Math 129 Problem Set 3

Lev Kruglyak

February 19, 2022

I did not collaborate with anyone for this problem set

Problem 2.19. Let R be a commutative ring and fix elements $a_1, a_2, \ldots, a_n \in R$. Prove that

$$\begin{vmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{vmatrix} = \prod_{1 \le r < s \le n} (a_s - a_r).$$

We'll proceed by induction. Clearly if $n = 1$ we get the desired result. Now suppose for some n that

$$\begin{vmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{vmatrix} = \prod_{1 \le r < s \le n} (a_s - a_r).$$

Note that for any polynomial $f(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0$, we have the equality of determinants:

$$\begin{vmatrix} 1 & a_1 & \cdots & a_1^{n-1} & a_1^n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} & a_n^n \\ 1 & a_{n+1} & \cdots & a_{n+1}^{n-1} & a_{n+1}^n \end{vmatrix} = \begin{vmatrix} 1 & a_1 & \cdots & a_1^{n-1} & f(a_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} & f(a_n) \\ 1 & a_{n+1} & \cdots & a_{n+1}^{n-1} & f(a_{n+1}) \end{vmatrix}.$$

This can be seen by simply performing repeated column operations; to the last column of the matrix add c_0 times the first column, c_1 times the second column, etc. Set $f(t) = \prod_{i=1}^{n}(t - a_i)$. Then

$$\begin{vmatrix} 1 & \cdots & a_1^{n-1} & a_1^n \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \cdots & a_n^{n-1} & a_n^n \\ 1 & \cdots & a_{n+1}^{n-1} & a_{n+1}^n \end{vmatrix} = \begin{vmatrix} 1 & \cdots & a_1^{n-1} & f(a_1) \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \cdots & a_n^{n-1} & f(a_n) \\ 1 & \cdots & a_{n+1}^{n-1} & f(a_{n+1}) \end{vmatrix} = \begin{vmatrix} 1 & \cdots & a_1^{n-1} & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \cdots & a_n^{n-1} & 0 \\ 1 & \cdots & a_{n+1}^{n-1} & f(a_{n+1}) \end{vmatrix}$$

$$= f(a_{n+1}) \left(\prod_{1 \le r < s \le n} (a_s - a_r) \right) = \prod_{1 \le r < s \le n+1} (a_s - a_r).$$

This completes the inductive step.

Problem 2.21. Let α be an algebraic integer and let f be a monic polynomial over $\mathbb{Z}$ (not necessarily irreducible) such that $f(\alpha) = 0$. Show that $\text{disc}(\alpha)$ divides $\text{N}^{\mathbb{Q}[\alpha]} f'(\alpha)$.

Since $f(x)$ is a monic polynomial vanishing at α, it must be a polynomial multiple of the minimal irreducible polynomial for α, $m_\alpha(x)$. Say $f(x) = m_\alpha(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$. Then by Theorem 2.8, $\text{disc}(\alpha) = \pm \text{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]} m'_\alpha(\alpha)$. But

$$\begin{aligned} \text{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]} f'(\alpha) &= \text{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]} m'_\alpha(\alpha)g(\alpha) + \text{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]} m_\alpha(\alpha)g'(\alpha) \\ &= \pm g(\alpha)\text{disc}(\alpha) \end{aligned}.$$

Thus $\text{disc}(\alpha) \mid \text{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]} f'(\alpha)$.

Problem 2.22. Let K be a number field of degree n over $\mathbb{Q}$ and fix algebraic integers $\alpha_1, \ldots, \alpha_n \in K$. Prove that $\text{disc}(\alpha_1, \ldots, \alpha_n) \equiv 0 \text{ or } 1 \mod 4$.

We know that $d = \text{disc}(\alpha_1, \ldots, \alpha_n)$ is in $\mathbb{Z}$; we will first show that $d \equiv 0 \text{ or } 1 \mod 4$. Letting $\alpha_1, \ldots, \alpha_n$ denote the embeddings of K in $\mathbb{C}$, we know that d is the square of the determinant $|\sigma_i(\alpha_j)|$. This determinant is a sum of $n!$ terms, one for each permutation of $\{1, \ldots, n\}$. Let P denote the sum of the terms corresponding to even permutations, and let N denote the sum of the terms (without negative signs)corresponding to odd permutations. Thus $d = (P - N)^2 = (P + N)^2 - 4PN$.

