## Solutions $\mathfrak{G}$

## Problems 1-27

## Problem\#1:

What is depicted in the diagram is an exaggeration. In fact there is no such point $p$ unless arcs $C_{1}$ and $C_{2}$ coincide. The arc $u$ on the left must be longer than the arc $v$ below it, because if one convex curve between 2 points lies entirely above another relative to their mutual base it must be larger. Therefore the arc of $\mathrm{C}_{1}$ from A to p must be larger than the arc of $\mathrm{C}_{2}$ from A to p .

Think of a belt maintained tightly about one's waist. The only way to lift the belt away from the waist, ( without breaking or self-intersection), is by increasing its length.

However, for the same reason, the arc of $C_{1}$ from $p$ to $B$ must be smaller than the arc of $C_{2}$ from $p$ to $B$. Yet one can't have both $u>v$, and $u<v$. Therefore $u=v$ and arc $C_{1}$ coincides with $\operatorname{arc} C_{2}$.

It follows that Area $\Delta_{1}=$ Area $\Delta_{2}=0$ !


## Prablem \#Q:

(i) Obviously, at the intersection of two curves of $\mathrm{C}, \rho$ and $\theta$ must coincide. If $\alpha_{1}=\alpha_{2}$, then one must have $D_{1}=D_{2}$.

Before carrying through the complete demonstration of (ii) let us show how the dual character of the defining equation of $C$ automatically results in the equivalent proof of (iii).

If, in equation $C$ one replaces $D$ by $1 / D^{2}$, and $\alpha$ by $-\alpha$, it becomes:

$$
D^{2} \rho^{2}(\theta)=\frac{D}{1+\sin (\theta+\alpha)} D>0,2 \pi>\alpha \geq 0
$$

The equation is completely symmetrical in $D$ and $\rho$, and in $\theta$ and $\alpha$.
This means that any theorem involving constant $\theta$ and $\rho$, (intersections), becomes a dual theorem involving constant D and $\alpha$ (lines). The geometry induced by C is therefore a projective geometry, in which two lines determine two points and two points determine two lines.

Without loss of generality one may consider the intersections of curves in C :

$$
\begin{aligned}
& L_{1}: \rho^{2}(\theta)=\frac{1}{1+\sin (\theta)} \\
& L_{2}: \rho^{2}(\theta)=\frac{D}{1+\sin (\theta-\alpha)}
\end{aligned}
$$

At their intersections these expressions are equal:

$$
\begin{aligned}
& D(1+\sin \theta)=1+\sin (\theta-\alpha) \\
& =1+\sin \theta \cos \alpha-\sin \alpha \cos \theta \\
& =1+a \sin \theta+b \cos \theta \\
& a=\cos \alpha, b=-\sin \alpha
\end{aligned}
$$

Re-arranging:

$$
D-1=(a-D) \sin \theta+b \cos \theta
$$

Let

$$
c=\sqrt{b^{2}+(D-a)^{2}}
$$

D is assumed to be positive. Therefore:

$$
\begin{aligned}
& \frac{1}{c}(D-1)=\frac{(a-D)}{c} \sin \theta+\frac{b}{c} \cos \theta \\
& =\cos \beta \sin \theta+\sin \beta \cos \theta \\
& =\sin (\theta+\beta) ; \beta=\sin ^{-1}(b / c)
\end{aligned}
$$

Note that every value of the function $\sin (\theta),($ or $\sin (\beta+\theta))$ occurs twice in the interval 0 to $2 \pi$, for all values of the argument except $\theta= \pm$ $\pi / 2$, where the $\sin$ is $\mathbf{1}$ or -1 . It is clear that $\mathrm{c}>\mathrm{D}$; thus one cannot have D-1 = c; also D cannot be 0 , or negative. Thus there are exactly two
solutions for all permissible values of $D$ and $\alpha . \mu=\theta+\beta$ is one of these solutions, then $\pi-\mu$ is the other one. Thus:

$$
\begin{aligned}
& \theta_{1}=\mu-\beta \\
& \theta_{2}=\pi-\mu+\beta
\end{aligned}
$$

(iv) One can first let $\mathrm{D}=1, \alpha=0$, then by rotation and similarity obtain all the other curves of $\mathrm{C}^{*}$. We compute:

$$
\begin{aligned}
& \rho^{2}(\theta)=\frac{1}{1+\cos (2 \theta)}=\frac{1}{1+\left(2 \cos ^{2} \theta-1\right)}=\frac{1}{2 \cos ^{2} \theta} \\
& 2 \cos ^{2} \theta \rho^{2}(\theta)=2 x^{2}=1 \\
& \therefore x=\sqrt{1 / 2}
\end{aligned}
$$

Otherwise stated, the basic curve of $C^{*}$ is simply a vertical line through the value $x=2^{-1 / 2}$. $C^{*}$ coincides with the collection of all lines in the plane that don't pass through the origin.

As a final observation, the equation for the straight line can also be put into the form:

$$
A \rho(\theta) \cos \theta+B \rho(\theta) \sin \theta=1
$$

Can something similar be done for the equation of the family $C$ ?

## $\mathscr{O P}_{\text {poblem }}$ 3:

Let $\Phi: L-->L$ be a continuous 1-1 function from $L$ onto itself, such that $f(A)=B, f(B)=C, \ldots . . . ., f(E)=F, f(F)=A . \Phi$ in other words, maps each segment clockwise onto the adjacent segment. Pick any point in A. Call it a Let $b=\Phi(a), c=\Phi(b)=\Phi^{2}(a), d=\Phi(c)=\Phi^{3}(a), e=\Phi(d)=\Phi^{4}(a)$, $f=\Phi(\mathrm{e})=\Phi^{5}(\mathrm{a}), \mathrm{a}=\Phi^{6}(\mathrm{a})$.

Draw tangents at all points a ... $f$, and identify the intersections $X$ of tangents at $a$ and $d, Y$ of tangents at $b$ and $e, Z$ of tangents at $c$ and $f$. Consider the triangle $T$ formed by the vertices $X Y Z$, with sides $S_{1}=X Y, S_{2}=X Z, S_{3}=Y Z$. If these points are already collinear, we are finished. Otherwise ( see diagram), we define a new function on $L$ $G(a, \Phi, L)=G(a)$ at the six points defined by a ..... f, as:

$$
\begin{aligned}
& G(a)=\gamma=\text { interior angle formed by } S_{1} \text { and } S_{2} \\
& G(b)=\alpha=\text { interior angle formed by } S_{1} \text { and } S_{3} \\
& G(c)=\beta=\text { interior angle formed by } S_{2} \text { and } S_{3} \\
& G(d)=2 \pi-\gamma=\text { exterior angle formed by } S_{1} \text { and } S_{2} \\
& G(e)=2 \pi-\alpha=\text { exterior angle formed by } S_{1} \text { and } S_{3} \\
& G(f)=2 \pi-\beta=\text { exterior angle formed by } S_{2} \text { and } S_{3}
\end{aligned}
$$

Now move the point a along $L$ in a clockwise direction. As a moves into each segment, the points $b, c, d$, etc. will move into distinct segments of their own. At no point $x$ will $\Phi(x)$ be in the same segment as itself.

Ultimately as moves to d , the angle $\gamma$ must turn into $2 \pi-\gamma$. Since G is continuous, a must reach a point $\mathrm{a}^{*}$ at which $\gamma$ is equal to $\pi$. At this point the intersections of the tangents will be collinear. This proves the theorem.

## 

## Or roblem\#4:

The two solutions for $\mathbf{n}=1$ are obviously $\mathbf{1}$ and -1 . It is easily seen that the solutions for $\mathrm{n}=2$ are all cyclotomic. If $\alpha$ is a root, then $\alpha *$, the complex conjugate is also a root, with $\alpha \alpha^{*}=1$. Let $\mathbf{u}=\alpha+\alpha^{*}$. The irreducible equation for a is $P(x)=x^{2}-u x+1$. u must therefore be an integer. As it is equal to twice the real part of $\alpha$, this must be an integer or a half integer. Since the absolute value of $\alpha$ is 1 , the only possibilities are $0,1 / 2$ and $-1 / 2$, which correspond to $i,-i$, and the cube roots of 1 and $\mathbf{- 1}$.

