Note: Unless otherwise stated, $K$ and $F$ are fields of characteristic 0.

12. (Continuation of Problem 8): a) If $K/\mathbb{Q}$ is a quadratic extension, then $K = \mathbb{Q}(\sqrt{d})$ for a unique square-free integer $d$.

b) If $d \equiv 2, 3 \mod 4$, let $D = 4d$, otherwise let $D = d$. Show that the discriminant of $K$ is $D$.

c) Show that if $K/\mathbb{Q}$ is a quadratic field, then $|\text{disc}_K| > 1$. [Remark: Later we will see that if $K/\mathbb{Q}$ has degree $n > 1$, then $|\text{disc}_K| > 1$. The latter was conjectured by Kronecker in 1881 and proved by Minkowski in 1890.]

13. Suppose $R$ is a commutative ring with unit, and $z_1, \ldots, z_n \in R$. Show that the Vandermonde matrix

$$V(z_1, \ldots, z_n) := (z_i^{j-1})_{1 \leq i, j \leq n}$$

has determinant

$$\det V(z_1, \ldots, z_n) = \prod_{1 \leq i < j \leq n} (z_i - z_j).$$

14. [“Existence of primitive element”] Let $F$ be a field of characteristic 0. Let $K/F$ be a finite extension. Show that there exists $\theta \in K$ such that $K = F(\theta)$.

[Hint: here is one way you could proceed; you may use the fact that there are $n = [K : F]$ distinct embeddings of $K$ into $\overline{F}$, where $F$ is an algebraically closed field $F$ containing $F$. Call these $\sigma_i$, $1 \leq i \leq n$. For $i \neq j$, consider the subset $V_{ij} := \{\alpha \in K \mid \sigma_i(\alpha) = \sigma_j(\alpha)\}$. Use linear algebra and the fact that $K$ is infinite to prove that the union of the $V_{ij}$ ($i \neq j$ of course!) is not all of $K$.]

15. Suppose $F$ is a characteristic 0 field, $A$ is a subring of $F$ which is integrally closed in $F$ and $K/F$ is a finite extension of degree $n$. Let $B$ be the integral closure of $A$ in $B$. Suppose we have $n$ elements

Check the website for the due date.
\[ \eta_1, \ldots, \eta_n \text{ belonging to } B \text{ which form a basis for } K/F \text{ and put } d = \text{disc}_{K/F}(\eta_1, \ldots, \eta_n). \text{ Recall we have proved in class that } d \neq 0. \]

(a) Show that \( dB \subseteq [\eta_1, \ldots, \eta_n]_A. \)

(b) Show that if \( F = \mathbb{Q} \) and \( A = \mathbb{Z} \) so that \( B = \mathcal{O}_K \), for every \( \alpha \in \mathcal{O}_K \), there exists \((c_1, \ldots, c_n) \in \mathbb{Z}^n \) satisfying \( d|c_j^2 \) \((j = 1, \ldots, n)\) such that

\[ \alpha = c_1\eta_1 + \cdots + c_n\eta_n. \]

[Hint: Given \( \xi \in B \), write \( \xi = \sum_{j=1}^n x_j\eta_j \) with \( x_1, \ldots, x_n \in F \). Now consider the linear system (for \( i = 1, \ldots, n \))

\[ \text{Tr}_{K/F}(\alpha\eta_i) = \sum_{j=1}^n \text{Tr}_{K/F}(\eta_i\eta_j)x_j. \]

Now use the fact that the left hand side is in \( A \) together with Cramer’s Rule ! (I bet you never thought you’d use Cramer’s Rule in a graduate course; those of you who took algebraic groups might already appreciate the wonders of this undervalued result).

16. Let \( K, F, A, B \) be as in 15) but assume in addition that \( A \) is a PID. Suppose \( M \) is a non-zero finitely generated \( B \)-submodule of \( K \). Show that \( M \) is a free \( A \)-module of rank \([K : F]\).

Hint: we essentially proved this in class for \( M = B \). The strategy is basically the same, though you might use 15) instead of the dual basis approach we used in class.

17. Suppose \( K = F(\theta) \) where \( f(x) = \text{Irr}_\theta(x; F) \) has degree \( n \). Show that

\[ \text{disc}_{K/F}(1, \theta, \ldots, \theta^{n-1}) = (-1)^{n(n-1)/2}N_{K/F}(f'(\theta)). \]

18. Use 17) to prove the (should-be) well-known formula for the discriminant of the trinomial \( f(x) = x^n + ax + b \):

\[ \text{disc}(x^n + ax + b) = (-1)^{n(n-1)/2} \left( n^n b^{n-1} + (-1)^{n-1} (n - 1)^{n-1} a^n \right). \]

19. Let \( K = \mathbb{Q}(\theta) \) where \( \theta^3 = 2 \). Show that \([1, \theta, \theta^2]_\mathbb{Z} = \mathcal{O}_K\). Use this to calculate \( \text{disc}_K \).

20. Let \( K = \mathbb{Q}(\theta) \) where \( \theta^3 = \theta + 4 \). [check that \( f(x) = x^3 - x - 4 \) is irreducible. Show that \([1, \theta, (\theta + \theta^2)/2]_\mathbb{Z} = \mathcal{O}_K\). Use this to calculate
disc$_K$. What is disc$_K$/disc$_f$? Does this agree with the relationship between the power basis $[1, \theta, \theta^2]$ and the integral basis you found?

