1. Let $G$ be a group and $H$ be a subgroup.
   a) Prove that two left cosets $aH$ and $bH$ of $H$ in $G$ are either disjoint or equal.
   b) Give an example of a left coset $aH$ in some group $G$, which is not a right coset.

2. Let $p$ be a prime and $G$ be group of order $p^n$ for some positive integer $n$. Let
   $\varphi: G \rightarrow S_p$ be a homomorphism to the symmetric group $S_p$ with non-trivial image.
   Show that the kernel of $\varphi$ is order $p^{n-1}$. (Hint: What is the order of $S_p$?)

3. Let $\theta: \mathbb{Z} \rightarrow \mathbb{Z}_m$ be a ring homomorphism.
   a) Show that if $m$ is a prime, then $\theta$ is either surjective or $\theta(k) = [0]$ for all $k \in \mathbb{Z}$.
   b) Is this true also for higher prime powers $m = p^r$? (Hint: $\theta(1)^r = \theta(1)^r$.)

4. Let $p$ be a prime and $f(x) \in \mathbb{Z}_p[x]$ be a polynomial of degree $d \geq 1$.
   a) How many elements are there in $\mathbb{Z}_p[x]/(f(x))$?
   b) Show that $F = \mathbb{Z}_p[x]/(x^2 + 1)$ is a field.
   c) Let $\alpha$ be the class of $x$ in $F$. Find a multiplicative inverse of $\alpha^{2014} + 2015$ in $F$.

5. Formulate and prove the fundamental homomorphism theorem for groups.

6. Show that any finite integral domain is a field.

All claims that are made must be motivated.
Solutions to examination in algebra: MMG500 / MVE 150 2015-03-20

1a) If \( aH \) and \( bH \) have a common element \( ah_1 = bh_2 \) and \( h \in H \), then \( ah = b(h_2h_1^{-1})h \in bH \) and \( bh = a(h_1h_2^{-1})h \in bH \). Hence \( aH \subseteq bH \) and \( bH \subseteq aH \) whenever \( aH \cap bH \neq \emptyset \).

1b) One may e.g. choose \( G = S_3 \) and \( H = \{(12)\} \). Then \( Ha = aH \) for \( a = (123) \). Indeed, \( (12)(123) = (23) \) while \( (23)(12) = (13) \). So \( Ha = \{(123),(23)\} \) while \( aH = \{(123),(13)\} \).

2. Let \( K = \ker \varphi \) and \( H = \text{im } \varphi \). Then \( G/K \cong H \) by the fundamental homomorphism theorem. So \( o(H) = o(H) = o(K) = o(G) \). Further, \( o(H) | o(S_p) \) by Lagrange's theorem. Hence \( o(H) \) divides \( \text{GCD}(o(G), o(S_p)) = (p^n, p!) = p \). But then \( o(H) = p \) as \( o(H) 
eq 1 \). So \( o(K) = o(G)/o(H) = p^{n-1} \).

3a) Let \( \theta : Z \rightarrow Z_p \) be a homomorphism of rings. Then \( \theta \) is additive and \( \theta (Z) \) an additive subgroup of \( Z_p \). Hence \( \theta (Z) = Z_p \) or \( \theta (Z) = \{0\} \) by a corollary of Lagrange's theorem.

3b) If \( \theta : Z \rightarrow Z_m \) be a ring homomorphism, then \( \theta (1)^2 = \theta (1 \cdot 1) = \theta (1) \). So if \( \theta (1) = [k]_m \), then \( m | k^2 - k = (k-1)k \). If now \( p \) is a prime, then \( p | (k-1) \) and \( p | k \) cannot both be true. Hence if \( m = p^r \), then \( p | (k-1) \) or \( p | k \). That is, \( \theta (1) = [1]_m \) or \( \theta (1) = [0]_m \). As \( \theta \) is additive, we have thus that either \( \theta (l) = [l]_m \) for all \( l \in Z \) or \( \theta (l) = [0]_m \) for all \( l \in Z \).

4a) It follows from the division algorithm that any coset has a unique representative of the form \( a_0 + a_1x^1 + \ldots + a_n x^n \in Z_p[x] \). There are thus \( p^n \) classes in \( Z_p[x]/(f(x)) \).

4b) It suffices by a theorem in Durbin's book to show that \( x^2 + 1 \) is an irreducible polynomial in \( Z_3[x] \). If \( x^2 + 1 \) were reducible then it would have a linear factor and a zero in \( Z_3 \). But there is no such zero as the squares in \( Z_3 \) are either \( [0] \) or \( [1] \). Hence \( x^2 + 1 \) is irreducible in \( Z_3[x] \).

4c) As \( x^2 + 1 = 0 \) in \( F = Z_3[x]/(x^2 + 1) \), we conclude that \( \alpha^{2014} = (\alpha^2)^{1007} = (-1)^{1007} = -1 \). Also, \( 2015 = 2 \) in \( Z_3 \subseteq F \). Hence \( \alpha^{2014 + 2015} = 1 \) in \( F \), the multiplicative inverse is thus \( 1 \).

5) See Durbin's book.

6) See Durbin's book.