Solution.

(i) Let $A$ have $(r,s)$-entry $a_{rs} \in \mathbb{C}$. Writing $a_{rs} = \beta_{rs} + i\gamma_{rs}$ with $\beta_{rs}, \gamma_{rs} \in \mathbb{R}$ we see that $A = P + iQ$ where $P$ and $Q$ have $(r,s)$-entries $\beta_{rs}$ and $\gamma_{rs}$ (respectively).

(ii) Since $(P + iQ)^t = (P - iQ)^t = P^t - iQ^t$ we see that $A = P + iQ$ is Hermitian if and only if $P^t = P$ and $Q^t = -Q$.

(iii) Recall that transposing reverses products; that is, $(XY)^t = Y^t X^t$ whenever the left hand side is defined. (Note that this implies that $(A^{-1})^t = (A^t)^{-1}$ whenever $A$ is nonsingular. It is also clear that taking complex conjugates preserves sums and products, and commutes with the maps $A \mapsto A^{-1}$ and $A \mapsto A^t$.) Let $v$ be an arbitrary column vector and let $z = v^t Av$. Since $z$ is a $1 \times 1$ matrix we have $v^t = z$, and so

$$z = ([v^t Av])^t = v^t A^t v = v^t Av = z.$$ 

Thus $z$ is real.

(iv) Suppose that $A$ is positive definite. Note first that since $A$ is Hermitian it must be square (as its transpose is the same shape as itself). Now let $v$ be in the nullspace of $A$; that is, $v$ is a column vector such that $Av = 0$. Then $v^t Av = 0$, and positive definiteness of $A$ gives $v = 0$. So the nullspace of $A$ is $\{0\}$; this implies that $A$ is nonsingular.

Let $A$ be an arbitrary positive definite $n \times n$ Hermitian matrix. We use induction on $n$ to prove that $A$ has the desired form; note that in the case $n = 1$ the matrix $A$ is simply a positive real number, and we may take $B = \sqrt{A}$. Let $e_1$ be the $1$-th column of the identity matrix (so that $e_1, e_2, \ldots, e_n$ comprise the standard basis of $\mathbb{C}^n$). The $(1,1)$-entry of $A$ is $\sqrt{a_{11}} a_{11}$, which must be positive since $A$ is positive definite. Thus we can write

$$A = \begin{pmatrix} a & \bar{x}^t \\ x & A' \end{pmatrix},$$

where $a$ is real and positive, $x \in \mathbb{C}^{n-1}$ and $A'$ is some $(n-1) \times (n-1)$ Hermitian matrix. Now set

$$D = \begin{pmatrix} \sqrt{a^{-1}} & 0 \\ -a^{-1} x & 1 \end{pmatrix}$$

and observe that $D$ is nonsingular; indeed, as a row operation matrix the effect of $D$ is to divide the first row by $\sqrt{a}$ and add multiples of the first row to the others. We see that the first column of $DA$ is $(\sqrt{a} e_1)$. Now postmultiplication by $D^*$ performs a corresponding sequence of column operations, and we find that

$$DAD^* = \begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix}.$$
Since $A$ was positive definite, this must be too. Hence $A''$ is a $(n-1) \times (n-1)$ positive definite matrix. By induction we can write $A'' = \overline{Y}^t Y$, and this gives

$$A = D^{-1} \left( \begin{array}{cc} 1 & 0 \\ 0 & Y \end{array} \right)^t \left( \begin{array}{cc} 1 & 0 \\ 0 & Y \end{array} \right) \overline{D}^{-1} = \overline{B}^t B$$

where $B = \left( \begin{array}{cc} 1 & 0 \\ 0 & Y \end{array} \right) \overline{D}^{-1}$.

(vi) If $A, B \in \text{GL}_n(\mathbb{C})$ are positive definite and $0 \neq v \in \mathbb{C}^n$ then

$$\overline{v} (A + B)v = \overline{v} Av + \overline{v} Bv > 0$$

(since $\overline{v} Av > 0$ and $\overline{v} Bv > 0$).

(vii) We see that $\overline{Y}^t AY = \sum_{X \in G} (\overline{Y} X^t)(XY) = \sum_{Z \in G} \overline{Z}^t Z = A$ (since $Z = XY$ runs through all elements of $G$ as $X$ does).

