Rigid motion must be injective, as if $\psi(p)=\psi(q)$, then $\|p-q\|=\|\psi(p)-\psi(q)\|=0$ so $p=q$.

22.7 (a) The set of rigid motions of R^{n+1} obviously forms a group under composition. It naturally satisfies associativity, neutral element is identity transformation, inverse element exists because rigid motions map onto R^{n+1} by ~~collo~~ corollary. Inverse is obviously rigid motion. Identity ~~belongs to~~ is a symmetry of S. For any symmetry of S ψ, as it maps onto S, it must be bijective. Its inverse is also a symmetry of S. Thus the symmetries of S form a subgroup.

(b) For any symmetry φ, suppose $\psi=\varphi_2\circ\varphi_1$ is the unique decomposition of ψ into an orthogonal transformation φ_1 followed by a translation φ_2. By definition, for any $p\in S^n$, $\varphi(p)=\varphi_1(p)+a \in S^n$ (let φ_2 be translation by a). As $-p\in S^n$, $\varphi(-p)=\varphi_1(-p)+a=-\varphi_1(p)+a\in S^n$. So $\|\varphi_1(p)+a\|=1=\|-\varphi_1(p)+a\|$.
So $a\cdot\varphi_1(p)=\frac{1}{4}(\|\varphi_1(p)+a\|^2-\|\varphi_1(p)-a\|^2)=0$, so $a\cdot\varphi(p)=a(\varphi_1(p)+a)=\|a\|^2$, $\in S^n$ $\forall p$.
But as ~~$\varphi(p)$~~ φ maps onto S^n, ~~as the only possi~~ there must be a $p_0\in S^n$, s.t. $\varphi(p_0)=-a/\|a\|$, then $a\cdot\varphi(p_0)=-\|a\|\neq\|a\|^2$ unless $a=0$.
So if φ is symmetry of S^n, then φ must be an orthogonal transformation ①.
Conversely, for any orthogonal transformation ψ, if $p\in S^n$, then $\|\psi(p)\|=\|p\|=1$. So $\psi(p)\in S^n$. By Corollary, ψ maps R^{n+1} onto R^{n+1}, so for any $q\in S^n$, there must be a $p\in R^{n+1}$, s.t. $\psi(p)=q$. then $\|p\|=\|\psi(p)\|=\|q\|=1$, i.e., $p\in S^n$. Thus ψ maps S^n onto S^n. Combining ①, we prove (b).

(c) Using ~~notation~~ as in (b), let φ_2 be ~~rotation~~ translation by (a_1,a_2,a_3), and $\varphi_1=(\alpha_1,\alpha_2,\alpha_3)$.
Then for any $p\in$ this cylinder C, $\varphi(p)\in C$, i.e., $(\alpha_1(p)+a_1)^2+(\alpha_2(p)+a_2)^2=a^2$ ①
As $-p$ and $\varphi(-p)\in C$, $(-\alpha_1(p)+a_1)^2+(-\alpha_2(p)+a_2)^2=a^2$ ②. ①−②: $\alpha_1(p)\cdot a_1+\alpha_2(p)\cdot a_2=0$
If φ maps C onto C, then there must be a $p_0\in C$, s.t. $\begin{pmatrix}\alpha_1(p_0)+a_1\\ \alpha_2(p_0)+a_2\end{pmatrix}=\begin{pmatrix}a_1\\ a_2\end{pmatrix}\cdot(-a/(a_1^2+a_2^2)^{1/2})$
then $\alpha_1(p_0)a_1+\alpha_2(p_0)a_2=\left[-\frac{a}{r}\begin{pmatrix}a_1\\ a_2\end{pmatrix}-\begin{pmatrix}a_1\\ a_2\end{pmatrix}\right]\cdot\begin{pmatrix}a_1\\ a_2\end{pmatrix}=-ar-r^2$, where $r=\sqrt{a_1^2+a_2^2}$.
assuming $a>0$. So $\alpha_1(p_0)a_1+\alpha_2(p_0)a_2\leq 0$ and it equals 0 iff $r=0$ i.e. $a_1=a_2=0$
Now look at restrictions on φ_1. $\varphi(p)=(\alpha_1(p),\alpha_2(p),\alpha_3(p)+a_3)$ By Ex 22.3 (c), A is orthonormal.
Let the matrix of φ_1 wrt standard basis of R^3 be $A=(\beta_1,\beta_2,\beta_3)^T$, $\forall p\in C$.
let $p=(p_1,p_2,p_3)$, then $\varphi(p)=\left(\sum_{k=1}^{3}\beta_{1k}p_k,\ \sum_{k=1}^{3}\beta_{2k}p_k,\ \sum_{k=1}^{3}\beta_{3k}p_k+a_3\right)$
Since p_3 can be in R, so if $\beta_{13},\beta_{23}\neq 0$, then the first two coordinates can go to infinity, rather than restricted on a circle of radius a. So $\beta_{13}=\beta_{23}=0$.
Then there is guarantee that $\left(\sum_{k=1}^{2}\beta_{1k}p_k\right)^2+\left(\sum_{k=1}^{2}\beta_{2k}p_k\right)^2=a^2$ as $\begin{pmatrix}\beta_{11}&\beta_{12}\\ \beta_{21}&\beta_{22}\end{pmatrix}$ is orthonormal ~~by Ex 22.3 (c)~~ and $\|p\|=a$. If $\beta_{33}=0$, then $\sum_{k=1}^{2}\beta_{3k}p_k+a_3$ ~~can only~~ must be bounded because p_1,p_2 are bounded ($p_1^2+p_2^2=a^2$). So $\beta_{33}\neq 0$. [This can also be seen by A being orthonormal and $\beta_{13}=\beta_{23}=0$]. But now β_{32} and β_{33} must be 0, because so far