The cases $n=4$ is more interesting. The result follows immediately from Galois Theory, but we will not assume that the problem-solver knows this. Write the equation as

$$
P(x)=x^{4}-u x^{3}+w x^{2}-p x+q
$$

Let the roots be designated $\alpha, \alpha^{*}, \beta, \gamma$. Let $\mathrm{s}=\alpha+\alpha^{*}$, $t=\beta+\gamma$ Then (the calculations are simple)
(i) $s+t=u$,
(ii) $1+q+s t=w$, or $s t=w-q-1$, an integer. $=k$

It is now clear that $s$ and $t$ are the two roots of a quadratic equation with integer coefficients. Its solution is

$$
s, t=\frac{u \pm \sqrt{u^{2}-4 k}}{2}
$$

Once again, $s / 2$ isthe real part of $\alpha$. The imaginary part is therefore given by $r_{1,2}= \pm \sqrt{1-s^{2}}$ The symmetrical form of equations (i) and (ii) implies that one could have taken $t / 2$ as the real part of $\alpha$. One therefore concludes that, if $P$ is to be irreducible, all 4 roots are generated from the solutions to (i) and (ii). By assumption they are all complex, and the symmetries of the form of the solution guarantee that they all have absolute value of $1: \gamma=\beta *=1 / \beta$.

This immediately implies that $\mathbf{u}=\mathrm{p}$, and $\mathrm{q}=1$.

Note that by a simple change of variable from $x$ to $-x$ one can arrange that $u$ is positive. Since $\alpha$ is on the unit circle, the real part of $\alpha$ is less than one, and $u$ is therefore less than 4 . One therefore looks at the 4 cases $u=0,1,2,3$ . Let be the root given by:

$$
\begin{aligned}
& \alpha=\frac{s+i \sqrt{4-s^{2}}}{2} \\
& s=\frac{u+\sqrt{u^{2}-4 k}}{2} \\
& \operatorname{Re} \alpha=\frac{s}{2} \\
& k=w-2
\end{aligned}
$$

From these equations one sees that $|\mathrm{s}|<2$ and $4 \mathrm{k}<\mathrm{u}^{2}$. However, k may also assume negative values
(i) u $=0$. Then $s=\sqrt{-k}$. The possibilities are $\mathbf{k}=0,-1,-2,-3$.

Plugging these into the coefficients of $\mathrm{P}(\mathrm{x})$ produces the list:

$$
\begin{aligned}
& P(x)= \\
& x^{4}+2 x^{2}+1 \\
& x^{4}+x^{2}+1 \\
& x^{4}+1 \\
& x^{4}-x^{2}+1 \\
& x^{4}-2 x^{2}+1
\end{aligned}
$$

All of these are cyclotomic.
(ii) $u=1$. Then $k=0$ and $k=-1$ are the only possibilities. $k=0$
gives the equation for the cube root of -1. If $k=-1$, then $w=1$, and $P(x)=x^{4}-x^{3}+x^{2}-x+1$, which is the equation for the $5^{\text {th }}$ root of $\mathbf{- 1}$.
(iii) $u=2$. If $k=0$, $a=1$; if $k=1$, $a$ is the cube root of -1 ; if $k=-1$, then the real part of a will be larger than 1 :

$$
\operatorname{Re} \alpha=\frac{1}{4}(2+\sqrt{4+4})=\frac{1}{2}(1+\sqrt{2})>1
$$

This possibility is therefore excluded. This completes the proof for $\mathbf{n}=4$.
The theorem is no longer true if one allows real values for the other roots $\beta$ and $\gamma$ of the 4 h degree equation. A counter-example is worth a thousand words: $P(x)=x^{4}-5 x^{3}+2 x^{2}-5 x+1$, which has roots:

$$
\begin{aligned}
& \alpha=\frac{1}{2}(5-\sqrt{21})+\frac{i}{2} \sqrt{10 \sqrt{21}-42} \\
& \alpha^{*}=\frac{1}{2}(5-\sqrt{21})-\frac{i}{2} \sqrt{10 \sqrt{21}-42} \\
& \beta=\frac{(5+\sqrt{21})+\sqrt{42+10 \sqrt{21}}}{2} \\
& \gamma=\frac{(5+\sqrt{21})-\sqrt{42+10 \sqrt{21}}}{2}
\end{aligned}
$$

## Oprablem 5:

When $\mathrm{n}=6$, one has the following result:

Theorem: Let $P(x)=x^{6}-u x^{5}+v x^{4}-w x^{3}+v x^{2}-u x+1$ be a symmetric equation, all of whose roots are complex. Then there is at least one pair of conjugate roots $\alpha, \alpha *$ on the unit circle.

The symmetry of the above form implies that when $r$ is a root, $1 / r$ will also be a root. If $\beta$ is a complex root, then $\beta *, 1 / \beta$ and $1 / \beta *$ are also roots. If $b$ is not on the unit circle, then the remaining pair of conjugate roots, $\alpha$ and $\alpha *$ must have the property that $\alpha *=1 / \alpha$. Q.E.D.

Informally, one sees that among all the symmetric integral equations of the $6^{\text {th }}$ degree, there must be many which are both irreducible, have only complex roots, and have one root, (and the other 3 which it generates) which are not on the unit circle.

For example, one can start with the polynomial $R(x)=(x+1)^{6}$. Let $k$ be any positive integer, and add to $R$ the polynomial $A(x)=k x^{4}+k x^{2}$. The polynomial $R(x)+A(x)$ is always positive, hence has no real roots. As it is symmetric, it must have one conjugate pair on the unit circle. If it is not irreducible, it must be factorable by a cyclotomic quadratic, and one can safely assume that this will not be true for most $k$.

## $\mathscr{P}_{\text {Poblem }} 6$ :

Assume that the entries in the table occur in the distribution $2,3,4$, and that $\phi$ generates a semigroup. Then $e_{1}, e_{2}, e_{3}$, can be represented by matrices, $\mathrm{M}_{1}, \mathrm{M}_{2}, \mathrm{M}_{3}$.

If any one of these matrices is non-singular, then ( $\mathrm{E}, \phi$ ) must have an identity, say $M_{1}$. Then $M_{2}$ and $M_{3}$ cannot both be nonsingular, which implies a group. Clearly the table of a 3-element group partitions as $3+3+3$.

If $\mathrm{M}_{2}$ is also non-singular, it must be the case that $\left(\mathrm{M}_{2}\right)^{\mathbf{2}}=$ $M_{1}$. One sees that in fact $M_{2}$ cannot be non- singular. If:
$\mathbf{M}_{2} \mathbf{M}_{3}=\mathbf{M}_{2}$.
This implies that $\mathrm{M}_{3}=$ Identity $=\mathrm{M}_{1}$.

$$
\mathbf{M}_{\mathbf{2}} \mathbf{M}_{3}=\mathbf{M}_{1} .
$$

This implies that $M_{3}=M_{2}^{-1}=M_{2}$
$\mathrm{M}_{2} \mathrm{M}_{3}=\mathrm{M}_{3}$. This partitions T as $\mathbf{2 + 2 + 5}$, since $\mathrm{M}_{3}$, being the only singular element, must be an annihilator.

Therefore, there can be at most one non-singular element, which is the Identity. In that case $\mathbf{e}_{11}=e_{1}$ is the only entry of $e_{1}$ in the table, contrary to the requirement that there be at least 2 entries for each element. Therefore $\mathbf{M}_{1}, \mathbf{M}_{2}, \mathrm{M}_{3}$ are all singular .

