feedback Allman

HW 8: Marcus Chapter 2 problems

8. (a) Let $\omega = e^{2\pi i/p}$, p an odd prime. Show that $\mathbb{Q}(\omega)$ contains $\sqrt{p}$ if $p \equiv 1 \pmod 4$, and $\sqrt{-p}$ if $p \equiv -1 \pmod 4$. (Hint: Recall that we have shown that $\mathrm{disc}(\omega) = \pm p^{p-2}$ with plus sign holding iff $p \equiv 1 \pmod 4$.) Express $\sqrt{-3}$ and $\sqrt{5}$ as polynomials in the appropriate ω.

$\in \mathbb{Q}\setminus\mathbb{Z}$ better: $p^{p-2} = p \cdot p^{p-3}$ with both factors in $\mathbb{Z}$.

Proof. Note that $\mathrm{disc}(\omega) = \pm p^{p-2} = \pm p^{-1} p^{p-1}$. Since p is odd, $p - 1 = 2m$ for some even m. Then $\mathrm{disc}(\omega) = \pm p^{-1} p^{2m}$ and since $\mathrm{disc}(\omega)$ is the square of an element in $\mathbb{Q}(\omega)$ it follows that $\sqrt{\pm p^{-1} p^{2m}} = \sqrt{\pm p^{-1}}\, p^m \in \mathbb{Q}(\omega)$ so $p^m \sqrt{\pm p^{-1}}\, p^{1-m} = \sqrt{\pm p} \in \mathbb{Q}(\omega)$ with plus sign holding iff $p \equiv 1 \pmod 4$ as desired.

The idea is to use sums of powers of ω coming from $\sqrt{\mathrm{disc}(\omega)} = \sqrt{\prod (\omega_i - \omega_k)^2}$

Observe that when $p = 3$, $\sqrt{-3} = 2\omega - 1 = 2(1/2 + i\sqrt{3}/2) - 1 = i\sqrt{3} = \sqrt{-3}$.
Using the fact that $5^{3/2} = \sqrt{\mathrm{disc}(\omega_5)}$, we find that $\sqrt{5} = 1 + 2\omega^2 + 2\omega^3$. ?? "$-\sqrt{5}$" ? ☐

(b) Show that the 8^{th} cyclotimic field contains $\sqrt{2}$.

Proof. Note that $\sqrt{2} = \omega_4 - \omega_4^3 = \omega_8^2 - \omega_8^6$ so $\sqrt{2} \in \mathbb{Q}(\omega_8)$. ☐

17. Here is another interpretation of the trace and norm: Let $K \subset L$ and fix $\alpha \in L$; multiplication by α gives a linear mapping of L to itself, considering L as a vector space over K. Let A denote the matrix of this mapping with respect to any basis $\{\alpha_1, \alpha_2, \dots\}$ for L over K. (Thus the j^{th} column of A consists of the coordinates of $\alpha\alpha_j$ with respect to the α_i.) Show that $T_K^L(\alpha)$ and $N_K^L(\alpha)$ are, respectively, the trace and determinant of A. (Hint: It is well known that the trace and determinant are independent of the particular basis chosen; thus it is sufficient to calculate them for any convenient basis. Fix a basis $\{\beta_1, \beta_2, \dots\}$ for L over $K[\alpha]$ and multiply by powers of α to obtain a basis for L over K. Finally, use Theorem 4′.)

Proof. Let A' be the matrix representing multiplication by α in $K[\alpha]$ with respect to the basis $\{1, \alpha, \dots, \alpha^{d-1}\}$. If α has minimal polynomial

$$f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1 x + c_0,$$

then the matrix A' has the form

$$A' = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \ddots & 0 & -c_2 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{pmatrix},$$

Nice!

because $\alpha^d = -c_{n-1}\alpha^{d-1} + \cdots - c_1\alpha - c_0$. Clearly, the trace of A' is $-c_{n-1} = t(\alpha)$, while if we calculate the determinant of A' by expanding about the top row, we find that it is $\pm(-c_0)\det(I) = \pm c_0$, with $+$ holding if and only if d is even. This precisely $d(\alpha)$.

