37 = 4 \times 9 + 1$

An expression of the form

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} \qquad \underset{\text{notation}}{=\!=} [a_1, a_2, \ldots, a_n] \qquad (a_i \in \mathbb{Z})$$

with $a_i \in \mathbb{Z} - \{0\}$ $(i > 1)$ $(\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\})$

is called a <u>continued fraction</u>.

<u>Every fraction can be converted to a continued fraction by successive division + remainder:</u>

e.g. $\frac{37}{5} = 7 + \frac{2}{5} = 7 + \frac{1}{5/2}$

$$= 7 + \cfrac{1}{2 + \frac{1}{2}}$$

$$\frac{37}{5} = [7, 2, 2].$$

Exercise 1. Let $F_n = [\underbrace{1,1,1,\ldots,1}_{n\ 1's}] = 1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{\ddots\ +\frac{1}{1}}}}$.

Thus $F_1 = 1/1$

$F_2 = 1+\frac{1}{1} = 2/1$

$F_3 = 1+\cfrac{1}{1+\frac{1}{1}} = 1+\frac{1}{2} = 3/2$

$F_4 = 1+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{1}}} = 1+\frac{1}{3/2} = 1+\frac{2}{3} = 5/3.$

Let $f_0=1, f_1=1, f_2=2, f_3=3, f_4=5, f_5=8, \ldots$ denote the Fibonacci sequence 1, 1, 2, 3, 5, 8, 13, ...

(a) Prove by induction that

$F_n = f_n/f_{n-1}$ for $n=1,2,3,\ldots$.

(Hint. Show that $F_{n+1} = 1+\frac{1}{F_n}$.)

(b) Assuming that $F = \lim_{n\to\infty} F_n$ exists, prove that

$F = \frac{1+\sqrt{5}}{2}$.

(Hint. Show that $F = 1+\frac{1}{F}$ & note that $F>0$.)

Converting a number to a continued fraction is a process of successive division.

$$\frac{59}{11} = 5 + \frac{4}{11}$$

$$= 5 + \frac{1}{11/4}$$

$$= 5 + \frac{1}{2+\frac{3}{4}} = 5 + \frac{1}{2+\frac{1}{4/3}}$$

$$= 5 + \frac{1}{2+\frac{1}{1+\frac{1}{3}}}$$

$$= [5, 2, 1, 3]$$

$59 = (5) \times 11 + 4$
$11 = (2) \times 4 + 3$
$4 = (1) \times 3 + 1$
$3 = (3) \times 1 + 0$

As you can see, the successive multipliers in the division process are the terms in the continued fraction.

example, 8/5:

$8 = (1) \times 5 + 3$
$5 = (1) \times 3 + 2$
$3 = (1) \times 2 + 1$
$2 = (2) \times 1 + 0$

$8/5 = [1, 1, 1, 2]$
$= [1, 1, 1, 1, 1]$.

In the successive division process you eventually arrive at a remainder of zero. The line just before, with the last non-zero remainder is crucial.

Consider the last example.

(i) $8 = 1 \times 5 + 3$

(ii) $5 = 1 \times 3 + 2$

(iii) $3 = 1 \times 2 + \underbrace{1}_{= d}$ ← last non-zero remainder d.

Consider the following argument:

If $n|8$ and $n|5$ then (i) $\Rightarrow n|3$.

If $n|5$ and $n|3$ then (ii) $\Rightarrow n|2$

If $n|3$ and $n|2$ then (iii) $\Rightarrow n|1$.

Thus if $n|8$ and $n|5$, then $n|1$.

Thus 8 and 5 have only 1 as a common factor. We say that 8 and 5 are <u>relatively prime</u>.

We can generalize this argument and conclude that:

<u>Theorem</u>: If $0 < n < m$ and d = greatest common divisor of n and m, then the successive division process (<u>Euclidean Algorithm</u>)

$$m = rn + s \qquad 0 \leq s < n$$
$$n = r's + s'$$
$$s = r''s' + s''$$
$$\cdots$$
$$\cdots \quad \underbrace{d}_{\text{last} \neq 0 \text{ remainder.}}$$

has last $\neq 0$ remainder $= d$.

