1. Let $A$ be Dedekind with fraction field $F$, $F''/F'/F$ a tower of finite separable extensions, and $A' \subseteq F'$ and $A'' \subseteq F''$ the integral closures of $A$ (so $A''$ is also the integral closure of $A'$ in $F''$).

(i) Let $p''$ be a maximal ideal of $A''$, lying over $p' \subseteq A'$ and $p \subseteq A$. Use prime factorization of nonzero ideals to prove that $e(p'') = e(p')d(p''/p)$, and also prove that $f(p'') = f(p')d(p''/p)$.

(ii) Show $p''$ is unramified over $p$ if and only if $p''$ is unramified over $p'$ and $p'$ is unramified over $p$. Prove $p$ is totally split in $F''$ if and only if it is totally split in $F'$ and each prime of $F''$ over $p$ is totally split in $F''$.

(iii) Assume that $F''/F$ and $F'/F$ are Galois extensions of number fields, with $A$, $A'$, and $A''$ the corresponding rings of integers. Prove that the quotient map $\text{Gal}(F''/F) \to \text{Gal}(F'/F)$ carries $D(p''/p)$ onto $D(p'/p)$ and $I(p''/p)$ into $I(p'/p)$ (finer methods show this is also onto), and that if $p$ is unramified in $F''$ then it carries $F_r(p''/p)$ to $F_r(p'/p)$. In the unramified case, also prove that $F_r(p''/p') = F_r(p''/p)F_r(p'/p)$. As an application, read the beautiful "algebraic number theory" proof of quadratic reciprocity in §6.5.

2. Fix a Galois extension $K'/K$ of number fields generated by a root of a monic irreducible $f \in K[X]$.

(i) For a maximal ideal $p$ of $\mathfrak{O}_K$ such that $f \in \mathfrak{O}_{K,p}[X]$ (holds for all but finitely many $p$), if $f \bmod p$ is irreducible over $\mathfrak{O}_{K,p}/p\mathfrak{O}_{K,p} = \mathfrak{O}_K/p$ then $p' := p\mathfrak{O}_{K'}$ is prime and $\text{Gal}(K'/K) = D(p'p)$ (cyclic). (Hint: Let $A$ be a DVR (e.g., $\mathfrak{O}_{K,p}$) with maximal ideal $m = F(\mathfrak{A})$, $f \in A[X]$ monic that is irreducible and separable over $F$, and $A'$ the integral closure of $A$ in $F' := F[X]/(f)$, so $A'$ is a finite free $A$-module ($A$ is a PID). Assume $f \bmod m$ is irreducible over $A/m$. Prove $j : A[X]/(f) \to A'$ is an injection between finite free $A$-modules of the same rank, and via ring-theoretic reasons prove $j \bmod m$ is injective! Deducce "det($j$) $\in A'$" (using $A$-bases), so $j$ is an isomorphism. Conclude that $A'/mA'$ is a field, so $mA'$ is prime.)

(ii) If $\text{Gal}(K'/K)$ is not cyclic, show that $f \bmod p$ must be reducible over $\mathfrak{O}_K/p$ for all but finitely many $p$.

Find an irreducible quartic $f \in \mathbb{Z}[X]$ that is reducible modulo $p$ for all but finitely many $p$!

3. For $p = 31$, prove $Q(\zeta_p)$ contains a unique subfield $L$ with $[L : Q] = 6$ and via the action of $\text{Gal}(Q(\zeta_p)/Q)$ is totally split in $\mathfrak{O}_L$. (Hint: it suffices to prove triviality of Frobenius at $2$ for $L/Q$; use Exercise 1(iii) and note that $2^k(2^6) = 1 \bmod p$ for $p = 31$.) Show that $F_2[\sqrt{2}, Y]$ has fewer than $6$ distinct maps to $F_2$ and deduce that $\mathfrak{O}_L$ requires at least three generators over $\mathbb{Z}$ (that is, $\mathfrak{O}_L \neq \mathbb{Z}[\alpha, \beta]$ for all $\alpha, \beta \in \mathfrak{O}_L$). Do not try to explicitly compute prime ideals (or $\mathfrak{O}_L$)!

4. Let $K = Q(\zeta_{23})$. The following shows $\mathbb{Z}[[\zeta_{23}]]$ is not a PID; $n = 23$ is minimal for this property.

