1. (i) For an odd prime $p$, use Galois theory to prove that $Q(\zeta_p)$ contains a unique quadratic subfield $K$, and use considerations with discriminants to prove that $\text{disc}(\mathcal{O}_K/Z) = \pm p$. Conclude that $K = Q(\sqrt{-1|p|p})$, where $(-1|p) = (-1)^{(p-1)/2}$ is the Legendre symbol.

(ii) Use discriminants to determine all three quadratic subfields of $Q(\zeta_3)$.

(iii) Let $p$ and $q$ be distinct positive odd primes, and let $\phi_q \in \text{Gal}(Q(\zeta_p)/Q) = (Z/pZ)^\times$ be the residue class of $q$ mod $p$. Prove that $\phi_q$ preserves all primes $\mathcal{O}$ of $Z[\zeta_p]$ over $q$, and hence $\phi_q|\mathcal{O}$ preserves the primes of $\mathcal{O}_K$ over $q$ for $K$ as in (i). By studying Galois-actions on finite residue fields and on primes over $qZ$ in $\mathcal{O}_K$, prove that $\phi_q$ has trivial image in $\text{Gal}(K/Q)$ if and only if $qZ$ is split in $\mathcal{O}_K$. (Hint: check that $\phi_q$ induces the $q$th-power automorphism on $Z[\zeta_p]/\mathcal{O}$ for every prime $\mathcal{O}$ over $qZ$, and so $\phi_q|\mathcal{O}$ does the same on $\mathcal{O}_K/q$ for all $q$ over $qZ$ in $\mathcal{O}_K$.) Also prove that $\phi_q|\mathcal{O} = 1$ if and only if $q$ is a square modulo $pZ$. Deduce quadratic reciprocity for odd primes; where does your argument use that $p$ and $q$ are positive?

(iv) Modify the method in (iii) by means of (ii) to prove the Legendre-symbol formula $(2|p) = (-1)^{(p^2-1)/8}$.  

2. (i) Compute the discriminant for $Q(\zeta_n)/Q$ (that is, compute $\text{disc}(Z[\zeta_n]/Z)$).

(ii) Choose an integer $n \geq 2$, and show that $K = Q(\zeta_n)$ is a CM field with maximal totally real subfield $K^+ = Q(\zeta_n + \zeta_n^{-1})$. Use your knowledge of $\mathcal{O}_K$ to prove $\mathcal{O}_{K^+} = Z[\zeta_n + \zeta_n^{-1}]$. (Hint: $[K^+ : Q] = [K : Q]/2$.)

(iii) For $p = 31$, explain why $Q(\zeta_p)$ contains a unique subfield $L$ of degree 6 over $Q$, and by studying the action of $\text{Gal}(Q(\zeta_p)/Q) = (Z/pZ)^\times$ on $\zeta_p$, prove that the prime $2Z$ is totally split in $\mathcal{O}_L$. (Hint: it suffices to prove triviality of a certain extension of finite residue fields, and note that $2^{p(p)/6} \equiv 1 \mod p$ for $p = 31$.) Use the fact that $F_2[X]$ does not contain 6 distinct monic linear polynomials to infer that $\mathcal{O}_L$ is not monogenic over $Z$ (that is, $\mathcal{O}_L \neq Z[\alpha]$ for all $\alpha \in \mathcal{O}_L$).

3. Let $A$ be a Dedekind domain whose residue fields at all maximal ideals are finite, and let $F$ be the fraction field of $A$. The Dedekind domain of most interest in number theory have this property.

(i) Prove that if $F'/F$ is a finite separable extension and $A'$ is the integral closure of $A$ in $F'$ then $A'$ has finite residue fields at all maximal ideals. Also prove that this finiteness property is inherited by all localizations $S^{-1}A$ that are Dedekind (that is, $S^{-1}A \neq F$).

(ii) Let $m$ be a maximal ideal of $A$ and let $M = mA_m$. Recall from class that the natural map $A/m^e \to A_m/m^e$ is an isomorphism carrying $m^i/m^e$ over onto $M^i/M^e$ for $0 \leq i \leq e$. Deduce from the fact that $A_m$ is a discrete valuation ring with residue field $A/m$ that $A/m^e$ is finite with size $|A/m^e|$.