Now we fix some basis $\{\beta_1, \beta_2, \dots, \beta_{n/d}\}$ for L over $K[\alpha]$, and multiply by powers of α to obtain a basis for L over K. We choose to order this basis as

$$\{\beta_1, \beta_1\alpha_1, \beta_1\alpha^2, \dots, \beta_1\alpha^{d-1}, \beta_2, \beta_2\alpha_1, \dots, \beta_{n/d}\alpha^{d-1}\}.$$

~~With respect to this ordering of the basis, multiplication by α has corresponding matrix (in block form)~~

$$A = \begin{pmatrix} A' & 0 & \cdots & 0 \\ 0 & A' & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & A' \end{pmatrix},$$

With respect to this ordering of the basis, multiplication by α has corresponding matrix (in block form)

$$A = \begin{pmatrix} A' & 0 & \cdots & 0 \\ 0 & A' & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & A' \end{pmatrix},$$ ✓

where A' is the $d \times d$ matrix from above, 0 is the $d \times d$ zero matrix, and there are $n/d \times n/d$ blocks in the block structure of A.

Then the trace of A adds n/d copies of $-c_{n-1}$, giving $\frac{n}{d}(-c_{n-1}) = \frac{n}{d}t(\alpha) = \mathrm{Tr}_K^L(\alpha)$. Similarly, the determinant of A is $|A'||A'|\cdots|A'| = |A'|^{n/d} = d(\alpha)^{n/d} = N_K^L(\alpha)$. ✓ □ great.

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 $\mathrm{disc}(\alpha)$ divides $N^{\mathbb{Q}[\alpha]}(f'(\alpha))$.

Proof. Suppose $f(\alpha) = 0$. Then if $m(x)$ is the minimal polynomial of α, we know that f has m as a factor; that is $f(x) = m(x)q(x)$ for some $q(x) \in \mathbb{Z}[x]$. Then

$$\mathrm{disc}(\alpha) = \pm N^{\mathbb{Q}[\alpha]}(m'(\alpha)),$$ up to sign

while

$$N(f'(\alpha)) = N((m \cdot q)'(\alpha)) = N(m'(\alpha)q(\alpha) + m(\alpha)q(\alpha)) = N(m'(\alpha))N(q(\alpha)),$$

using the multiplicity of the norm. Because q is in $\mathbb{Z}[x]$ and α is an algebraic integer, $q(\alpha) \in \mathcal{O}$, so $N(q(\alpha)) \in \mathbb{Z}$. Thus, $\mathrm{disc}(\alpha) = N(m'(\alpha)) \mid N(f'(\alpha))$. ✓ □

See note.

22. Let K be a number field of degree n over $\mathbb{Q}$ and fix algebraic integers $\alpha_1, \ldots, \alpha_n \in K$. We know that $d = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ is in $\mathbb{Z}$; we will show that $d \equiv 0$ or $1 \mod 4$. Letting $\sigma_1, \ldots, \sigma_n$ 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 $d = (P - N)^2 = (P + N)^2 - 4PN$. Complete the proof by showing that $P + N$ and PN are in $\mathbb{Z}$. (Suggestion: Show that they are algebraic integers and that they are in $\mathbb{Q}$; for the latter, extend all σ_i to some normal extension L of $\mathbb{Q}$ so that they become automorphisms of L.)

In particular we have $\mathrm{disc}(\mathbb{A} \cap K) \equiv 0$ or $1 \mod 4$. This is known as *Stickelberger's criterion.*

Proof. First, note that

$$|\sigma_i(\alpha_j)|^2 = \left[\sum_{\tau\in A_n} \sigma_{\tau(1)}(\alpha_1)\cdots\sigma_{\tau(n)}(\alpha_n) - \sum_{\gamma\in S_n\setminus A_n} \sigma_{\gamma(1)}(\alpha_1)\cdots\sigma_{\gamma(n)}(\alpha_n)\right]^2 = (P-N)^2.$$

$d=(P-N)^2$

Let L be the normal closure of K (i.e., the smallest L such that L contains K and L is normal over $\mathbb{Q}$). Then each of the σ_i extend to an automorphism of L, which we will also call σ_i. If σ is any automorphism of L, then σ restricted to K is a $\mathbb{Q}$-embedding of K, so σ is the extension of some σ_j. In particular, for all i, $\sigma\sigma_i = \sigma_j$ for some j, when we restrict to K. Thus, we can view σ as simply permuting the elements of the set $\{\sigma_1,\dots,\sigma_n\}$.

Choose some $\beta\in \mathrm{Gal}(L/\mathbb{Q})$ and apply β to P. We find that

$$\begin{aligned}\beta P &= \beta\left[\sum_{\tau\in A_n}\sigma_{\tau(1)}(\alpha_1)\cdots\sigma_{\tau(n)}(\alpha_n)\right]\\ &= \sum_{\tau\in A_n}\beta\sigma_{\tau(1)}(\alpha_1)\cdots\beta\sigma_{\tau(n)}(\alpha_n)\\ &= \sum_{\tau\in A_n}\sigma_{\beta\tau(1)}(\alpha_1)\cdots\sigma_{\beta\tau(n)}(\alpha_n).\end{aligned}$$

If β is an even permutation, then $\beta\tau$ is even, so summing across all $\beta\tau\in A_n$ is equivalent to summing across all $\tau\in A_n$, and $\beta P = P$. On the other hand, if β is an odd permutation, then $\beta\tau$ is odd, so summing across all $\beta\tau\in A_n$ is equivalent to summing across all $\gamma\in S_n\setminus A_n$, and $\beta P = N$.