None of these can be an annihilator, which would generate 5 entries in the table. If there is no annihilator, then neither a row, nor a column, can be entirely filled with a single element. And if there is no non-singular element, one cannot have all elements $\mathrm{e}_{1}$, $e_{2}$, and $e_{3}$, in any row or column.

Only 4 possibilities remain consistent with the hypothesis:

| $\phi$ | $e_{1}$ | $e_{2}$ | $e_{3}$ |
| :---: | :--- | :--- | :--- |
| $e_{1}$ | $e_{1}$ | $e_{2}$ | $e_{2}$ |
| $e_{2}$ | $e_{3}$ | $e_{1}$ | $e_{3}$ |
| $e_{3}$ | $e_{3}$ | $e_{2}$ | $e_{3}$ |


| $\phi$ | $e_{1}$ | $e_{2}$ | $e_{3}$ |
| :---: | :--- | :--- | :--- |
| $e_{1}$ | $e_{3}$ | $e_{2}$ | $e_{3}$ |
| $e_{2}$ | $e_{3}$ | $e_{1}$ | $e_{3}$ |
| $e_{3}$ | $e_{2}$ | $e_{2}$ | $e_{1}$ |


| $\phi$ | $e_{1}$ | $e_{2}$ | $e_{3}$ |
| :---: | :--- | :--- | :--- |
| $e_{1}$ | $e_{1}$ | $e_{3}$ | $e_{3}$ |
| $e_{2}$ | $e_{2}$ | $e_{1}$ | $e_{2}$ |
| $e_{3}$ | $e_{2}$ | $e_{3}$ | $e_{2}$ |


| $\phi$ | $e_{1}$ | $e_{2}$ | $e_{3}$ |
| :---: | :---: | :---: | :---: |
| $e_{1}$ | $e_{2}$ | $e_{3}$ | $e_{2}$ |
| $e_{2}$ | $e_{2}$ | $e_{1}$ | $e_{2}$ |
| $e_{3}$ | $e_{3}$ | $e_{3}$ | $e_{1}$ |

None of these are semi-groups.

## Orablem 7:

In fact, $2+3+4$ is the only partition of 9 that is incompatible with a semigroup. One may find it enjoyable to construct semigroup tables for each of the possible partitions of 9 .
$O_{\text {Prablem }} 8$ :
Suppose $S$ is maximal and contains an element $x, x \in S \wedge x^{-1} \notin S$. Then $S=S \cup\left\{x^{-1}\right\}$ is not an antigroup. Let $\mathbf{u}, \mathbf{v}$ be elements of $S$. There are 5 possibilities:

$$
\begin{aligned}
& \text { (i) } u v=x^{-1} \\
& \text { (ii) } u x^{-1}=v \rightarrow u=v x \\
& \text { (iii) } u^{-1} x=v \rightarrow x=u v \\
& \text { (iv) }\left(x^{-1}\right)^{2}=x^{-1} \\
& \text { (v) }\left(x^{-1}\right)^{2}=u
\end{aligned}
$$

(ii) and (iii) are ruled out since $S$ is an antigroup and $u, v, x$ are all in $S$, (v) is a variant of (i) as it implies (iv) $x^{-1}=x u, x, u \in S$
(iv) implies that $x$ is the identity which cannot be a member of an antigroup. This leaves only (i), so $\boldsymbol{x}^{\mathbf{- 1}}$ is a member of $\mathbf{S}^{\mathbf{2}}$.

## $\mathscr{P}_{\text {roblem }} 9:$

From the above we know that $u, v \in S \rightarrow u^{-1} v, u v^{-1} \in S^{3}$
Let $g$ be any element of $G$ which is not in $S$. Since $S$ is maximal, there are these alternatives:

$$
\begin{aligned}
& \text { (i) } u v=g \rightarrow g \in S^{2} \\
& \text { (ii) } u g=v \rightarrow g=u^{-1} v \in S^{3} \\
& \text { (iii) } g u=v \rightarrow g=v u^{-1} \in S^{3} \\
& \text { (iv) } g^{2} \in S \rightarrow g \in V
\end{aligned}
$$

These match all the sets in the proposed decomposition.

## Orablem 10:

(a) Let $u, v, x \in A ; \Phi(x)=x u v$. As $\mathbf{x}$ moves through all elements of $\mathbf{A}$, so does $F(x)$. There must therefore be an element $y$, such that $y u v=v$. Therefore $y=u^{-1}$.
(b) Choose $a, b, a=u v, b=w z$, with $u, v, w, z \in A$.

Then $a b=u v w z=(u v w) z=t z$, where $t$ is also an element of $A$. Therefore $\mathrm{ab} \varepsilon \mathrm{A}^{2}$.

Since, by (a), A contains all of its inverses, so does $\mathrm{A}^{\mathbf{2}}$, which also contains the identity, and is therefore a group.
(c) It is clear that any product of elements of $B=A \cup A^{2}$ must remain in $B$, which also contains all its inverses and the identity
(d) It is obvious that $A^{2}$ is normal in $B$. Let $\sigma$ be any element of $A$. Then $\sigma A=A^{2}$. By a classic theorem of group theory, one can find an element $k$ in A such that $\mathrm{a}^{\mathbf{2}}=\mathrm{e}$.

OProblem 11:
(1) $Z_{2}, Z_{3}, Z_{4}$.
(2) $\mathrm{Z}_{5}$ to $\mathrm{Z}_{9}$.
(3) $\mathrm{k}=9 ; \mathrm{S}=\{2,3\} ; \mathrm{S}^{2}=\{4,5,6\} ; \mathrm{S}^{3}=\{7,8,6,0) ; \mathrm{V}=\{1\}$

## $\mathscr{P}_{\text {roblem }}$ 12:

The Norm is computed by squaring each of the entries in $\psi(\sigma)$, adding them together and taking the positive square root. Since each positive integer , (multiplied by $-1 / 2$ ) occurs in the exponent of 2 , once and only once in any arrangement of $\sigma$, the sum of the squares will always add up to 1.

## $\mathscr{P}_{\text {roblem } 18:}$

Observe that the inner product $\mu\left(\sigma \rho^{-1}\right)$ is symmetric in the entries. In fact:

$$
\mu\left(\sigma \rho^{-1}\right)=\sum_{i=1}^{\infty} 2^{-\left(s_{i}+r_{i} / 2\right)}=\mu\left(\rho \sigma^{-1}\right)
$$

Note: this is not the same as $\mu\left(\sigma^{-1} \rho\right)\left(=\mu\left(\rho^{-1} \sigma\right)\right)$ !

## OPrablem 14:

(i) $\mu(\mathrm{e}, \rho)$ is never equal to 0 for any permutation $\rho$. However it can be made as small as one likes by pushing a long sequence of integers $1,2, \ldots \mathrm{~N}$ at the beginning of the identity, $e$, very far out on the sequence, then bringing down to the beginning a collection of integers on $e$ which are even further away. In this
way the sum $\mathrm{s}_{\mathrm{i}}+\mathrm{r}_{\mathrm{i}}$ may be kept above any pre-assigned number $\mathbf{N}$, and $\mu$ will be reduced accordingly.
(ii) Using the bilinearity of the inner product, one can multiply out the expression for $D$ under the square root and confirm the expression presented in the problem.
(iii) The method for doing this is in the solution to (i)

## OPrablem 15:

First Solution: Begin with the identity,

$$
1+x^{\frac{1}{2}}=\frac{1-x}{1-x^{\frac{1}{2}}}
$$

Replacing the first term of the infinite product gives :

$$
\begin{aligned}
& \frac{1-x}{1-x^{\frac{1}{2}}} \bullet \frac{1+x^{\frac{1}{4}}}{2} \ldots=(1-x)^{1 / 22} \frac{\left(1+x^{\frac{1}{4}}\right)}{\left(1+x^{\frac{1}{4}}\right)\left(1-x^{\frac{1}{4}}\right)} \Pi^{\prime} \ldots \\
& =(1-x) 1 / 2^{3} \frac{\left(1+x^{\frac{1}{8}}\right)}{\left(1+x^{\frac{1}{8}}\right)\left(1-x^{\frac{1}{8}}\right)} \prod^{\prime \prime} \ldots=\ldots \text { etc. }
\end{aligned}
$$

After $k$ steps, what remains of the infinite product will converge to 1 . The expression to its left has the form:

$$
E_{k}=(1-x) 1 / 2 k \frac{1}{\left(1-x^{\frac{1}{2 k}}\right)}
$$

Now, $\lim _{k \rightarrow \infty} \frac{1 / 2 k}{1-x^{\frac{1}{2^{k}}}}=\lim _{z \rightarrow 0} \frac{z}{1-x^{z}}=-\ln x$, by L'Hôpital's Rule.
Finally, $\frac{1-x}{-\ln x}=\frac{x-1}{\ln x}$
Q.E.D.

