(1) (6.26) Let $\phi : U(16) \to U(16)$ be defined by $x \mapsto x^3$. Show that $\phi$ is an automorphism of $U(16)$.

**Proof.** Note that $U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$, so the order of the group is 8. First we show that the map is structure preserving. Let $x, y \in U(16)$. Then $\phi(xy) = (xy)^3 = x^3y^3$, since the group is abelian.

Next we show that it is injective, which is sufficient to show that it is a bijection, since the group is finite. This has to be done by brute force at this point. Namely look at all 8 elements and then list the cube of each element. We see that there is no repetition. On the other hand, after the next section, we could use Lagrange's Theorem. To see how just note that $x^3 = y^3$ implies $(xy^{-1})^3 = 1$. Thus the order of $xy^{-1}$ must divide 3. Since it also must divide 8, the order of the element is one. Equivalently, $x = y$, which shows that th map is injective.

It is clear, that if 3 is replaced with any odd number the map is still a bijection, and hence an automorphism.

(2) (7.26) Show that if $G$ is a group with more than one element and such that $G$ has no proper subgroups, then $|G|$ is finite

**Proof.** Let $a \in G$ such that $a \neq e$. Then $\langle a \rangle$ is a nontrivial subgroup of $G$. Hence by assumption it is all of $G$. Thus $G$ is cyclic. Next suppose that $G$ is infinite. Then $a^2$ generates a proper subgroup of $G$ - contradiction. Thus $G$ is finite. Finally suppose that $|G| = n$ is not prime and let $d$ be a divisor of $n$, where $d \neq 1$ and $d \neq n$. By the Fundamental Theorem of cyclic groups, $G$ has a subgroup of order $d$ - contradiction (note Lagrange's Theorem is not relevant here, one needs the converse of Lagrange, which only exists for cyclic groups).

(3) (7.30) Show that a group $G$ of order 8 must have an element of order 2.

**Proof.** By Lagrange every element of $G$ other than $e$ has order either 2, 4 or 8. If $x \in G$ has order 4, then $x^2$ has order 2. Similarly if $y \in G$ has order 8, then $x^4$ has order 2 - done.

(4) (7.32) Determine all finite subgroups of $\mathbb{C}^*$, the group of nonzero complex numbers under multiplication.

**Proof.** First note that any nonzero element $z$ of the complexes can be written in the form

$$r(\cos(\theta) + i\sin(\theta))$$

where $r$ is a positive real number, and $0 \leq \theta < 2\pi$. Moreover, if $z' = r'(\cos(\theta') + i\sin(\theta'))$, then

$$zz' = rr'(\cos(\theta + \theta') + i\sin(\theta + \theta')).$$

Now let $H$ be a finite subgroup of $\mathbb{C}^*$, and let $z \in H$. Then for some $n$, $1 = z^n = r^n(\cos(n\theta) + i\sin(n\theta))$. But $r^n = 1$ implies that $r = 1$, i.e., $z$ is on the unit circle. We also have that$n\theta$ is a multiple of $2\pi$, i.e. $n\theta = k(2\pi)$ or $\theta = 2k\pi/n$ (a rational multiple of $\pi$).

Finally we claim that $H$ must be cyclic. Let $\alpha$ be the minimal angle among all $z \in H$, say $z = \cos(\alpha) + i\sin(\alpha)$. If $z$ does not generate, let $z' = \cos(\beta) + i\sin(\beta) \in H$ not be a power of $z$. Thus $\beta$ is not an integer multiple of $\alpha$. Since $\beta$ is minimal, there exists an integer $m > 0$ such that $\alpha > \beta - m\alpha > 0$. In particular $z'(z^{-m}) = \cos(\beta - m\alpha) + i\sin(\beta - m\alpha) \in H$. But this contradicts the minimality of $\alpha$ among angles in $H$. Thus $z'$ cannot exist and so $H$ is cyclic.