We'll prove that $P+N \in \mathbb{Z}$ and $PN \in \mathbb{Z}$. First note that $P+N$ and PN are algebraic integers, being sums and products of algebraic integers. Pick some normal extension L of $\mathbb{Q}$ containing K, and let σ be any automorphism of L. Then for any complex embedding σ_i, $\sigma\sigma_i$ is also a complex embedding, so $\{\sigma\sigma_1, \ldots, \sigma\sigma_n\}$ is a permutation of $\{\sigma_1, \ldots, \sigma_n\}$. Let $\pi \in S_n$ be the permutation such that $\sigma\sigma_i = \sigma_{\pi(i)}$.

If π is an even permutation, pick any even permutation $\tau \in S_n$ so we have $\sigma(\sigma_{\tau(1)}(\alpha_1) + \cdots + \sigma_{\tau(n)}(\alpha_n)) = \sigma_{\pi\tau(1)}(\alpha_1) + \cdots + \sigma_{\pi\tau(n)}(\alpha_n)$. Since $\pi\tau$ is even, every term on the left is sent to a term on the right so $\sigma(P) = P$ and $\sigma(N) = N$. Thus $\sigma(P + N) = P + N$ and $\sigma(PN) = PN$. Similarly if π is an odd permutation, we get $\sigma(P) = N$ and $\sigma(N) = P$. Since L is a normal extension, and $P + N$ and PN are preserved by every automorphism of L, $P + N, PN \in \mathbb{Q}$ and so $P + N, PN \in \mathbb{Z}$ since they are algebraic integers.

Finally $d = (P + N)^2 - 4PN \equiv (P + N)^2 \mod 4$ so $d \equiv 0 \text{ or } 1 \mod 4$.

Problem 2.23. Just as with the trace and norm, we can define the relative discriminant disc_K^L of an n-tuple, for any pair of number fields $K \subset L$, $[L:K] = n$.

(a) Generalize Theorems 2.6-2.8 and the corollary to Theorem 2.6

(b) Let $K \subset L \subset M$ be number fields; $[L:K] = n$, $[M:L] = m$ and let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_m\}$ be bases for L over K and M over L respectively. Establish the formula:

$$\mathrm{disc}_K^M(\alpha_1\beta_1, \ldots, \alpha_n\beta_m) = (\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n))^m \mathrm{N}_M^L \mathrm{disc}_L^M(\beta_1, \ldots, \beta_m).$$

(c) Let K and L be number fields satisfying the conditions to Corollary 1, Theorem 12. Show that $\mathrm{disc}(T) = \mathrm{disc}(R)^{[L:Q]} \cdot \mathrm{disc}(S)^{[K:Q]}$.

(a) The proofs of all of the theorems are basically the same, just replacing trace and nrm with relative traces. For any pair of number fields $K \subset L$ with $[L:K] = n$:

Theorem 2.6.
$$\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n) = \left|T_K^L(\alpha_i\alpha_j)\right|.$$

Corollary. $\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n) \in K$; and if all of the α_i are algebraic integers then $\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n) \in \mathbb{A} \cap K$.

Theorem 2.7. $\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n) = 0$ if and only if $\alpha_1, \ldots, \alpha_n$ are linearly dependent over K.

Theorem 2.8. Suppose $L = K[\alpha]$, and let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α over K. Then
$$\mathrm{disc}_K^L(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \le r < s \le n} (a_r - a_s)^2 = \pm \mathrm{N}_K^L(f'(\alpha)).$$

(b)

(c)

Problem 2.28. Let $f(x) = x^3 + ax + b$, a and $b \in \mathbb{Z}$,and assume f is irreducible over $\mathbb{Q}$. Let α be a root of f.

(a) Show that $f'(\alpha) = -(2a\alpha + 3b)/\alpha$.

(b) Show that $2a\alpha + 3b$ is a root of $\left(\frac{x-3b}{2a}\right)^3 + a\left(\frac{x-3b}{2a}\right) + b$. Use this to find $\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha + 3b)$.

(c) Show that $\mathrm{disc}(\alpha) = -(4a^3 + 27b^2)$.