Example. Find the gcd (greatest common divisor) of 33 and 177.

Solution: $177 = 5 \times 33 + 12$

$33 = 2 \times 12 + 9$

$12 = 1 \times 9 + (3)$

$\therefore 3 = \gcd(33, 177)$.

Now note that once we have the list of successive division equations, we can use them to write d as a combination of the original two numbers.

$3 = 12 - 1 \times (9)$

$= 12 - 1 \times (33 - 2 \times 12)$

$= 3 \times (12) - 1 \times 33$

$= 3 \times (177 - 5 \times 33) - 1 \times 33$

$\boxed{3 = 3 \times \underline{\underline{177}} - 16 \times \underline{\underline{33}}}$

Euclid's Theorem. If $n, m \in \mathbb{N}$ and $d = \gcd(n, m)$, then $\exists\, r, s \in \mathbb{Z}$ such that $d = rn + sm$.

We started with continued fractions, and in fact Euclid's Theorem is closely related to continued fractions. In order to see this, we will use some matrices.

Let $M(a) = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$.

<u>Theorem</u>. $M(a_1)M(a_2)\cdots M(a_n) = \begin{pmatrix} P & R \\ Q & S \end{pmatrix}$

where $P/Q = [a_1, a_2, \ldots, a_n]$

$R/S = [a_1, a_2, \ldots, a_{n-1}]$ $(n>1)$

and $PS - QR = (-1)^n$.

<u>Proof</u>. Note that $\mathrm{Det}(M(a)) = -1$.
Thus $\mathrm{Det}(M(a_1)\cdots M(a_n)) = (-1)^n$ since the det of a product is the product of the determinants. Thus $PS-QR=(-1)^n$ follows from this. We prove the other assertions by induction.
Note $M(a) = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$ & $\frac{a}{1} = [a]$.

$M(a)M(b) = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} b & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} ab+1 & a \\ b & 1 \end{pmatrix}$

& $a + \frac{1}{b} = \frac{ab+1}{b}$, proving the Theorem for $n=2$.

So suppose we know the Theorem for n & examine the case $(n+1)$.

$$M(a_1)\underbrace{M(a_2)M(a_3)\cdots M(a_{n+1})}$$

$$\| \quad \text{by inductive assumption}$$

$$M(a_1)\begin{pmatrix} P & R \\ Q & S \end{pmatrix}, \quad \frac{P}{Q} = [a_2, \ldots, a_{n+1}], \quad \frac{R}{S} = [a_2, \ldots, a_n]$$

$$\|$$

$$\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} P & R \\ Q & S \end{pmatrix} = \begin{pmatrix} a_1P+Q & a_1R+S \\ P & R \end{pmatrix}$$

So $\dfrac{a_1P+Q}{P} = a_1 + Q/P = a_1 + \dfrac{1}{P/Q}$

$$\Rightarrow \frac{a_1P+Q}{P} = [a_1, a_2, \ldots, a_{n+1}]$$

& $\dfrac{a_1R+S}{R} = a_1 + \dfrac{S}{R} = a_1 + \dfrac{1}{R/S}$

$$\Rightarrow \frac{a_1R+S}{R} = [a_1, a_2, \ldots, a_n].$$

This completes the proof. //

---

ex: $M(1)M(2)M(3) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 10 & 3 \\ 7 & 2 \end{pmatrix}$

$1 + \dfrac{1}{2+\frac{1}{3}} = 1 + \dfrac{3}{7} = \dfrac{10}{7}$ ←

$1 + \dfrac{1}{2} = \dfrac{3}{2}$ ←

& $10 \cdot 2 - 3 \cdot 7 = -1 = (-1)^3$ ←

Recall $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ & $(XY)^T = Y^T X^T$ for any matrices X & Y that can be composed.

