1. (a) Suppose \( ap \neq 0 \) and \((ap)(bp) = 0\). Then \( pq \mid (ap)(bp)\). Since \( \gcd(p, q) = 1, q \mid ab \). Since \( q \) is prime, \( q \mid b \) and so \( bp = 0 \).

(b) It suffices to show that there is a unity. We need \( a \) such that \((ap)(bp) = bp \) modulo \( pq \) for every \( b \). This will happen if \((ap)p = p \) modulo \( pq \), which will happen if \( ap = 1 \) modulo \( q \), which has a solution since \( p \in U_q \).

(c) Every nonzero element of \( S \) is a zero divisor.

2. They are \( M = \{0, 3\} \) with \( \mathbb{Z}_6/M \cong \mathbb{Z}_2 \) via \( \varphi(3 + \mathbb{Z}_6) = 1 \), and \( M = \{0, 2, 4\} \) with \( \mathbb{Z}_6/M \cong \mathbb{Z}_3 \) via \( \varphi(4 + \mathbb{Z}_6) = 1 \).

3. Suppose \( a \) and \( b \) are in the union. Then there are \( j, k \) such that \( a \in I_j \) and \( b \in I_k \). Let \( n = \max(j, k) \). Then \( a, b \in I_n \), which is an ideal. Thus \( ra, a+b \) and \( a-b \) are all in \( I_n \) and hence the union.

4. (a) \( \omega = e^{2\pi i/5} \) is a zero of \( x^5 - 1 \) and the remaining zeroes are \( \omega^k \) for \( 0 \leq k < 5 \).

(b) You can cite the result from class: \( U_5 \). Alternatively, you can derive it: To specify an automorphism, it suffices to specify \( \varphi(\omega) \) and the possibilities are \( \varphi_k(\omega) = \omega^k \) where \( 0 < k < 5 \).

(c) If you computed the order of the group in (b), you receive full credit, regardless if (b) is correct.
   If you note that \( x^4 + x^3 + x^2 + x + 1 \) is irreducible without proof and give 4 as the answer, you’ll receive 4 points since you did not prove irreducibility.

5. (a) There are various ways to do this. One is to note that the intersection of subgroups is a subgroup and so \( E = E_1 \cap E_2 \) is a subgroup under addition and \( E^* = E_1^* \cap E_2^* \) is a subgroup under multiplication.

(b) Since \([E_1 : F] = [E_1 : E][E : F]\), it follows that \([E : F]\) must divide both 12 and 18. Thus \([E : F]\) must be a divisor of 6. The possibilities are 1, 2, 3, 6.

6. If the side of an equilateral triangle has length \( s \), it’s area is \( \frac{1}{2} \sqrt{3} s^2 \). The side of a square of the same area has length \( \sqrt{\frac{1}{2} \sqrt{3}} s \). Since \( \sqrt{\frac{1}{2} \sqrt{3}} \) is constructible, the answer is yes.

7. \( C_{k+1} \) can always detect up to \( k \) errors, but \( C_k \) is only guaranteed to detect up to \( k-1 \) errors. 
   (a) In addition, \( C_3 \) can always correct one error, but \( C_2 \) cannot.
   (b) Nothing additional.

8. We may write \( E = \mathbb{Q}(a) \) for some \( a \in E \). Suppose \( a \) is a zero of \( p(x) \in \mathbb{Q}[x] \). Let \( K \) be the splitting field of \( p(x) \) over \( \mathbb{Q} \). Since elements of \( \text{Gal}(K/\mathbb{Q}) \) permute the zeroes of \( p(x) \), \( \text{Gal}(K/\mathbb{Q}) \) is finite. Since there is a bijection between subgroups of \( \text{Gal}(K/\mathbb{Q}) \) and subfields of \( K \), \( K \) has only a finite number of subfields and hence so does \( E \) since \( E \subseteq K \).