19.4.1) In Figure 19.2, number the diagonals $AA', BB', CC', DD'$ as 1, 2, 3, 4, respectively. Let $G$ be the symmetry group of the cube (i.e., the group of rotations of $\mathbb{R}^3$ that map the cube to itself). Then $G$ acts on the set of diagonals, which has been identified with the set \{1, 2, 3, 4\}, so we get a homomorphism $\phi: G \to S_4$ describing the action. Problem 19.4.1 asks us to show that $\phi$ is surjective (every permutation of the four diagonals is induced by symmetry of the cube), and Problem 19.4.2 asks us to show that $\phi$ is injective.

Let us prove the surjectivity. Since $S_4$ is generated by the transpositions (12), (23), and (34), it suffices to prove that each of these is in the image of $\phi$.

Let $\rho_1$ be the $180^\circ$ rotation around the line joining the midpoint of $AB$ and the midpoint of $A'B'$. Then $\rho_1$ maps $AA'$ to $BB'$, $BB'$ to $AA'$, $CC'$ to $C'C'$, and $DD'$ to $D'D'$, so $\phi(\rho_1) = (12)$. Let $\rho_2$ be the $180^\circ$ rotation around the line joining the midpoint of $BC$ and the midpoint of $B'C'$. A calculation like the one above shows that $\phi(\rho_2) = (23)$. Let $\rho_3$ be the $180^\circ$ rotation around the line joining the midpoint of $CD$ and the midpoint of $C'D'$. A calculation like the one above shows that $\phi(\rho_3) = (34)$.

19.4.2) Now we prove that $\phi$ is injective. Suppose $\rho$ is in the kernel. Thus $\rho$ is a symmetry of cube that maps each diagonal to itself. Hence $\rho$ maps $A$ to either $A$ or $A'$, maps $A'$ to either $A$ or $A'$, maps $B$ to either $B$ or $B'$, and so on.

Suppose that $\rho(A) = A$. Then the segment $AB$ is mapped by $\rho$ to either $AB$ or $AB'$ (since $B$ is mapped to $B$ or $B'$), but $AB'$ has the wrong length, so $\rho$ must map $B$ to $B$. Similarly $\rho$ must fix each vertex adjacent to $A$. By the same argument, $\rho$ must fix the vertices adjacent to the vertices adjacent to $A$, and so on. Thus $\rho$ must fix all the vertices, so $\rho$ must be the identity.

By the same argument, if $\rho \in \ker \phi$ fixes any vertex, it must be the identity. The alternative is that $\rho$ maps each vertex to its opposite. The right-handed coordinate system formed by the vectors $\overrightarrow{AB}$, $\overrightarrow{AC}$, $\overrightarrow{AD}$ would then be mapped to $\overrightarrow{A'B'}$, $\overrightarrow{A'C'}$, $\overrightarrow{A'D'}$, which is left-handed. This is a contradiction, since rotations preserve orientation.

20.4.3) Suppose $x, y, z \in \mathbb{Q}$ and $x^2 + y^2 + z^2 = 8n + 7$. Let $d$ be the least common denominator of $x, y, z$. Multiplying both sides by $d^2$ gives an equation

$$a^2 + b^2 + c^2 = (8n + 7)d^2$$

where $a, b, c, d \in \mathbb{Z}$ are integers. Moreover, $\gcd(a, b, c, d) = 1$, since otherwise $d$ would not have been the least common denominator.

The $8n$ is a hint to reduce the equation modulo 8. Doing so and adding $d^2$ to both sides gives

$$a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{8}.$$  
Computing $x^2 \pmod{8}$ for $0 \leq x \leq 7$ shows that an integer square is 0, 1, or 4, modulo 8, with 1 occurring only if $x$ is odd. Checking possibilities shows that the only way to get 0 mod 8 as a sum of four numbers that are 0, 1, 4 modulo 8 is to use only the 0’s and 4’s (a quick
way to see this is to work first modulo 4). But then $a, b, c, d$ are all even, contradicting the fact that $\gcd(a, b, c, d) = 1$.

20.5.3) Expanding gives

$$q\bar{q} = (\alpha + \beta i + \gamma j + \delta k)(\alpha - \beta i - \gamma j - \delta k)$$

$$= \alpha^2 - \beta^2i^2 - \gamma^2j^2 - \delta^2k^2 - 2\alpha\beta(ij + ji) - \beta\delta(ik + ki) - \gamma\delta(jk + kj)$$

$$= \alpha^2 + \beta^2 + \gamma^2 + \delta^2,$$

since $i^2 = j^2 = k^2 = -1$ and $ij + ji = ik + ki = jk + kj = 0$.

20.7.2) According to Figure 20.1,

$$i(jl) = in = -o$$

$$(ij)l = kl = o.$$

1) First, $F$ is the splitting field of $(x^2 - 2)(x^2 - 3)$, so Galois theory applies to $F$. Let $\sigma \in G := \text{Gal}(F/Q)$. Then $\sigma$ acts as the identity on $Q$, since $\sigma(1) = 1$ and rational numbers can be built up from 1 using the operations $+, -, \cdot, /$, which are respected by $\sigma$.