Via a similar proof, $\beta N = N$ if β is an even permutation, and $\beta N = P$ if β is odd. In either case, $\beta(N+P) = N+P$ and $\beta(NP) = NP$. Thus, $N+P$ and NP are in the fixed field of $\mathrm{Gal}(L/\mathbb{Q})$, which is precisely $\mathbb{Q}$. Thus, $N+P$ and NP are rational.

Good.

On the other hand, each of the α_i are algebraic integers, as are all their conjugates. Thus, N and P are also algebraic integers, so $N+P$ and NP are rational algebraic integers—that is, $N+P, NP\in\mathbb{Z}$.

4

– typo!

To see that Stickelberger's criterion holds, note that $d\equiv (P+N)^2 \mod 4$. However, for $m\in\mathbb{Z}$, $m^2\equiv 0$ or $1 \mod 4$, so $d\equiv (P+N)^2\equiv 0$ or $1 \mod 4$. $\square$

$d=(P-N)^2$
$=(P+N)^2-4PN$
with $P+N,\ PN\in\mathbb{Q}\cap\mathbb{Z}$
$=\mathbb{Z}$

The problem is that $P+N\notin\mathbb{Z}$ possible.
Eg. $\mathbb{Q}(\omega_5)$
$\Delta(\omega_5)=5$
but $\sqrt{5}\notin\mathbb{Z}$

i.e. $P-N\notin\mathbb{Z}$ is possible

26. Prove the following generalization of Theorem 11: Let $\beta_1,\dots,\beta_n$ and $\gamma_1,\dots,\gamma_n$ be any members of K (a number field of degree n over $\mathbb{Q}$) such that the β_i and γ_i generate the same additive subgroup of K. Then $\mathrm{disc}(\beta_1,\dots,\beta_n) = \mathrm{disc}(\gamma_1,\dots,\gamma_n)$. (Thus we can define $\mathrm{disc}(G)$ for any additive subgroup G of K which is generated by n elements. This is only interesting when the n elements are linearly independent over $\mathbb{Q}$, in which case G is free Abelian of rank n.)

Proof. Because the β_i and γ_i generate the same additive subgroup of K, we may write each of the β_i as a $\mathbb{Z}$-linear combination of the γ_i. That is,

$$\beta_1 = c_1\gamma_1 + c_2\gamma_2 + \cdots + c_n\gamma_n,$$

where the $c_i \in \mathbb{Z}$. In matrix form, if β is the column vector of the β_i and γ is the column vector of the γ_i, we have

$$\beta = M\gamma,$$

where $M \in M_n(\mathbb{Z})$. For $1 \leq i \leq n$, we apply σ_i to the transpose of this equation to find

$$\sigma_i(\beta^T) = \sigma_i(\gamma^T M^T) = \sigma_i(\gamma_i)M^T,$$

because the σ_i fix $\mathbb{Q}$. Letting i and j each run from 1 to n, we can write this as the matrix equation

$$(\sigma_i(\beta_j)) = (\sigma_i(\gamma_j))M^T.$$

Taking the determinant of each side and squaring, we find that

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = \operatorname{disc}(\gamma_1, \ldots, \gamma_n)|M|^2.$$

✓

Recalling that $\operatorname{disc}(\beta_1, \ldots, \beta_n)$ and $\operatorname{disc}(\gamma_1, \ldots, \gamma_n)$ are rational, let d be the least common multiple of their denominators. Then, multiplying through both sides so that we have an equation in the integers, we find that

$$d\operatorname{disc}(\beta_1, \ldots, \beta_n) \mid d\operatorname{disc}(\gamma_1, \ldots, \gamma_n).$$

However, it is equally true that each of the γ_i is a $\mathbb{Z}$-linear combination of the β_i, so we also have that

$$d\operatorname{disc}(\gamma_1, \ldots, \gamma_n) \mid d\operatorname{disc}(\beta_1, \ldots, \beta_n).$$

Thus,

$$d\operatorname{disc}(\beta_1, \ldots, \beta_n) = d\operatorname{disc}(\gamma_1, \ldots, \gamma_n),$$

and

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = \operatorname{disc}(\gamma_1, \ldots, \gamma_n).$$

Nice

$\square$