21. Suppose $A$ is a subring of an integral domain $B$ and that $B$ is integral over $A$, i.e. every element of $B$ satisfies a monic polynomial with coefficients in $A$. Show that $A$ is a field if and only if $B$ is.

22. Let $A$ be a domain. Show that if $A$ is integrally closed (in its fraction field) then so is the polynomial ring $A[x]$.

23. In the polynomial ring $A = \mathbb{Q}[x, y]$, let $p$ be the principal ideal $p = (y^2 - x^3)$. Show that $p$ is a prime ideal but $A/p$ is not integrally closed. [Remark. The existence of such a prime ideal is related to the geometric fact that the curve $y^2 - x^3 = 0$ has a singularity at $(0, 0)$, i.e. both partials of $y^2 - x^3$ at that point vanish. To learn more about this mysterious remark, you should take algebraic geometry next term with Tom Weston.]

24. (a) Prove that a finite integral domain is always a field.
(b) Prove that a PID is always integrally closed.

25. Consider a degree $n$ polynomial $f \in \mathbb{Z}[x]$ which is monic and irreducible. Let $\theta$ be a root of $f$.

(a) Suppose $f'(r) = 0$ for some $r \in \mathbb{Z}$. Prove that $f(r)$ divides disc$(1, \theta, \ldots, \theta^{n-1})$. [Hint: what could Gauss tell you about $f(x)/(x - r)$?]

(b) If $f'(r) = 0$ for some $r \in \mathbb{Q}$ (as opposed to $r \in \mathbb{Z}$), could you say anything about disc$(1, \theta, \ldots, \theta^{n-1})$?

(c) Suppose there exist $g, h \in \mathbb{Z}[x]$ such that $g, h$ both split completely into linear factors over $\mathbb{Q}$ and such that

$$g(x)f'(x) = h(x) + f(x)e(x)$$

for some polynomial $e \in \mathbb{Z}[x]$. Describe a simple procedure for calculating disc$(1, \theta, \ldots, \theta^{n-1})$.

26. Prove the irreducibility criterion of Eisenstein: Let $R$ be a PID with field of fractions $F$, $p$ a prime element of $R$, and suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$ satisfies: i) $p|a_i$ for $0 \leq i \leq n-1$, and ii) $p^2 \not| a_0$. Then $f$ is irreducible over $F$.

27. Suppose $p$ is an odd prime number. Let $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$ be the $p$-cyclotomic polynomial.
(a) Show that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$. [Hint: hit $\Phi_p(x + 1)$ with Eisenstein; why is this enough?]

(b) Let $K = \mathbb{Q}[x]/(\Phi_p(x))$; it is a number field of degree $p - 1$ by (a). Let $\omega = x + (\Phi_p(x))$ be a root in $K$ of $\Phi_p(x)$. Compute $\text{disc}(\Phi_p(x)) = \text{disc}(1, \omega, \ldots, \omega^{p-2})$. [Hint: Use 17; for calculating $\Phi'_p(x)$, use the fact that $\Phi_p(x)(x - 1) = x^p - 1$; to compute $NK/\mathbb{Q}(\omega - 1)$, ask yourself if there is an easy way to compute the constant coefficient of the minimal polynomial of $\omega - 1$ (or of $1 - \omega$ if you prefer).]

(c) Show that $\mathbb{Z}[\omega] = \mathbb{Z}[1 - \omega]$ and
\[
\text{disc}(1, \omega, \ldots, \omega^{p-2}) = \text{disc}(1, 1 - \omega, \ldots, (1 - \omega)^{p-2}).
\]

(d) Show that
\[
\prod_{k=1}^{p-1}(1 - \omega^k) = p.
\]

(e) Show that $\mathcal{O}_K = \mathbb{Z}[\omega]$; thus $\mathcal{O}_K$ admits a power basis even though its discriminant is far from being square-free. [Hint: Suppose not; then there exists $\alpha \in \mathcal{O}_K$ which is not in $\mathbb{Z}[1 - \omega]$. Use (d) and 15 to obtain a contradiction.]

28\footnote{I should probably be giving more of a hint for this problem, or I could just put this footnote alerting you to the fact that this is a “starred” problem.} Let $K$ be a number field with signature $(r_1, r_2)$. What this means is that if $\sigma_1, \ldots, \sigma_n$ are the $n = [K : \mathbb{Q}]$ embeddings of $K$ into $\mathbb{C}$, then $r_1$ of them have image contained in $\mathbb{R}$ and $2r_2 = n - r_1$ of them do not. Let $\text{disc}_K$ be the discriminant of $K$, i.e. $\text{disc}_K(\omega_1, \ldots, \omega_n)$ where $\omega_1, \ldots, \omega_n$ is some integral basis for $K/\mathbb{Q}$, i.e. for $\mathcal{O}_K/\mathbb{Z}$.

a) Show that the sign of $\text{disc}_K$ is $(-1)^{r_2}$.

b) Prove Stickelberger’s Theorem: $\text{disc}_K \equiv 0, 1 \mod 4$.

[If you get tired of butting heads with Herr Dr Professor Stickelberger, you might consult your favorite book in algebraic number theory for a hint; or try Googling him! Be sure to quote your sources!]