Second Solution :

$$
\text { Let } J_{k}(x)=\prod_{n=1}^{k}\left(\frac{1+x^{2-n}}{2}\right)
$$

One can multiply through all the factors of this product and express the result as a sum of the form:

$$
J_{k}(x)=\frac{1}{2 k} \sum_{\alpha} x^{\alpha}
$$

where $\alpha$ is a real number ranging over all finite binary decimals of the form $\quad \alpha=\frac{1}{2 r_{1}}+\frac{1}{2 r_{2}}+\ldots \frac{1}{2 r_{k}}, 0 \leq r_{i} \leq k$.

As there are 2 k such combinations, as $\mathrm{k} \rightarrow \infty$ this assumes the form of a Riemann sum , with differential increment $\Delta \mathrm{y}=1 / 2^{k}$ , and the function $f(y)=x y$ under the integral sign. The infinite product can therefore be replaced by an integral

$$
\begin{equation*}
\prod_{1}^{\infty}(. .)=\int_{0}^{1} x y d y=\int_{0}^{1} e^{y \ln x} d y=\frac{x-1}{\ln x} \tag{!}
\end{equation*}
$$

(ii) One uses the familiar identity:

$$
1+x^{k^{-n}}+x^{2 \bullet k^{-n}}+\ldots+x(k-1) \bullet k^{-n}=\frac{x^{k^{-n+1}-1}}{x^{k^{-n}-1}}
$$

(iii) The same trick used in Solution I can therefore be applied to all exponents $k$.

By recognizing that the exponents of the corresponding sum eventually yield, or lead in the limit, to the base $n$ decimal representations of all the real numbers in the interval $(0,1)$, one can also employ the methods of the 2 nd Solution

## OProblem 16:

Look at the properties of a self-inverting analytic function

$$
\phi(z)=\sum_{n=1}^{\infty} \frac{a_{n}}{n!} z^{n}
$$

The even coefficients of $\phi$ will appear in $z^{2} \alpha\left(z^{2}\right)$, the odd coefficients in $\mathrm{z} \boldsymbol{\beta}\left(\mathrm{z}^{2}\right)$ Since $\boldsymbol{\beta ( 0 )}=\mathbf{- 1}, \mathrm{a}_{1}=\mathbf{- 1}$.

Let $g(z)=\phi(\phi(z))=z$. Then $g^{\prime}(0)=y^{\prime} \phi^{\prime}$ where

$$
y^{\prime}=d \phi / d z ; \phi^{\prime}=d g / d \phi=d \phi(\phi(z)) / d \phi
$$

Since $\phi(0)=0$, these two derivatives coincide at 0 , or

$$
d \phi /_{d z \mid z=0}=d g /_{d \phi_{\mid z=0}}=a_{1}=-1
$$

Therefore $g^{\prime}(0)==\left(a_{1}\right)^{\mathbf{2}}=+1$. Calculating the first few derivatives of $g$, recalling that, at 0 , the value of $\phi^{(i)}$ coincides with that of $\mathbf{y}(\mathbf{i})$ :

$$
g^{\prime \prime}(0)=y^{\prime \prime} \phi^{\prime}+\left(y^{\prime}\right)^{2} \phi^{\prime}=a_{1} a_{2}+a_{1}^{2} a_{2}=a_{1} a_{2}\left(1+a_{1}\right)=0
$$

Since $\mathbf{a}_{\mathbf{1}}=\mathbf{- 1}$ by hypothesis. $\mathbf{a}_{\mathbf{2}}$ may be freely chosen.

$$
\begin{aligned}
& g^{\prime \prime \prime}(0)=y^{\prime \prime \prime} \phi^{\prime}+y^{\prime \prime} y^{\prime} \phi^{\prime \prime}+2 y^{\prime} y^{\prime \prime} \phi^{\prime \prime}+\left(y^{\prime}\right)^{3} \phi^{\prime \prime \prime} \\
& =a_{3} a_{1}+3 a_{1} a_{2}^{2}+a_{1}^{3} a_{3}=a_{1}\left(a_{3}+3 a_{2}^{2}+a_{1}^{2} a_{3}\right)
\end{aligned}
$$

Since $\mathbf{a}_{1}=\mathbf{- 1}$, it follows that $a_{3}=-\frac{3}{2} a_{2}^{2}$. We will show, in general, that all of the even indexed coefficients may be chosen arbitrarily, while the odd indexed coefficients may be calculated as functions of those of lower index. ( The requirement that the derivatives of $\alpha$ be uniformly bounded has been posited only to assure convergence of $\boldsymbol{\beta}$.)

Write the general expression for the derivatives of $g$ as:

$$
g^{(n)}(z)=\sum_{i \leq n} P_{i}\left(y^{\prime}, y^{\prime \prime}, \ldots y^{(n)}\right) \phi^{(i)}(z)
$$

the $\mathrm{P}_{\mathrm{i}}$ being polynomials in the derivatives. An easy induction shows that this expression is of the form

$$
g^{(n)}(z)=y^{(n)} \phi^{\prime}(z)+[\ldots \ldots]+\left(y^{\prime}\right)^{n} \phi^{(n)}(z)
$$

At $\mathrm{z}=0$, this reduces to

$$
\begin{aligned}
& g(n)(z)=a_{n} a_{1}+[\ldots \ldots .]+\left(a_{1}\right)^{n} a_{n} \\
& =a_{1} a_{n}\left(1+a_{1}^{n-1}\right)+[\ldots \ldots .]
\end{aligned}
$$

The left-hand part of the right side of the equation is 0 when $n$ is even; hence $a_{n}, n=2 j$ may be freely chosen.

It is equal to $\mathbf{- 2 a n}$ when $\mathbf{n}=\mathbf{2 j + 1}$. Since $a_{n}$ does not occur in the bracketed expression, and since $g^{(n)}(z)=0$ for all $n$ except 1 ( because $\phi$ is self-inverting), one can use the above equation to compute the value of $\mathbf{a}_{2 j+1}$ in terms of the previous a's. This shows that the coefficients of $\boldsymbol{\beta}$ can be completely calculated from those of $\alpha$.Establishing convergence of $\beta$ :
(1) The number of terms in the expression for $g(n)(z)$ is easily seen to be less than or equal to $n!$.
(2) The total exponent of each monomial in $g(n)(z)$ is less than or equal to $A^{n+1}$, where $A$ is the uniform upper bound on the derivatives. Therefore

$$
\|\beta(z)\|<\sum_{j=2 k+1}^{8} \frac{j!A j+1_{z} j}{j!}=\frac{A}{1-A z}
$$

and $\beta$ converges for $|\mathrm{z}|<1 / \mathrm{A}$
Note : When the derivatives of $\alpha$ are not uniformly bounded, one can still construct $\beta$, but it must be checked for convergence.