Also $\sigma$ maps $\sqrt{2}$ to another zero of $x^2 - 2$, so $\sigma(\sqrt{2}) = \pm \sqrt{2}$. Similarly $\sigma(\sqrt{3}) = \pm \sqrt{3}$.

Hence we have a map

$$\phi: G \to \{\pm 1\} \times \{\pm 1\}$$

sending each automorphism $\sigma$ to the signs determining its action on $\sqrt{2}$ and $\sqrt{3}$.

The map $\phi$ is injective, since if the two signs are given, then $\sigma(\sqrt{6})$ is determined since it equals $\sigma \sqrt{2} \sigma \sqrt{3}$, and then $\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})$ is determined for all $a, b, c, d \in Q$.

On the other hand, by Galois theory, $\#G = [F : Q] = 4$, so there actually exist 4 automorphisms. Thus $\phi$ is a bijection. Explicitly, the automorphisms are

$$\sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

$$\sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

$$\sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

$$\sigma_4(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.$$ 

The group $G$ is of order 4, so it is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The first case can be ruled out, since a calculation shows that $\sigma_i^2$ is the identity for each $i$. Thus $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

In particular $G$ has five subgroups: the trivial subgroup, three subgroups of order 2, and $G$ itself.

Let us list subfields of $F$. Besides $Q$ and $F$, there are three subfields of degree 2, namely $Q(\sqrt{2})$, $Q(\sqrt{3})$, and $Q(\sqrt{6})$. These are different, since each contains a square root not belonging to the other two. (And these three fields are different from $Q$ and $F$, since they have degree 2.) Thus $F$ has at least five subfields.

But by Galois theory, the number of subfields of $F$ equals the number of subgroups of $G$, so $F$ has no more subfields than those already listed.

2) Let $P_0, P_1, \ldots, P_{n-1}$ be vertices of a regular $n$-gon, ordered counterclockwise. The dihedral group $D_{2n}$ is the group of symmetries of this $n$-gon. Let $O$ be the center of the $n$-gon. Let $\tau$ be the reflection in the line $OP_0$. Then $\tau$ maps each $P_i$ to $P_{i \mod n}$, so $\tau \in D_{2n}$. Let $\sigma$ be the counterclockwise rotation by an angle $2\pi/n$ around $O$. Then $\sigma$ maps $P_i$ to
\( p_{i+1} \mod n \), so \( \sigma \in D_{2n} \). Let \( \nu = \tau \sigma \). Then \( \nu \) maps \( p_i \) to \( p_{-\tau(i+1) \mod n} \), and \( \nu^2 \) maps \( p_i \) to \( p_{-\tau(i+1) \mod n} = p_i \), so \( \nu^2 = 1 \). Also \( \tau \nu = \tau \tau \sigma = \sigma \), so \( (\tau \nu)^n = \sigma^n = 1 \).

Thus if \( G := \langle a, b : a^2 = b^2 = (ab)^n = 1 \rangle \), there is a homomorphism \( \phi : G \to D_{2n} \) mapping \( a \) to \( \tau \) and \( b \) to \( \nu \). The image contains \( \tau \) and \( \nu \), and hence also \( \tau \nu = \sigma \), and we showed in class that \( \tau \) and \( \sigma \) generate \( D_{2n} \), so \( \phi \) is surjective.

To prove that \( \phi \) is an isomorphism, it will suffice to prove that \( \#G \leq 2n \). Every element of \( G \) is a word in \( a \) and \( b \), that is, a product of terms from \( \{a, b, a^{-1}, b^{-1}\} \). The relations \( a^2 = b^2 = 1 \) imply that \( a^{-1} = a \) and \( b^{-1} = b \). Any word containing two adjacent \( a \)'s or two adjacent \( b \)'s can be reduced using the relation \( a^2 = 1 \) or \( b^2 = 1 \), so every word is equivalent to one in which \( a \) and \( b \) alternate.

We next claim that every alternating word starting with \( b \) is equivalent to an alternating word starting with \( a \). Suppose we have a word \( w \) starting with \( b \) and containing \( m \) letters. Choose a positive multiple \( N \) of \( n \) such that \( 2N > m \). Then \( (ab)^N \) is a power of \( (ab)^n = 1 \), so \( (ab)^N = 1 \). The product \( (ab)^N \cdot w \) can be reduced by canceling terms in the middle, starting with the last \( b \) in \( (ab)^N \) and the first \( b \) in \( w \). Eventually all of \( w \) cancels with the last \( m \) letters in \( (ab)^N \), and what remains is a word equivalent to \( w \), and it is an initial segment of \( (ab)^N \) so it starts with \( a \).

Thus it remains to consider words starting with \( a \) in which \( a \) and \( b \) alternate. If such a word has \( 2n \) or more letters, we can cancel \( (ab)^n \) from its front, so it suffices to consider such words having \( < 2n \) letters. These are (starting with the empty word)

\[
\emptyset, a, ab, aba, abab, ababa, \ldots, (ab)^{n-1}a.
\]

There is one of these of each length between 0 and \( 2n - 1 \), so there are \( 2n \) such words. Thus \( \#G \leq 2n \). As explained earlier, this implies that the surjective homomorphism \( \phi : G \to D_{2n} \) must be an isomorphism.