So if $\begin{pmatrix} P & R \\ Q & S \end{pmatrix} = M(a_1) \cdots M(a_n)$, then

$$\begin{pmatrix} P & Q \\ R & S \end{pmatrix} = \begin{pmatrix} P & R \\ Q & S \end{pmatrix}^T = M(a_n)^T M(a_{n-1})^T \cdots M(a_1)^T$$

$$\begin{pmatrix} P & Q \\ R & S \end{pmatrix} = M(a_n) M(a_{n-1}) \cdots M(a_1)$$

Thus the Theorem tells us that

$$\frac{P}{R} = [a_n, a_{n-1}, \ldots, a_1].$$

We have

(i) $\frac{P}{Q} = [a_1, \ldots, a_n]$

(ii) $\frac{P}{R} = [a_n, a_{n-1}, \ldots, a_1]$

(iii) $PS - QR = (-1)^n$

$\Rightarrow QR = (-1)^{n+1} + PS$

$\Rightarrow \boxed{QR \equiv (-1)^{n+1} \pmod{P}}$

This tells us how, using continued fractions, to find the inverse of $Q \bmod P$ when P and Q are relatively prime.

[Recall $\mathbb{Z}_p = \{[0],[1],\dots,[p-1]\}$ residue classes mod P and
$\mathcal{U}_p = \{[x] \mid [x] \text{ is not a zero divisor mod } P\}$
$\mathcal{U}_p = \{[x] \mid x \text{ is relatively prime to } P\}$]

We take $x = Q$, $0 < Q < P$, $P+Q$ rel prime. Then the continued fraction method finds R s.t. $0 < R < P$ & $QR \equiv (-1)^{(n+1)} \pmod P$).
If $n+1$ even then $[R] = [Q]^{-1}$.
If $n+1$ odd then $[P-R] = [-R] = [Q]^{-1}$.

---

example: Find $[11]^{-1} \in \mathbb{Z}_{59}$.

Solution. $\frac{59}{11} = 5 + \frac{4}{11} = 5 + \frac{1}{2+3/4}$

$$= (5) + \frac{1}{(2)+\frac{1}{(1)+1/(3)}} = [5,2,1,3]$$

$$[3,1,2,5] = 3 + \frac{1}{1+\frac{1}{2+\frac{1}{5}}} = 3 + \frac{1}{1+\frac{5}{11}} = 3 + \frac{11}{16}$$

$$= \frac{59}{16}$$

$11 \times 16 = 176 = (177-1) \overline{\overline{\quad}} (3 \times 59) - 1$

$11 \times 16 \equiv -1 \pmod{59}$

$11 \times (-16) \equiv 1 \pmod{59}$

$11 \times 43 \equiv 1 \pmod{59} \Longrightarrow [43] = [11]^{-1}$ in $\mathbb{Z}_{59}$.

Knowing that every $\neq 0$ elt of $\mathcal{U}_n$ has an inverse is sufficient to prove that $\mathcal{U}_n$ is a group under multiplication.

Note that if p is prime then $\mathcal{U}_p = \mathbb{Z}_p - \{0\}$. The $\neq 0$ elts of $\mathbb{Z}_p$ form a group.

Exercise 2. See Goodman for a proof of:
If p is a prime number, then $\mathcal{U}_p$ is $\cong C_{(p-1)}$ the cyclic group of order $(p-1)$. (Goodman uses $\Phi(p)$ for $\mathcal{U}_p$).
Verify this result directly for $p = 2, 3, 5, 7, 11$.

Exercise 3. Find $\mathcal{U}_8$, $\mathcal{U}_{10}$ (we did them in class) and $\mathcal{U}_{30}$. By "find" I mean, determine the multiplication table and figure out the isomorphic group that you already know that fits $\mathcal{U}_n$.