For example, if $a_{n}=\mathbf{- 1}$, for all even $\mathbf{n}$, then $a_{\mathbf{n}}=\mathbf{- 1}$ for all $n$, and $\phi$ is the function:

$$
\phi(z)=-z-z^{2}-z^{3}-\ldots=\frac{z}{z-1}
$$

which is self-inverting.
However, if $a_{n}=+1$ for all even $n$, then $\beta(z)$ will diverge.

## OPrablem 17.

We are asked to describe all analytic solutions to the differential equation:

$$
E(z)=z^{2} f^{\prime}(z)+(z-1) f(z)+1=0
$$

(i) Deleting the constant term 1 yields the auxiliary equation

$$
\begin{aligned}
& A: \quad z^{2} f^{\prime}(z)+(z-1) f(z)=0 \\
& \frac{f^{\prime}}{f}=\frac{1-z}{z^{2}}=\frac{1}{z^{2}}-\frac{1}{z}
\end{aligned}
$$

This readily integrates into

$$
\begin{aligned}
& \ln f=-\frac{1}{z}+\ln z+k \\
& f=e^{k} z e^{-1 / z}=c z e^{-1 / z}
\end{aligned}
$$

The auxiliary solution may be adjoined to any solution convergent in a circle around a point away from the origin, to produce a 1-parameter family of solutions.
(ii) Successive differentiations of $\mathrm{E}(\mathrm{z})=0$ produces the recursions

$$
\begin{aligned}
& f^{\prime}=\frac{(1-z) f-1}{z^{2}} \\
& f^{\prime \prime}=\frac{-f+(3 z-1) f^{\prime}}{z^{2}}, \text { etc } \ldots
\end{aligned}
$$

This shows that if there is a solution $f$ at any point away from 0 , then derivatives exist of all degrees. This suggests expanding $f$ in a MacLaurin series at points $k$ other than 0 . Let $k$ be any number, real or complex, other than 0 . Substituting $g(z)=f(z-k)$ in $E$, one derives:

$$
E(z, k)=(z-k)^{2} g^{\prime}(z)+(z-1-k) g(z)+1=0
$$

(iii) The MacLaurin Series for $f$ around $-k$ is the same as the Taylor's Series for $g$ around 0 . Write $g(z)=\sum_{n=0}^{\infty} a_{n} z^{n}$ and substitute in $\mathrm{E}(\mathbf{z}, \mathbf{k})$ :

$$
\begin{aligned}
& g(z)=\sum_{n=0}^{\infty} a_{n} z^{n}=a_{0}+\sum_{n=1}^{\infty} a_{n} z^{n} \\
& g^{\prime}(z)=\sum_{n=1}^{\infty} n a_{n^{2}} z^{n-1} \\
& z^{2} g^{\prime}(z)=\sum_{n=1}^{\infty} n a_{n^{2}} z^{n+1} \\
& -2 z k g^{\prime}(z)=-\sum_{n=1}^{\infty} 2 k n a_{n^{2}} z^{n} \\
& k^{2} g^{\prime}(z)=\sum_{n=1}^{\infty} k^{2} n a_{n^{2}} z^{n-1} \\
& z g(z)=\sum_{n=1}^{\infty} a_{n} z^{n+1} \\
& -k g(z)=-\sum_{n=1}^{\infty} k a_{n} z^{n} \\
& -g(z)=-\sum_{n=1}^{\infty} a_{n} z^{n} \\
& 1=1
\end{aligned}
$$

Taking the sum, grouping coefficients by powers of $z$ and setting the whole equal to 0 leads to the recursion

$$
(n+1) a_{n}-(2 k n+3 k+1) a_{n+1}+k^{2}(n+2) a_{n+2}=0
$$

or

$$
a_{n+2}=\frac{-(n+1) a_{n}+(2 k n+3 k+1) a_{n+1}}{k^{2}(n+2)}
$$

$\mathrm{a}_{0}$ and $\mathrm{a}_{1}$ are connected by $\mathrm{E}(\mathrm{z}, \mathrm{k})$, through setting $\mathrm{z}=0$

$$
\begin{aligned}
& k^{2} a_{1}-(1+k) a_{0}+1=0 \\
& a_{1}=\frac{(1+k) a_{0}-1}{k^{2}}
\end{aligned}
$$

The remaining coefficients can be determined from the recursion. Since both numerator and denominator are linear in $n$, as long as $k \neq 0$, the coefficients will grow on the order of $O\left(\left(\frac{3}{k}\right)^{2 n}\right)$ or less, guaranteeing a positive radius of convegence.
(iv) The coefficients take a particularly simple form when $\mathrm{k}=1$, and the circle of convergence is around the point $(-1,0)$ in the complex plane:

$$
\begin{aligned}
& a_{n+2}=\frac{-(n+1) a_{n}+(2 n+4) a_{n+1}}{(n+2)} \\
& =+2 a_{n+1}-\frac{n+1}{n+2} a_{n}
\end{aligned}
$$

We have a surprise in store for us when $k$ is set equal to 0 . First multiply both sides in the recursion formula by $\mathbf{k}^{2}$, then let k go to 0 . The result is:

$$
a_{n+1}=(n+1) a_{n}
$$

Setting $a_{1}=1$, the formula for $f$ becomes:

$$
\begin{equation*}
f(z)=\sum_{n=0}^{\infty} n!z^{n} \tag{!}
\end{equation*}
$$

This diverges everywhere except at $\mathrm{z}=0, \mathrm{f}(0)=1$. At 0 . f has derivatives of all orders: $f(n)(0)=(n!)^{2}$. This function can therefore be characterized as an analytic function around the origin with radius of convergence $R=0$.

Plugging the above formula into E , one sees that it does indeed constitute a "formal" solution to this differential equation.
(v) For any point $k$ on the complex plane away from the origin, the radius of convergence excludes the origin, and shrinks to nothing as $k$ approaches the origin. As the recursion formula allows $a_{0}$ to be freely chosen, one can set it to 1 . Then the solutions to $\mathrm{E}(-\mathrm{k})$ around k will move continuously to the origin even as the domain of convergence shrinks to a point.


## OProblem 18:

(i) fix $1=0$, fix $_{2}=2 / 3$. Clearly, given any $0 \leq y</ 12, l(l(y))=9 / 4 y$ cannot equal $y$, unless $y=0$, which is a fixed point, not a 2 -cycle

Likewise $\mathrm{r}(\mathrm{r}(\mathrm{y}))=\mathrm{y}=4 \mathrm{y}-2$, or $\mathrm{y}=2 / 3$. This is the other fixed point $r(l(y))=y=2(1-3 y / 2)=2-3 y$, or $y=1 / 2$. In this case $y$ cannot be an argument for 1 . in fact $1 / 2->1-->0$, and can hardly be considered a two-cycle
(ii) Finally $l(r(y))=0=3 / 2(2(1-y)=y=3-3 y$, or $y=3 / 4$. However, under the action of $\chi, 3 / 4$--> $1 / 2$--> 1 -->0

This shows that the the Linear Chaos Machine has no 2-cycles.
(iii) $\gamma=2 / 5->3 / 5->4 / 5->2 / 5$ is the only 3 cycle, corresponding to action by the iterate function $r(r(l)))=\gamma$ Examining the other iterate possbilities shows that this is the only one.

There are two 4-cycles:
$C_{1}=1 / 4$--> 3/8--> 9/16 --> 7/8 --> 1/4
$C_{2}=9 / 13$--> 8/13 --> 10/13 --> 6/13 --> 9/13
(iv) Each n-cycle corresponds to a solution of the fixed point equation for some combination of $l$-functions and r-functions in sequence. Since the Chaos Machine is linear, all $n$-cycle equations are linear, of the form $q x+t=x, q$ $\neq 0$, with unique solutions $x=-t /(q-1)$.