(d) Suppose $\alpha^3 = \alpha + 1$. Prove that $\{1, \alpha, \alpha^2\}$ is an integral basis for $\mathbb{A} \cap \mathbb{Q}[\alpha]$. Do the same if $\alpha^3 + \alpha = 1$.

(a) Note that $f'(x) = 3x^2 + a$ and $\alpha^3 + a\alpha + b = 0$ so $\alpha^2 = \frac{-a\alpha - b}{\alpha}$. Thus $f'(\alpha) = 3\left(\frac{-a\alpha - b}{\alpha}\right) + a =$

$-(2a\alpha+3b)/\alpha$ so we are done.

(b) Since plugging in $x = 2a\alpha + 3b$ to $\frac{x-3b}{2b}$ gives α, clearly $2a\alpha+3b$ is a root of $\left(\frac{x-3b}{2a}\right)^3 + a\left(\frac{x-3b}{2a}\right) + b$. This polynomial is irreducible because it is simply a linear substitution of an irreducible polynomial. Then by Theorem 2.4, the norm of $2a\alpha+3b$ is simply the negative ratio of the x^0 and x^3 coefficients, so $\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha+3b) = 27b^3 + 4a^3b$.

(c) Note that by Theorem 2.8, $\mathrm{disc}(\alpha) = \pm\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]} f'(\alpha)$ where f is the minimal polynomial for α. By (a), $\mathrm{disc}(\alpha) = -\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]} - (2a\alpha+3b)/\alpha = -\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(-1)\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha+3b)/\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha)$. $\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(-1) = -1$ and $\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha) = -b$ so by (b), $\mathrm{disc}(\alpha) = -(27b^3+4a^3b)/b = -27b^2 - 4a^3$.

(d) First we'll prove a convenient lemma relating the discriminant to an integral basis.

> **Claim.** Let α be an algebraic integer of degree d. Then $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is an integral basis for $\mathbb{Q}[\alpha]$ if $\mathrm{disc}(\alpha)$ is squarefree.

> **Proof.** Let $\{\beta_1, \ldots, \beta_{d-1}\}$ be an integral basis for $\mathbb{Q}[\alpha]$. Then there is some matrix $A \in M_{d\times d}(\mathbb{Z})$ such that
>
> $$\mathrm{disc}(\alpha) = \mathrm{disc}(1, \alpha, \ldots, \alpha^{d-1}) = (\det A)^2 \mathrm{disc}(\beta_1, \ldots, \beta_{d-1}).$$
>
> However since $\mathrm{disc}(\alpha)$ is squarefree, $\det A = \pm 1$ therefore $1, \alpha, \ldots, \alpha^{d-1}$ is an integral basis for $\mathbb{Q}[\alpha]$. □

If $\alpha^3 = \alpha + 1$ then α has minimal polynomial $x^3 - x - 1$, which is irreducible by the rational root theorem. Then by (c) $\mathrm{disc}(\alpha) = -23$ which is a squarefree integer so $\{1, \alpha, \alpha^2\}$ is an integral basis for $\mathbb{Q}[\alpha]$. If $\alpha^3 + \alpha = 1$ then α has minimal polynomial $x^3 + x - 1$ which is again irreducible by the rational root theorem. Then $\mathrm{disc}(\alpha) = -31$ which is squarefree integer so $\{1, \alpha, \alpha^2\}$ is an integral basis for $\mathbb{Q}[\alpha]$.

> **Problem 2.33.** Let $\omega = e^{2\pi i/m}$, $m \geq 3$. We know that $\mathrm{N}(\omega) = \pm 1$ since ω is a unit. Show that the $+$ sign holds.

Note that since $m > 2$, ± 1 are not conjugates of ω. Also the product of ω^i and $\overline{\omega^i}$ is 1 because $\overline{\omega^i} = \omega^{m-i}$. Thus $\mathrm{N}(\omega) = 1$ because it is the product of all of the conjugates of ω.

> **Problem 2.34.** Let $\omega = e^{2\pi i/m}$ for m a positive integer.
>
> (a) Show that $1 + \omega + \omega^2 + \cdots + \omega^{k-1}$ is a unit in $\mathbb{Z}[\omega]$ if k is relatively prime to m.
>
> (b) Let $m = p^r$, p a prime. Show that $p = u(1-\omega)^n$ where $n = \varphi(p^r)$ and u is a unit in $\mathbb{Z}[\omega]$.