(i) Prove that $47Z$ splits completely in $\mathbb{Z}[[\zeta_{23}]]$, and that $Q(\sqrt{-23})$ is the unique quadratic subfield of $K$.

(ii) Assume $\mathbb{Z}[[\zeta_{23}]]$ is a PID, and let $x \in \mathbb{Z}[[\zeta_{23}]]$ generate a prime over $47Z$. Let $y = N_{K/Q}(\sqrt{-23})(x)$. Prove $y \in Z\{1 + \sqrt{-23}\}/2$ must have norm $47$ in $\mathbb{Z}$, but show no $z \in \mathbb{Z}\{1 + \sqrt{-23}\}/2$ has norm $47$!

5. Let $K = Q(\sqrt{5}, \sqrt{-1})$. Prove any $p \neq 2, 5$ is unramified in $K$. Use quadratic reciprocity and Exercise 1(iii) to find $F_p \in \text{Gal}(K/Q)$ depending on $p \bmod 20$. Prove $\text{Gal}(K/Q)$ is the decomposition group at $2$ (i.e., $g_2 = 1$), $Gal(K/Q(i))/Q(\sqrt{-23})$ is the decomposition group at $5$, and find the inertia subgroup in each.

6. Let $K = Q(\alpha, i)$ with $\alpha^2 = 3$ and $i^2 = -1$, so $G := \text{Gal}(K/Q) \simeq D_4$ with generators $s$ and $t$ satisfying $s(\alpha) = i\alpha, s(i) = i, \ t(\alpha) = \alpha, t(i) = -i$ (so $s^2 = t^2 = 1$ and $tst^{-1} = s^{-1}$). Write $e_p, f_p, g_p$ for the invariants attached to a prime $p$ relative to $K/Q$. (You do not need to compute any rings of integers below!)

(i) Using Exercise 1(i) applied to $K/Q(i)/Q$, $\mathfrak{O}_K/Q(i)/Q$, show that $e_3 = 4$ and $f_3 = 2$, so $g_3 = 1$. Deduce that the unique prime over $3$ is $p := \alpha\mathfrak{O}_K$, and that $D(p[3\mathbb{Z}]) = G$. Prove $I(p[3\mathbb{Z}]) = \langle s \rangle$.

(ii) Check that $T^4 - 3$ is irreducible over $F_5$, and use the tower $K'/Q(i)/Q$ to show $4|f_5$. Using $K/Q(i)/Q$, show $2|g_5$, and conclude that $e_5 = 1, f_5 = 4$, and $g_5 = 1$. Hence, there are exactly two primes $q$ and $q'$ of $\mathfrak{O}_K$ over $5Z$, labelled with $q$ over $(1 + 2i)Z[i]$ and $q'$ over $(1 - 2i)Z[i]$. Explain why $Fr(q)(1 + 2i)Z[i]$ $= Fr(q)(5Z)$, and prove $q = (1 + 2i)\mathfrak{O}_K$ and $q' = (1 - 2i)\mathfrak{O}_K$.

(iii) Since $5$ splits in $Q(i)$, prove $D(q[5\mathbb{Z}]) = D(q'[5\mathbb{Z}]) = Gal(K/Q(i))/Q$ = $\langle s \rangle$. Since $Fr(q[5\mathbb{Z}])$ and $Fr(q'[5\mathbb{Z}])$ generate this group, each is $s$ or $s^3$. Figure out which is which. (Hint: $\alpha \notin q, q'$, and $F_5 \simeq Z[i]/(1 + 2i)$ identifies $i$ with $\pm 2 \bmod 5$!) Explain why this is consistent with the fact that $t$ swaps $q$ and $q'$.

(iv) Prove that $7$ is unramified in $K$ with $2|f_7$ using $K/Q(\alpha)/Q$. Prove that the only nontrivial $\sigma \in G$ which can satisfy $\sigma(\alpha) = x^2 \bmod 3\mathbb{F}_3$ for a prime $\mathfrak{P}$ of $\mathfrak{O}_K$ over $2$ are the elements $st$ and $s^2t$ with order $2$! (Hint: consider $x = x$ and $x = i$). Deduce that $f_7 = 2, g_7 = 4$, and $7\mathbb{Z}[i]$ is totally split in $\mathfrak{O}_K$.