## Orablem 18 :

(i) $F=1 / 3$. Any value between $O$ and $F$ will remain on the right branch after 3 iterations. Any value larger than $F$ will go beyond 0 in the return swing produced by the 3 rd iteration. The situation is made plain by the graph.
(ii) Since $F$ cycles to 0 in 3 iterations, (2/3)F $=2 / 9$ will cycle to 0 in 4 iterations. Uniqueness is easily established.
(iii) $I=5 / 12$ is the larger value. The smaller one is the second inverse iteration from $F=2 / 3 \times 2 / 3 \times 1 / 3=4 / 27$.
(iv) $C=2 / 3 ; G=4 / 9$
(v) Follow the trajectories on the above diagram. Note that, under the action of $\chi$ :
[FI] inverts into [AB] ; [1/3, 5/12] --> [1/2, 5/8]
[AB] rotates to [DE]; [ $1 / 2,5 / 8]$--> [3/4 ,1]
[DE] jumps across to the entire left branch [O,H), plus the isolated point $A=(1 / 2,1)$.
[OH) iterates into itself plus the segment [A,D). A final iteration covers the entire domain $[0,1]$.
(vi) Observe how [IG] inverts into [C J] ; [GH] inverts into [C,D] ; [C,J] rotates into $[B, C]$; $[B C]$ rotates into $[C, D]$; $[C D]$ rotates into $[C A]$; [CA] rotates into [CE] ; [C,E] both rotates into [AC] and jumps across to [O,A) .

A final iteration covers the entire domain $[0,1]$.

## Orablem QO:

(a) A transition (by application of $\mathbf{l}$ ) from $\mathrm{x} \boldsymbol{\varepsilon} \mathrm{L}$ to $\mathrm{y} \boldsymbol{\varepsilon} \mathrm{R}$ implies that $2 / 3$ $\geq y \geq 1 / 2>x$. Therefore one application of $r$ is needed to bring $y$ down to or below the fixed point , and one or more after that to produce a value $z<1 / 2$ $\varepsilon \mathrm{L}$.

Therefore a segment of the form ..LRL .. never occurs in the iterate sequence produced by any $x$ in the domain $[0,1]$.
Orablem 21:
(i) The iterate sequence of a periodic cycle is equivalent to any of its cyclic shifts : LLR $\sim$ LRL $\sim$ RLL, etc. Since the second of these is improper, they are all improper.
(ii) The Chaos Machine $\mathbf{M}$ is linear. After $n$-iterations a sequence $S(x)=(x) S=A_{0} A_{1} \ldots . . . A_{k-1}$ is produced, which, if it is a cycle, will be equal to $x$. The final equation with be of the form $q x+t=x, q \neq 0$, with unique solution $x=-t /(q-1)$. See also problem 28.
Of course not every iterate sequence corresponds to a cycle.

## OProblem QQ:

If $0 \leq \alpha<\frac{3}{4}$, there will be two "inverses", $\tau_{1}, \tau_{2}$ which iterate to $\alpha$, $\tau_{1}$ in $L, \tau_{2}$ in $R$. If, however $\frac{3}{4} \leq \beta \leq 1, \beta$ will have only one inverse, $\tau_{3}$, which is in $R$. In setting up the chain of back-reconstructions, these conditions are precisely those required for any sequence from $\boldsymbol{\beta}$ forwards to $\boldsymbol{\alpha}$ be strictly proper.

Example: Let $\alpha=1 / 3$. The chain of back-iterations begins with:


The chain can be extended indefinitely. Any any stage $k$, by advancing along all possible paths back to $1 / 3$, one produces all
possible strictly proper iterate sequences. For example, the sequence corresponding to $7 / 18$ is LRR, which is the function $y$ $=r(r(l(x)))=6 x-2$. Substituting gives $6(7 / 18)-2=1 / 3$.

## OProblem 23:

Since the numerator and denominator of $\varphi(\mathbf{r})$ are already in lowest terms, the first iteration of $\varphi$ is:

$$
\begin{aligned}
& \varphi^{(2)}(r)=\varphi \varphi(r)=\frac{p^{2} P\left(p^{2} / q(1+p)\right.}{q(1+p)\left(1+P\left(\frac{p^{2}}{q(1+p)}\right)\right.} \\
& =\frac{p^{2}}{q(1+p)} \frac{p^{2}}{\left(1+p^{2}\right)}=\frac{p^{4}}{q(1+p)\left(1+p^{2}\right)} \\
& =\left(\frac{p}{q}\right) \frac{p^{3}}{(1+p)\left(1+p^{2}\right)}=r \frac{1}{q\left(1+\frac{1}{p}\right)\left(1+\frac{1}{p^{2}}\right)}
\end{aligned}
$$

The $\mathbf{n}^{\text {th }}$ iteration of this formula extends it to:

$$
\varphi^{(n)}(r)=r \frac{1}{\left(1+\frac{1}{p}\right)\left(1+\frac{1}{p^{2}}\right) . .\left(1+\frac{1}{p^{2^{n}}}\right)}
$$

To evaluate this product, notice that when the multiplications are performed, the exponents of $p$ will be all of the positive integers, expressed in the binary system, up to the exponent $2^{\mathrm{n}+1}-1$. Therefore:

$$
\begin{aligned}
& \lim _{n \rightarrow \infty} \varphi^{(n)}(r)=r \frac{1}{\left(1+\frac{1}{p}+\frac{1}{p^{2}}+\frac{1}{p^{3}}+\ldots . .\right.} \\
& =\frac{p}{q} \frac{1}{\left(\frac{1}{\left.1-\frac{1}{p}\right)}\right.}=\frac{p-1}{q}(!)
\end{aligned}
$$

## OPrablem Q4:

(i) Let:

$$
I=\left(\begin{array}{ll}
1 & 0 \\
0 & 1
\end{array}\right) ; \alpha_{1}, \alpha_{2}, \beta_{1}, \beta_{2} \in M_{2}
$$

Then one may write :

$$
\begin{aligned}
& P(x, y)=x^{2}+a x y+b x+c y=\left(I x+\alpha_{1} y+\beta_{1}\right)\left(I x+\alpha_{2} y+\beta_{2}\right) \\
& \left.=x^{2}+x y\left(\alpha_{1}+\alpha_{2}\right)+x\left(\beta_{1}+\beta_{2}\right)+\alpha_{1} \alpha_{2} y^{2}+y \alpha_{1} \beta_{2}+\beta_{1} \alpha_{2}\right)+\beta_{1} \beta_{2}
\end{aligned}
$$

Identifying terms on both sides of the equation:

$$
\begin{aligned}
& \text { (i) } \alpha_{1} \alpha_{2}=0 \\
& \text { (ii) } \beta_{1} \beta_{2}=0 \\
& \text { (iii) } \alpha_{1}+\alpha_{2}=a I ; \alpha_{2}=a I-\alpha_{1} \\
& \text { (iv) } \beta_{1}+\beta_{2}=b I ; \beta_{2}=b I-\beta_{1} \\
& \text { (v) } \alpha_{1} \beta_{2}+\beta_{1} \alpha_{2}=c I
\end{aligned}
$$

Substituting (iii) and (iv) into (i) and (ii) :

$$
\begin{aligned}
& \alpha_{1}\left(a I-\alpha_{2}\right)=0 \\
& \beta_{1}\left(b I-\beta_{2}\right)=0
\end{aligned}
$$

Write $\alpha_{1}$ and $\beta_{1}$ in terms of their entries, to be determined:

$$
\alpha_{1}=\left(\begin{array}{cc}
r_{1} & r_{2} \\
r_{3} & r_{4}
\end{array}\right) ; \beta_{1}=\left(\begin{array}{ll}
s_{1} & s_{2} \\
s_{3} & s_{4}
\end{array}\right)
$$

