MATH 797AP ASYMPTOTIC FAMILIES
NUMBER FIELDS HOMEWORK PROBLEMS

FARSHID HAJIR

FEBRUARY 26, 2014 – 11 : 09

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

1. A polynomial $f(x) \in \mathbb{Z}[x]$ is *primitive* if the greatest common divisor of its coefficients is 1. Prove *Gauss's Lemma*: If $f(x), g(x) \in \mathbb{Z}[x]$ are primitive, then $f(x)g(x)$ is primitive.

[Hint: Fill in all the details for the following idea: Write $f(x) = \sum_{i=0}^{n} a_i x^{n-i}$ and $g(x) = \sum_{j=0}^{m} b_j x^{m-j}$. Suppose p is a prime and i, j are the smallest indices satisfying $p \not| a_i$ and $p \not| b_j$. Consider the coefficient x^{i+j} in $f(x)g(x)$.]

2. Recall that if K is a field containing $\mathbb{Q}$, an element $\alpha \in K$ is called an *algebraic number* if and only if there exists $g(x) \in \mathbb{Q}[x]$ such that $g(\alpha) = 0$. If α is an algebraic number, we let $\mathrm{Irr}_\alpha(x; \mathbb{Q}) = \mathrm{Irr}_\alpha(x)$ be the monic polynomial in $\mathbb{Q}[x]$ of least degree having α as a root. An algebraic number α is called an *algebraic integer* if there exists a **monic** polynomial in $\mathbb{Z}[x]$ having α as a root.

(a) Use Gauss' Lemma to prove that if α is an algebraic integer, then $\mathrm{Irr}_\alpha(x) \in \mathbb{Z}[x]$.

(b) Prove that an algebraic number α is an algebraic integer if and only if $\mathrm{Irr}_\alpha(x) \in \mathbb{Z}[x]$.

3. (a) Suppose all roots in $\mathbb{C}$ of a monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$$

have absolute value 1. Show that $|a_r| \leq \binom{n}{r}$ for $0 \leq r \leq n-1$.

(b) Show that for a fixed positive integer n, there are only finitely many algebraic integers of degree n whose minimal polynomial has all of its roots in $\mathbb{C}$ on the unit circle. [Hint: think about Problem 2.]

(c) Show that if the minimal polynomial of an algebraic integer α has all its roots on the unit circle, then $\alpha^k = 1$ for some integer k. This is a famous theorem of Leopold Kronecker. [Hint: can the sequence of powers of α be non-repeating?]

4. Let $\alpha = \sqrt{5} + \sqrt{13}$. Show that α is an algebraic integer. Show that $2|\alpha$ in the sense that $\alpha/2$ is also an algebraic integer. Show that $4 \not| \alpha$.

5. Let α be an algebraic number. Show that there exists an integer m such that $m\alpha$ is an algebraic integer.

6. Suppose $\alpha, \beta, \gamma \in K$ where K is an algebraic number field. Suppose α, β are algebraic integers and γ satisfies $x^2 + \alpha x + \beta = 0$. Show that γ is an algebraic integer. Can you generalize this result?

7. Suppose $f(x) = x^2 + mx + n \in \mathbb{Z}[x]$ is irreducible. Suppose K is a field of degree 2 over $\mathbb{Q}$ and containing an element α such that $f(\alpha) = 0$. (For instance $K = \mathbb{Q}[x]/(f)$ and $\alpha = x + (f)$ or $K = \mathbb{Q}(\alpha)$ and α is given by the quadratic formula, but no matter). Let $\mathbb{Q}[\alpha] = \{g(\alpha) \mid g(x) \in \mathbb{Q}[x]\}$ be the set consisting of all $\mathbb{Q}$-polynomial expressions in α. Let $\mathbb{Q}(\alpha)$ be the fraction field of $\mathbb{Q}[\alpha]$, i.e. the smallest subfield of K that contains $\mathbb{Q}[\alpha]$. Let $d_f = m^2 - 4n$ be the discriminant of f and suppose $d_f = dk^2$ where d is *square-free*, meaning the only square that divides it is 1. Show that

(i) $\mathbb{Q}[\alpha]$ is a subring of K;

(ii) $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$;

(iii) $\mathbb{Q}[\alpha] = \mathbb{Q}[\beta]$, where $\beta = (2\alpha + m)/k$ satisfies $\beta^2 = d$.

8. Staying with the situation of the preceding problem, let us assume $\alpha = (-m + \sqrt{d_f})/2 \in \mathbb{C}$ so that $\beta = \sqrt{d}$. Let $\mathcal{O}_K \subseteq \mathbb{Q}(\alpha)$ be the set of algebraic integers in $K = \mathbb{Q}(\alpha)$.

(i) Suppose $d \equiv 2, 3 \bmod 4$. Show that $\mathcal{O}_K = [1, \sqrt{d}]_{\mathbb{Z}}$.