(viii) By (vii) we can find a positive definite $A$ such that $\overline{Y}^t AY = A$ for all $Y \in G$, and by (v) we can put $A = \overline{D}^t B$. But the equation $\overline{Y}^t B^t BY = \overline{B}^t B$ can be written as $BY^{-1}B^{-1} = (\overline{B}^{-1})^t \overline{B}^t$, or, equivalently,

$$(BYB^{-1})^{-1} = (\overline{B}^tD)^t,$$

showing that $BYB^{-1}$ is unitary for all $Y \in G$.

2. Recall that the dot product on $\mathbb{C}^n$ is defined by $u \cdot v = \overline{v} v$, and that unitary matrices preserve it (in the sense that $(Xu) \cdot (Xv) = u \cdot v$ for all $u$ and $v$ if $X$ is unitary). Recall also that if $U$ is a subspace of $\mathbb{C}^n$ then $\mathbb{C}^n = U \oplus U^\perp$, where

$$U^\perp = \{ v \in \mathbb{C}^n \mid u \cdot v = 0 \text{ for all } u \in U \}$$

(the orthogonal complement of $U$).

Let $G$ be a finite group of $n \times n$ unitary matrices, and let $U$ be a $G$-invariant subspace of $\mathbb{C}^n$. (That is, if $X \in G$ and $u \in U$ then $Xu \in U$.) Prove that the orthogonal complement of $U$ is also $G$-invariant.

Solution.

Let $v \in U^\perp$ and let $X \in G$. Then for all $u \in U$ we have that $X^{-1}u \in U$ (since $X^{-1} \in G$ and $U$ is $G$-invariant), and so

$$(Xv) \cdot u = Xv \cdot X(X^{-1}u)$$

$= v \cdot X^{-1}u$ (since $X$ is unitary)

$= 0$ (since $v \in U^\perp$).

Hence $Xv \in U^\perp$, and since this holds for all $X \in G$ and $v \in U^\perp$ we have shown that $U^\perp$ is $G$-invariant.

3. Let $H$ and $N$ be groups and $\phi : H \to \text{Aut}(N)$ a homomorphism. Define

$$H \ltimes N = \{(h, x) \mid h \in H, x \in N\}$$

with multiplication given by

$$(h, x)(k, y) = (hk, x^{\phi(h)}y)$$

for all $h, k \in H$ and $x, y \in N$. Prove that this makes $H \ltimes N$ into a group. (Such a group is called a semidirect product of $N$ by $H$. If $\phi$ is the trivial homomorphism $(h \mapsto 1 \in \text{Aut}(N)$ for all $h \in H$) we get the direct product of $N$ and $H$.)

Solution.

Since $\phi$ is a homomorphism we have $\phi(1) = 1$, where the 1 on the left hand side is the identity element of $H$ and the 1 on the right hand side is the identity automorphism of $N$. Hence our multiplication rule gives

$$(h, x)(1, 1) = (h1, x^{\phi(1)}1) = (h, x).$$

Since all automorphisms of $N$ map 1 to 1 we also find that

$$(1, 1)(h, x) = (1h, 1^{\phi(h)}x) = (h, x).$$

So $H \ltimes N$ has an identity element. The following calculation proves associativity:

$$((h, x)(k, y))(l, z) = (hk, x^{\phi(k)}y)(l, z) = (hkl, (x^{\phi(k)}y)^{\phi(l)}z)$$

$$= (h, x)(kl, y^{\phi(l)}z) = (h, x)((k, y)(l, z)).$$

Let $(h, x)$ be an arbitrary element of $H \ltimes N$, and let $k = h^{-1}$ and $y = (x^{-1})^{\phi(k)}$. Since $(x^{-1})^{\phi(k)} = (x^{\phi(k)})^{-1}$ we see that $(h, x)(k, y) = (hk, x^{\phi(k)}y) = (1, 1)$. Moreover, since $\phi(k)\phi(h) = \phi(hk)$ we also have that $y^{\phi(h)} = x^{-1}$, and $(k, y)(h, x) = (kh, y^{\phi(h)}x) = (1, 1)$, so that $(k, y)$ is definitely the inverse of $(h, x)$.  