Despite the absence of a term in $\mathbf{y}^{2}$, the relations (i) - (v) are symmetric in the $\alpha$ 's and $\boldsymbol{\beta}$ 's, while relations (i) - (iv) are symmetric in the indices $\mathbf{1}$ and 2 Looking first at the $\alpha$ 's :

$$
\begin{aligned}
& 0=\alpha_{1} \alpha_{2}=\alpha_{1}\left(a I-\alpha_{1}\right)=\left(\begin{array}{ll}
r_{1} & r_{2} \\
r_{3} & r_{4}
\end{array}\right)\left(\begin{array}{cc}
a-r_{1} & -r_{2} \\
-r_{3} & a-r_{4}
\end{array}\right) \\
& \text { (vi) } r_{1} a-r_{1}^{2}-r_{2} r_{3}=0 \\
& \text { (vii) }-r_{1} r_{2}+a r_{2}-r_{2} r_{4}=0 \\
& \text { (viii) } a r_{3}-r_{1} r_{3}-r_{3} r_{4}=0 \\
& \text { (ix) }-r_{2} r_{3}+a r_{4}-r_{2}^{4}=0
\end{aligned}
$$

Simple algebraic manipulations yield:

$$
\begin{aligned}
& r_{2}\left(a-\left(r_{1}+r_{4}\right)\right)=0 \\
& r_{3}\left(a-\left(r_{1}+r_{4}\right)\right)=0
\end{aligned}
$$

Case 1: $r_{2}=r_{3}=0 ; r_{1}+r_{4}$ need not equal $a$.

Case2: $\mathrm{r}_{1}+\mathrm{r}_{4}=\mathrm{a}$

## Case 1 :

From equations (vi) and (ix) one sees that:

$$
\begin{aligned}
& r_{1} a=r_{1}^{2} ; r_{4} a=r_{4}^{2} \\
& {\left[\left(r_{1}=a\right) \vee\left(r_{1}=0\right)\right] \wedge\left[\left(r_{4}=a\right) \vee\left(r_{4}=0\right)\right]}
\end{aligned}
$$

For Case I therefore, the choices for the matrices $\alpha_{1}, \alpha_{2}$ are distributed among: $\left(\begin{array}{ll}a & 0 \\ 0 & a\end{array}\right),\left(\begin{array}{ll}0 & 0 \\ 0 & a\end{array}\right),\left(\begin{array}{ll}a & 0 \\ 0 & 0\end{array}\right),\left(\begin{array}{ll}0 & 0 \\ 0 & 0\end{array}\right)$;

$$
\alpha_{1}=\left(\begin{array}{ll}
a & 0 \\
0 & a
\end{array}\right) \rightarrow \alpha_{2}=\left(\begin{array}{ll}
0 & 0 \\
0 & 0
\end{array}\right)
$$

Staying with this option for the moment, substitute into equation (v) :

$$
\begin{aligned}
& \alpha_{1} \beta_{2}+\beta_{1} \alpha_{2}=c=a \beta_{2} \\
& \therefore \beta_{2}=(c / a) I
\end{aligned}
$$

The symmetry relations allow us to also write: $\beta_{2}=b I ; \beta_{1}=0$. Therefore $\mathbf{b}=\mathbf{c} / \mathbf{a}$. We have shown that:
(i) Theorem I: $b=c / a$ is the condition for having non-singular matrices in the decomposition of $P(x, y)$ into linear factors over $M_{2}$.
(ii) The other possibility in the Case 1 option is:

$$
\alpha_{1}=\left(\begin{array}{ll}
a & 0 \\
0 & 0
\end{array}\right) ; \alpha_{2}=\left(\begin{array}{ll}
0 & 0 \\
0 & a
\end{array}\right)
$$

; or the reverse. Substituting into (v):

$$
\begin{aligned}
& \left(\begin{array}{ll}
a & 0 \\
0 & 0
\end{array}\right)\left(\begin{array}{cc}
b-s_{1} & -s_{2} \\
-s_{3} & b-s_{4}
\end{array}\right)+\left(\begin{array}{ll}
s_{1} & s_{2} \\
s_{3} & s_{4}
\end{array}\right)\left(\begin{array}{ll}
0 & 0 \\
0 & a
\end{array}\right)=\left(\begin{array}{ll}
c & 0 \\
0 & c
\end{array}\right) \\
& =\left(\begin{array}{cc}
a\left(b-s_{1}\right) & 0 \\
0 & a s_{4}
\end{array}\right)
\end{aligned}
$$

Therefore:

$$
\begin{aligned}
& a b-a s_{1}=c ; a s_{4}=c \\
& s_{1}=\frac{a b-c}{a} ; s_{4}=\frac{c}{a} \\
& \therefore s_{1}+s_{4}=b
\end{aligned}
$$

It has been shown that:
Theorem II : If the r's are in Case 1, then the s's are in Case 2. If the s's are in Case 1, the r's are in Case 2.

We have not yet looked at Case 2.
Case 2: If the $\alpha$ 's satisfy the relation of Case 2 , then we may compute the values of the r's in terms of any one of them from the basic relations:

$$
\begin{aligned}
& r_{1}+r_{4}=a \\
& r_{1} a=r_{1}^{2}+r_{2} r_{3} \\
& r_{4} a=r_{4}^{2}+r_{2} r_{3}
\end{aligned}
$$

$r_{1}$ and $r_{4}$ are the two roots of the quadratic equation:

$$
\begin{aligned}
& \theta^{2}-a \theta+r_{2} r_{3}=0 \\
& \therefore r_{1}, r_{4}=\frac{a \pm \sqrt{a^{2}-4 r_{2} r_{3}}}{2} ; \\
& \therefore r_{1} r_{4}=r_{2} r_{3}
\end{aligned}
$$

Likewise , if the $\boldsymbol{\beta}$ 's are in the Case 2, one has

$$
\begin{aligned}
& s_{1}+s_{4}=b \\
& s_{1} s_{4}=s_{2} s_{3}
\end{aligned}
$$

Theorem III : If the $\alpha$ 's are in Case 1, then the $\beta$ 's are in Case 2 , with these values (up to symmetry):

$$
\begin{aligned}
& \alpha_{1}=\left(\begin{array}{ll}
a & 0 \\
0 & 0
\end{array}\right) ; \alpha_{2}=\left(\begin{array}{ll}
0 & 0 \\
0 & a
\end{array}\right) \\
& s_{1}=\frac{a b-c}{a} ; s_{4}=\frac{c}{a} \\
& s_{2} s_{3}=s_{1} s_{4}=\frac{c}{a}\left(\frac{a b-c}{a}\right)=\frac{a b c-c^{2}}{a^{2}}
\end{aligned}
$$

$\mathbf{s}_{2}$ ( or s3) can be arbitrary. All other values are uniquely determined.
Likewise, if the $\boldsymbol{\beta}$ 's are in Case 1 :

$$
\begin{aligned}
& \beta_{1}=\left(\begin{array}{ll}
a & 0 \\
0 & 0
\end{array}\right) ; \beta_{2}=\left(\begin{array}{ll}
0 & 0 \\
0 & a
\end{array}\right) \\
& r_{1}=\frac{a b-c}{b} ; r_{3}=\frac{c}{b} \\
& r_{2} r_{3}=r_{1} r_{4}=\frac{c}{b}\left(\frac{a b-c}{b}\right)=\frac{a b c-c^{2}}{b^{2}}
\end{aligned}
$$

The only remaining question is: are there solutions for which both the $\alpha$ 's and the $\beta$ 's are in Case 2 ? The conditions are:

$$
\begin{aligned}
& r_{1}+r_{4}=a ; s_{1}+s_{4}=b \\
& r_{1} r_{4}=r_{2} r_{3} ; s_{1} s_{4}=s_{2} s_{3}
\end{aligned}
$$

Substituting in relation (v) :

$$
\left(\begin{array}{ll}
c & 0 \\
0 & c
\end{array}\right)=\left(\begin{array}{cc}
r_{1} & r_{2} \\
r_{3} & r_{4}
\end{array}\right)\left(\begin{array}{cc}
b-s_{1} & -s_{2} \\
-s_{3} & b-s_{4}
\end{array}\right)+\left(\begin{array}{ll}
s_{1} & s_{2} \\
s_{3} & s_{4}
\end{array}\right)\left(\begin{array}{cc}
a-r_{1} & -r_{2} \\
-r_{3} & a-r_{4}
\end{array}\right)
$$