Notation: Whenever $\gamma_1, \ldots, \gamma_t$ are elements of a field F and R is a subring of F, we let $[\gamma_1, \ldots, \gamma_t]_R$ be the set of all $\mathbb{R}$-linear combinations $\sum_{i=1}^t r_i \gamma_i$.

(ii) if $d \equiv 1 \bmod 4$, show that $\mathcal{O}_K = [1, \frac{1+\sqrt{d}}{2}]_{\mathbb{Z}}$. [Hint: don't forget the useful criterion of problem 2].

(iii) Show that in either case, $\mathcal{O}_K = [1, \frac{d+\sqrt{d}}{2}]_{\mathbb{Z}}$.

9. Let $\omega = e^{2\pi i/3}$. What is the quickest way to show that ω is an algebraic integer? Now determine $\mathrm{Irr}_\omega(x)$.

10. Prove or disprove: if α is an algebraic number, with minimal polynomial $\mathrm{Irr}_\alpha(x)$, then $\mathrm{Irr}_\alpha(x)$ does not have repeated roots (in $\mathbb{C}$).

11. Let α be an algebraic number of degree n over $\mathbb{Q}$, i.e. $\mathrm{Irr}_\alpha(x; \mathbb{Q})$ has degree n. Suppose $f, g \in \mathbb{Q}[x]$ are polynomials of degree strictly less than n such that $f(\alpha) = g(\alpha)$. Show that $f = g$.

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 $d \equiv 2, 3 \bmod 4$, 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 $|\mathrm{disc}_K| > 1$. [Remark: Later we will see that if $K/\mathbb{Q}$ has degree $n > 1$, then $|\mathrm{disc}_K| > 1$. 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

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

has determinant
$$\det V(z_1,\dots,z_n)=\prod_{1\le i<j\le n}(z_i-z_j).$$

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 σ_i, $1\le i\le n$. For $i\ne j$, 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} ($i\ne j$ 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 $\eta_1,\dots,\eta_n$ belonging to B which form a basis for K/F and put $d=\mathrm{disc}_{K/F}(\eta_1,\dots,\eta_n)$. Recall we have proved in class that $d\ne 0$.

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

(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 $(c_1,\dots,c_n)\in\mathbb{Z}^n$ satisfying $d|c_j^2$ $(j=1,\dots,n)$ such that
$$\alpha=\frac{c_1\eta_1+\cdots+c_n\eta_n}{d}.$$

[Hint: Given $\xi\in B$, write $\xi=\sum_{j=1}^n x_j\eta_j$ with $x_1,\dots,x_n\in F$. Now consider the linear system (for $i=1,\dots,n$)
$$\mathrm{Tr}_{K/F}(\alpha\eta_i)=\sum_{j=1}^n\mathrm{Tr}_{K/F}(\eta_i\eta_j)x_j.$$
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 $f(x)=\mathrm{Irr}_\theta(x;F)$ has degree n. Show that
$$\mathrm{disc}_{K/F}(1,\theta,\dots,\theta^{n-1})=(-1)^{n(n-1)/2}\mathbb{N}_{K/F}(f'(\theta)).$$

18. Use 17) to prove the (should-be) well-known formula for the discriminant of the trinomial $f(x)=x^n+ax+b$:
$$\mathrm{disc}(x^n+ax+b)=(-1)^{n(n-1)/2}\left(n^nb^{n-1}+(-1)^{n-1}(n-1)^{n-1}a^n\right).$$

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 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 $\mathrm{disc}_K/\mathrm{disc}_f$? 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 $\mathfrak{p}$ be the principal ideal $\mathfrak{p} = (y^2 - x^3)$. Show that $\mathfrak{p}$ is a prime ideal but $A/\mathfrak{p}$ 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 θ be a root of f.
(a) Suppose $f'(r) = 0$ for some $r \in \mathbb{Z}$. Prove that $f(r)$ divides $\mathrm{disc}(1, \theta, \ldots, \theta^{n-1})$. [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 $\mathrm{disc}(1, \theta, \ldots, \theta^{n-1})$?
(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 the discriminant $\mathrm{disc}(1, \theta, \ldots, \theta^{n-1})$.

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 $0 \le i \le n - 1$, and ii) $p^2 \nmid a_0$. 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 $\mathrm{disc}(\Phi_p(x)) = \mathrm{disc}(1, \omega, \ldots, \omega^{p-2})$.

[Hint: Use 17; for calculating $\Phi_p'(x)$, use the fact that $\Phi_p(x)(x-1) = x^p - 1$; to compute $\mathbb{N}K/\mathbb{Q}(\omega - 1)$, 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

$$\operatorname{disc}(1, \omega, \ldots, \omega^{p-2}) = \operatorname{disc}(1, 1-\omega, \ldots, (1-\omega)^{p-2}).$$

(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.[1] 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 disc_K be the discriminant of K, i.e. $\operatorname{disc}_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n)$ 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 disc_K is $(-1)^{r_2}$.

b) Prove *Stickelberger's Theorem:* $\operatorname{disc}_K \equiv 0, 1 \bmod 4$.

[1] 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. 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!