Exercise 4. For $n \in \mathbb{N}$, the number of $k \in \mathbb{N}$ s.t. $k \leq n$ and k is relatively prime to n is called $\phi(n)$, the Euler ϕ-function.
Thus $\phi(n)$ = the number of elements in the group $\mathcal{U}_n$. Show that p prime $\Rightarrow \phi(p) = p^n - p^{n-1}$.

Exercise 5. Use our continued fraction method to find $[7]^{-1}$ in $\mathbb{Z}_{52}$.

Exercise 6. Make a multiplication table for $\mathcal{U}_{16}$ and find out as much as you can about this group.

Exercise 7. Let $\mathbb{H}$ denote the 8-element quaternion group. $\mathbb{H} = \{1, -1, i, -i, j, -j, k, -k\}$
$k^2 = i^2 = j^2 = ijk = -1$ $(-x = (-1)x = x(-1))$.

Let $Kl_4 = \{1, A, B, AB\}$ be the Klein 4-group with $A^2 = 1$, $B^2 = 1$, $AB = BA$. Define $f : \mathbb{H} \longrightarrow Kl_4$ by
$f(1) = 1$, $f(-x) = f(x)$ all x, $f(i) = A$
$f(-1) = 1$ $f(j) = B$
$f(k) = C$.

Show: (i) f is a well-defined homomorphism of groups.

(ii) $\mathrm{Ker}(f) = \{x \in \mathbb{H} \mid f(x) = 1\}$ is isomorphic to the cyclic group of order 2.

(iii) Suppose $g : \mathbb{G} \longrightarrow H$ is any homomorphism of groups. Let $K = \mathrm{Ker}(g) = \{x \in \mathbb{G} \mid g(x) = 1\}$. Show that if $x \in K = \mathrm{Ker}(g)$ and $a \in \mathbb{G}$, then $axa^{-1} \in K$.

[Recall that g homomorphism means $g(1) = 1$ and $g(xy) = g(x)g(y)$ $\forall x, y \in \mathbb{G}$.]

2° A little more Number Theory

Theorem. p a prime, and $a, b \in \mathbb{N}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. By Euclid, if $p \nmid a$ then
$\exists\, r, s \in \mathbb{Z}$ s.t. $rp + sa = 1$.
$\Rightarrow rpb + sab = b$.
But $p \mid (rpb + sab)$ $\therefore p \mid b$.
Thus $p \nmid a \Rightarrow p \mid b$. This is sufficient to prove the Theorem. //

This result actually tells us that prime factorization is unique. For example suppose $2 \cdot 3 = p \cdot q \cdot r$ where p, q and r are primes. Then $2 \mid p(qr)$
$\Rightarrow 2 \mid p$ (making $2 = p$) or $2 \mid qr$.
But $2 \mid qr \Rightarrow 2 \mid q$ or $2 \mid r$.
Thus $2 = p$ or $2 = q$ or $2 = r$.
We leave it to you to elaborate this argument and get uniqueness.

This last theorem and the uniqueness of prime decomposition depends on our Euclid result. Without it the uniqueness result can fail. For example, consider

$$\mathcal{R} = \mathbb{Z}[\sqrt{-5}] = \{n + m\sqrt{-5} \mid n, m \in \mathbb{Z}\}$$

This is called a "ring of Gaussian integers." In $\mathcal{R}$ we have

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3.$$

One can prove that $2, 3, (1+\sqrt{-5})$ and $(1-\sqrt{-5})$ are all "prime" in $\mathcal{R}$ in the sense that none of them can be reduced to simpler products of non-invertible elements. ($+1$ and -1 are the only invertible elements). Thus $\mathcal{R}$ does not have unique factorization.

To prove things about $\mathcal{R}$ it is useful to define $\mathcal{N}: \mathcal{R} \longrightarrow \mathbb{Z}$

$\mathcal{N}(z) = z\bar{z}$. i.e.

$\mathcal{N}(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2 + 5b^2$.

Show that $\mathcal{N}(zw) = \mathcal{N}(z)\mathcal{N}(w)$ for any $z, w \in \mathcal{R}$ and use that to prove our irreducibility assertions!