This translates into four equations:

$$
\begin{aligned}
& E_{1}: b r_{1}+a s_{1}-2 r_{1} s_{1}-\left(r_{2} s_{3}+r_{3} s_{2}\right)=c \\
& E_{2}: b r_{4}+a s_{4}-2 r_{4} s_{4}-\left(r_{2} s_{3}+r_{3} s_{2}\right)=c \\
& E_{3}: b r_{3}+a s_{3}-\left(r_{3} s_{1}+r_{1} s_{3}+r_{3} s_{4}+r_{4} s_{3}\right)=0 \\
& E_{4}: b r_{2}+a s_{2}-\left(r_{2} s_{1}+r_{1} s_{2}+r_{2} s_{4}+r_{4} s_{2}\right)=0
\end{aligned}
$$

Subtracting $\mathrm{E}_{2}$ from $\mathrm{E}_{1}$ and wading through the computations one ends up with the equations

$$
\begin{aligned}
& E_{5}: a s_{1}+b r_{1}-r_{1} s_{1}=a b \\
& E_{5}: a s_{4}+b r_{4}-r_{4} s_{4}=a b
\end{aligned}
$$

In combination with the conditions: $r_{1}+r_{4}=a ; s_{1}+s_{4}=b$, the other equations turn out to be identities. Therefore we know that

$$
\begin{aligned}
& s_{1}\left(a-r_{1}\right)=a b-r_{1} b=b\left(a-r_{1}\right) \\
& \therefore s_{1} r_{4}=b r_{4}
\end{aligned}
$$

If $s_{2}=0$, then the a's are in Case 1. If $\mathbf{r}_{\mathbf{4}} \neq 0$, then divide through to derive $s_{1}=b$, and the s's are in Case $1!$ Likewise for $r_{2}=0, s_{4} \neq 0$

Theorem IV: The r's are in Case 1 IF AND ONLY IF the s's are in Case 2. The s's are in Case 1 IF AND ONLY IF the r's are in Case 2 .

This is the general solution, covering both singular and non-singular factorizations.

Note: When $\mathrm{ab}=\mathrm{c}, \mathrm{P}(\mathrm{x}, \mathrm{y})$ factors as $\mathrm{P}(\mathrm{x}, \mathrm{y})=(\mathrm{x}+\mathrm{ay})(\mathrm{x}+\mathrm{b})$.
(iii) Factoring the general quadratic equation in 2 variables can always be done in terms of quaternions $i, j, k$. Since for any 3 linear forms $(A x+B y+C)$ in $x$ and $y, T_{1}, T_{2}, T_{3}$ one has

$$
T_{1}^{2}+T_{2}^{2}+T_{3}^{2}=\left(i T_{1}+j T_{2}+k T_{3}\right)\left(-i T_{1}-j T_{2}-k T_{3}\right)
$$

one can readily put any quadratic form $F$ into the form of a sum squares of 3 linear forms. This is known as the Inertia Theorem and is extensively used in Differential Geometry.
OPrablem 25:
We will construct a set of numbers $S_{R}$ derived from the indices, that will be invariant under row operations and switching operations. Observe that if:

$$
R_{j}=a_{j 1} \quad a_{j 2} \quad \ldots a_{j n}
$$

then the sum of all the indices of all of its entries is given by:

$$
(j+1)+(j+2)+\ldots+(j+n)=n\left(j+\frac{n+1}{2}\right) \equiv r_{j}
$$

Calculating this figure for each $\mathbf{j}$ produces a set of numbers:

$$
S_{R}=\left(r_{1}, r_{2}, \ldots, r_{j}, \ldots, r_{n}\right)
$$

The corresponding set of numbers for the columns $\mathrm{S}_{\mathrm{C}}$ is identical.

## Theorem:

Neither row operations nor switching operations alter the content of $S_{R}$ or $S_{C}$. Since row operations merely permute the order of rows or columns, and that of the elements within them, without altering their content, this part is clear. The switching operations $\sigma_{\mathbf{j}}$ are all of the form $a_{i j} \leftrightarrow a_{j i}, i=1,2, \ldots, n$, which does not alter the sum $\mathbf{i}+\mathbf{j}$ that goes into the corresponding entries in $S_{R}$ or $S_{C}$.

Consider now what happens when $a_{11}$ and a12 are switched. The sum of all the indices in $\mathrm{C}_{1}$ becomes

$$
\begin{aligned}
& s_{1}=(1+2)+(2+1)+\ldots+(N+1) \\
& =n\left(1+\frac{n+1}{2}\right)+1
\end{aligned}
$$

It is evident that this cannot be any of the entries in SC before these terms were interchanged; for one thing, the difference of any two elements of $S_{C}$ is divisable by $n$, but subtracting the above from $s_{j}$ for example, produces the number $\mathrm{n}(\mathrm{j}-1)-1$. Q.E.D.

(i) $A=\left\{a_{i j}\right\}, i, j=1,2, \ldots ., n$

We can expand det A in terms of its co-factors in two ways

$$
\begin{aligned}
& \text { (a) } \operatorname{det} A=a_{11} M_{11}+a_{12} M_{12}+\ldots+a_{1 n} M_{1 n} \\
& \text { (b) } \operatorname{det} A=a_{11} M_{11}+a_{21} M_{21}+\ldots+a_{n 1} M_{n 1}
\end{aligned}
$$

Since the operator $P(A)$ only affects the top row of $A$, the co-factors of expansion (a) are unchanged by it, and one can write:

$$
\operatorname{det} P(A)=a_{21} M_{11}+a_{11} M_{12}+\ldots+a_{1 n} M_{1 n}
$$

Likewise, the transpose inverse of $\mathrm{A}, \mathrm{B}=\left(\mathrm{A}^{\mathrm{T}}\right)^{-1}$, has entries

$$
b_{i j}=\frac{M_{i j}}{\operatorname{det} A}
$$

Therefore:

$$
\begin{aligned}
& \operatorname{det} P\left(\left(A^{T}\right)^{-1}\right)=\operatorname{det} T\left(P\left(\left(A^{T}\right)^{-1}\right)\right. \\
& =\operatorname{det} P T\left(A^{-1}\right) \\
& =\left(\frac{a_{21}}{\operatorname{det} A}\right) \frac{M_{11}}{\operatorname{det} A}+\left(\frac{a_{11}}{\operatorname{det} A}\right) \frac{M_{12}}{\operatorname{det} A}+\ldots+\left(\frac{a_{1 n}}{\operatorname{det} A}\right)\left(\frac{M_{1 n}}{\operatorname{det} A}\right) \\
& \frac{a_{21} M_{11}+a_{11} M_{21}+\ldots+a_{n 1} M_{n 1}}{(\operatorname{det} A)^{2}} \\
& =\frac{\operatorname{det} P(A)}{(\operatorname{det} A)^{2}} \\
& \therefore \frac{\operatorname{det} P(A)}{\operatorname{det} P^{T}\left(A^{-1}\right)}=(\operatorname{det} A)^{2}
\end{aligned}
$$

(ii) $\operatorname{Trace} \mathrm{PP}^{\mathrm{T}}(\mathrm{A})$ begins with the entries $\mathrm{a}_{12}+\mathrm{a}_{22}$. Trace $\mathrm{P}(\mathrm{A})$ also begins with these entries. Since these operators only affect entries a11, a12, and $a_{21}$, the rest of the trace is left unaltered. The result follows
(iv) P cannot be cancelled from both sides in this equation, because $P$ acts like a function on different matrices on the left and the right.
(v) Prablem Q7: Left as an exercise for the reader!