(iii) Use the Chinese Remainder Theorem to conclude that if $I \subseteq A$ is a nonzero ideal then the quotient ring $A/I$ is finite. We write $N(I)$ to denote its cardinality, and this is called the absolute norm of $I$.

(iii) Prove that $N(IJ) = N(I)N(J)$ for any two nonzero ideals $I$ and $J$ of $A$, and in the setup of (i) prove that $N(I'A') = N(I)[F'^e:F]$ for any nonzero ideal $I$ of $A'$. In the special case that $A = Z$ and $A' = \mathcal{O}_K$ for a number field $K$, prove $N(I) = [N_K/Q(I)]$ for all nonzero ideals $I$ of $A'$ (hint: reduce to the case when $K/Q$ is Galois). Prove an analogous relationship between absolute norm and ring-theoretic norm in the case when $A = k[X]$ for a finite field $k$ and $A'$ is its integral closure in a finite separable extension of $F = \text{Frac}(A)$.

4. Let $A$ be a Dedekind domain with fraction field $F$, and let $A_0 \subseteq A$ be a subring with fraction field $F$ such that $A$ is a finitely generated $A_0$-module. We call such an $A_0$ an order in $A$. The purpose of this exercise and the next one is to define the concept of class group for orders and to relate them to the class group of $A$.

(i) Explain why the above definition of “order” recovers our earlier notion of order (as a subring with finite lattice-index) in the case when $A$ is the ring of integers of a number field, and in general prove that all nonzero prime ideals of $A_0$ are maximal and that $A$ is the integral closure of $A_0$ in $F$ (so $A$ is intrinsic to $A_0$). Construct a nonzero $a \in A$ such that $aA \subseteq A_0$, so $A_0[1/a] = A[1/a]$, and define the conductor of $A_0$ to be $c = c_{A/A_0} = \{a \in A \mid aA \subseteq A_0\}$, so $c \neq 0$. Show that $c$ is an ideal of $A$ that is contained in $A_0$ (so it has the peculiar property of being an ideal in both $A_0$ and $A$), and show that all ideals of $A$ contained in $A_0$ are in fact contained in $c$ (so $c_{A/A_0} = A$).
if and only if \( A_0 = A \)). If \( \mathcal{O} \) is the order of index \( f \) in the ring of integers \( \mathcal{O}_K \) of a quadratic field \( K \), prove that \( \mathcal{O}_K \mathcal{O} = f \mathcal{O}_K \).

(ii) Let \( S \) be a multiplicative set of \( A_0 \) that is disjoint from some maximal ideal of \( A_0 \) (that is, \( S^{-1}A_0 \neq F \)), so \( S^{-1}A \) is the integral closure of \( S^{-1}A_0 \) and is a finitely generated \( S^{-1}A_0 \)-module (so \( S^{-1}A \) is Dedekind). Show that \( S^{-1}\epsilon_{A/A_0} = \epsilon_{S^{-1}A/S^{-1}A_0} \), as ideals of \( S^{-1}A \) (or of \( S^{-1}A_0 \)).

(iii) Prove that \( \overline{A}_0 = A_0/c \) is a subring of \( \overline{A} = A/c \) such that \( \overline{A}_0 \) is a finitely generated \( \overline{A} \)-module and such that no nonzero principal ideals of \( \overline{A} \) lie in \( \overline{A}_0 \) and \( A_0 \) is the preimage of \( \overline{A} \) under the projection \( A \to \overline{A} \). Show that this observation is “universal” in the sense that for any nonzero ideal \( I \) of \( A \) and any subring \( \overline{A} \) of \( A/I \) such that \( \overline{A} \) does not contain nonzero principal ideals of \( A/I \) and such that \( A/I \) is finitely generated as an \( \overline{A} \)-module, the preimage \( R \) of \( \overline{R} \) in \( A \) is an order of \( A \) with conductor equal to \( I \). In this sense, all orders can be “described” by ring-theoretic congruence conditions. Deduce in particular that \( A_0^c = A_0 \cap A^c \), and that if \( A \) has finite residue fields at all maximal ideals then for any nonzero ideal \( I \) of \( A \) there exist only \textit{finitely many} orders \( A_0 \) of \( A \) such that \( \epsilon_{A/A_0}I \).