(a) Suppose k is relatively prime to m. Then k has a modular inverse modulo m so there is some ℓ such that $k\ell \equiv 1 \mod m$ and so $\omega^{k\ell} = \omega$. This gives us the element of $\mathbb{Z}[\omega]$,

$$\frac{1-\omega}{1-\omega^k} = \frac{1-\omega^{k\ell}}{1-\omega^k} = 1 + \omega^k + \cdots + \omega^{k(\ell-1)}.$$

This is actually an inverse to $1+\omega+\omega^2+\cdots+\omega^{k-1}$, since

$$\frac{1-\omega}{1-\omega^k}(1+\omega+\omega^2+\cdots+\omega^{k-1}) = \frac{1-\omega}{1-\omega^k}\frac{1-\omega^k}{1-\omega} = 1.$$

So $1+\omega+\omega^2+\cdots+\omega^{k-1} \in \mathbb{Z}[\omega]^\times$.

(b) Recall that Lemma 2 of Theorem 2.10 states that

$$p = \prod_{p\nmid k}^{p^r}(1-\omega^k).$$

(a) implies that $(1-\omega^k) = u_k(1-\omega)$, for $u_k = 1+\omega+\omega^2+\cdots+\omega^{k-1} \in \mathbb{Z}[\omega]^\times$. Since there are $\varphi(p^r)$ terms in the product, it follows that $p = u(1-\omega)^{\varphi(p^r)}$ where $u = \prod_{p\nmid k}^{p^r} u_k$.

Problem 2.35. Set $\theta = \omega + \omega^{-1}$ for $\omega = e^{2\pi i/m}$, $m \geq 3$.

(a) Show that ω is a root of a polynomial of degree 2 over $\mathbb{Q}[\theta]$.

(b) Show that $\mathbb{Q}[\theta] = \mathbb{R} \cap \mathbb{Q}[\omega]$ and that $\mathbb{Q}[\omega]$ has degree 2 over this field.

(c) Show that $\mathbb{Q}[\theta]$ is the fixed field of the automorphism σ of $\mathbb{Q}[\omega]$ given by $\sigma(\omega) = \omega^{-1}$. Note that σ is just complex conjugation.

(a) Clearly ω is a root of $x^2 - \theta x + 1 \in \mathbb{Q}[\theta, x]$ since $\omega^2 - \theta\omega + 1 = \omega^2 - \omega^2 - 1 + 1 = 0$.

(b) Since $\omega \notin \mathbb{R}$ yet $\theta \in \mathbb{R}$, $\mathbb{Q}[\theta] \subsetneq \mathbb{Q}[\omega]$. This combined with (a) means that $[\mathbb{Q}[\omega] : \mathbb{Q}[\theta]] = 2$. So we have $\mathbb{Q}[\theta] \subset \mathbb{R} \cap \mathbb{Q}[\omega] \subsetneq \mathbb{Q}[\omega]$. By the degree tower property,

$$[\mathbb{R} \cap \mathbb{Q}[\omega] : \mathbb{Q}[\theta]] = \frac{[\mathbb{Q}[\omega] : \mathbb{Q}[\theta]]}{[\mathbb{Q}[\omega] : \mathbb{R} \cap \mathbb{Q}[\omega]]} < 2$$

yet $[\mathbb{Q}[\omega] : \mathbb{Q}[\theta]] = 2$ so $[\mathbb{R} \cap \mathbb{Q}[\omega] : \mathbb{Q}[\theta]] = 1$ and thus $\mathbb{Q}[\theta] = \mathbb{R} \cap \mathbb{Q}[\omega]$. This also implies that $[\mathbb{Q}[\omega] : \mathbb{R} \cap \mathbb{Q}[\omega]] = 2$.

(c) Since σ is just complex conjugation, the fixed field of σ in $\mathbb{Q}[\omega]$ is $\mathbb{R} \cap \mathbb{Q}[\omega] = \mathbb{Q}[\theta]$, since $\mathbb{R}$ is the fixed field of σ in $\mathbb{C}$.