5. A nonzero ideal \( I \) in a noetherian domain \( R \) is \textit{invertible} if \( I_m = IR_m \) is principal for all maximal ideals \( m \) of \( R \), and a \textit{fractional ideal} of \( R \) is an \( R \)-submodule \( \mathcal{I} \) of \( K = \text{Frac}(R) \) having the form \( cI \) for \( c \in K^\times \) and \( I \) an ordinary ideal of \( R \). Two fractional ideals \( I \) and \( I' \) of \( R \) are \textit{linearly equivalent} if \( I = cI' \) for some \( c \in K^\times \).

(i) Prove that if \( \mathcal{I} \) is a nonzero fractional ideal of \( R \) then \( \mathcal{I}' = \{ x \in K \mid x \mathcal{I} \subseteq R \} \) is also a nonzero fractional ideal of \( R \). We say that \( \mathcal{I} \) is \textit{invertible} if \( \mathcal{I} \mathcal{I}' = R \); prove that this condition is unaffected by linear equivalence and that it recovers the initial notion of invertibility when \( \mathcal{I} \) is an ordinary ideal of \( R \).

(ii) Prove that if \( \mathcal{I}_1 \) and \( \mathcal{I}_2 \) are invertible fractional ideals of \( R \) then so is \( \mathcal{I}_1 \mathcal{I}_2 \), and that in fact \( \mathcal{I}_1 \otimes_R \mathcal{I}_2 \) is a torsion-free \( R \)-module such that the natural map \( \mathcal{I}_1 \otimes_R \mathcal{I}_2 \to \mathcal{I}_1 \mathcal{I}_2 \) is an isomorphism. Explain how the set \( \text{Pic}(R) \) of linear equivalence classes of invertible fractional ideals of \( R \) forms an abelian group via tensor products and dualization (over \( R \)). This is the \textit{class group} of \( R \).

(iii) In the special case when \( R = A_0 \) is an order in a Dedekind domain \( A \), use weak approximation for \( A \) to prove that every invertible fractional ideal of \( A_0 \) is linearly equivalent to an invertible ordinary ideal \( I_0 \) of \( A_0 \) that is coprime to \( \epsilon_{A/A_0} \) in the sense that \( I_0 + \epsilon_{A/A_0} = A_0 \).

(iv) Prove that \( I_0 \mapsto I_0A \) and \( I \mapsto I \cap A_0 \) are inverse bijections between the set of invertible ordinary ideals of \( A_0 \) coprime to \( \epsilon = \epsilon_{A/A_0} \) and invertible ordinary ideals of \( A \) coprime to \( \epsilon \), and that these bijections are compatible with formation of products of such ideals. (Hint: Use gluing of ideals and (ii) to reduce to the case when \( A_0 \) is local and \( A \) is semi-local, so \( A \) is a PID whose maximal ideals all contain \( \epsilon \) if \( A_0 \neq A \). Deduce that if \( m_0 \) is a maximal ideal of \( A_0 \) then the following are equivalent: \( m_0 \) is coprime to \( \epsilon \), \( m_0 \) is invertible, and \( (A_0)_{m_0} \) is integrally closed (and hence is a discrete valuation ring).

(v) Use the bijection with ideals of \( A \), in conjunction with (iii), to define an exact sequence of abelian groups

\[ 1 \to A^\times /A_0^\times \to (A/\epsilon)^\times / (A_0/\epsilon)^\times \to \text{Pic}(A_0) \to \text{Pic}(A) \to 1, \]

and deduce that if all residue fields of \( A \) are \textit{finite} and \( \text{Pic}(A) \) is finite then \( \text{Pic}(A_0) \) is finite for every order \( A_0 \) of \( A \).