Solutions 3

1. a) Let $P = (x_0 : \ldots : x_n)$, and let K be a number field such that $x_0, \ldots, x_n \in K$ (so $P \in \mathbb{P}^n_K$). Let $x = (x_0, \ldots, x_n) \in \mathbb{A}^{n+1}_K$, and let $d = [K : \mathbb{Q}]$. Then $x_j \neq 0$ for some $j \in \{0, 1, \ldots, n\}$, so

$$h'(P) = \frac{1}{d} \sum_v \log \|x\|'_v = \frac{1}{d} \sum_v \log \max\{\|x_i\|_v ;\, 0 \leq i \leq n\} \geq$$
$$\geq \frac{1}{d} \sum_v \log \|x_j\|_v = 0$$

due to the product formula.

If v is an non-archimedean place of K, then $\|x\|_v = \|x\|'_v$.

If v is a real place of K corresponding to the embedding $\tau \colon K \to \mathbb{R}$, then $n_v = 1$, and $\|x\|_v = \left(\sum_{i=0}^n \tau(x_i)^2\right)^{1/2}$, $\|x\|'_v = \max\{|\tau(x_i)|;\, 0 \leq i \leq n\}$, so $\|x\|'_v \leq \|x\|_v \leq \sqrt{n+1}\|x\|'_v$.

If v is a complex place of K, then $n_v = 2$, and $\|x\|_v = \sum_{i=0}^n |\tau(x_i)|^2$, $\|x\|'_v = \max\{|\tau(x_i)|^2;\, 0 \leq i \leq n\}$, so $\|P\|'_v \leq \|P\|_v \leq (n+1)\|P\|'_v$.

So $\|P\|'_v \leq \|P\|_v \leq (n+1)^{n_v/2}\|P\|'_v$ for all archimedean places v. After taking logarithms, summing up, and dividing by d, we get that

$$h'(P) \leq h(P) \leq h'(P) + \frac{1}{d} \sum_{v|\infty} \frac{n_v}{2} \log(n+1) = h'(P) + \frac{1}{2}\log(n+1),$$

where we have used that $\sum_{v|\infty} n_v = d$.

b) Let K be a number field containing x, and let $d = [K : \mathbb{Q}]$. Then

$$h(x) = \frac{1}{d} \sum_v \log^+ \|x\|_v = \frac{1}{d} \sum_v \log \max(\|x\|_v, 1) =$$
$$= \frac{1}{d} \sum_v \log \max(\|x\|_v, \|1\|_v) = \frac{1}{d} \sum_v \log \|(x,1)\|'_v = h'(x : 1).$$

c) Show that $h(xy) \leq h(x) + h(y)$ for every $x, y \in \overline{\mathbb{Q}}$.

Let $x, y \in K$ for some number field K. Then it is enough to prove that $h_K(xy) \leq h_K(x) + h_K(y)$.

Claim: $\log^+(ab) \leq \log^+(a) + \log^+(b)$ for every $a, b \geq 0$. Proof: $\log^+(ab) = \max(0, \log(ab))$, so it is enough to show that $0 \leq \log^+(a) + \log^+(b)$ and $\log(ab) = \log(a) + \log(b) \leq \log^+(a) + \log^+(b)$. Both of these are trivial.

Using the claim, we get that

$$h_K(xy) = \sum_v \log^+ \|xy\|_v = \sum_v \log^+(\|x\|_v \|y\|_v) \leq$$
$$\leq \sum_v \log^+ \|x\|_v + \log^+ \|y\|_v = h_K(x) + h_K(y).$$

d) According to b), $h(y) = h'(y : 1) = h'(\tilde{y})$ for every $y \in \overline{\mathbb{Q}}$, where $\tilde{y} \in \mathbb{A}^1_{\overline{\mathbb{Q}}}$ corresponds to $y \in \overline{\mathbb{Q}}$. So this is just the special case of e) when $n = 1$.

e) More generally, show that $h'(P_1 + \cdots + P_m) \leq h'(P_1) + \cdots + h'(P_m) + \log(m)$ for every $P_1, \ldots, P_m \in \mathbb{A}^n_{\overline{\mathbb{Q}}}$.

Hint: First show that $\log^+(\sum_{i=1}^m a_i) \leq \log(m) + \sum_{i=1}^m \log^+(a_i)$ *for* $a_1, \ldots, a_m \in \mathbb{R}_{\geq 0}$ *and* $m \geq 1$.

Let K be a number field such that $P_1, \ldots, P_m \in \mathbb{A}^n_K$, and let $d = [K : \mathbb{Q}]$. Note that if $P = (z_1, \ldots, z_n) \in \mathbb{A}^n_K$, then

$$h'(P) = h'(z_1 : \ldots : z_n : 1) = \frac{1}{d} \sum_v \log \max\{\|z_1\|_v, \ldots, \|z_n\|_v, \|1\|_v\} =$$
$$= \frac{1}{d} \sum_v \log^+ \max_{1 \leq i \leq n} \|z_i\|_v.$$

Now let $P_j = (x_{j,1}, \ldots, x_{j,n}) \in \mathbb{A}^n_K$ for every $j \in \{1, \ldots, m\}$, and let $Q = \sum_{j=1}^m P_j = (y_1, \ldots, y_n) \in \mathbb{A}^n_K$, where $y_i = \sum_{j=1}^m x_{j,i}$.

We will prove that

$$\log^+ \max_{1 \leq i \leq n} \|y_i\|_v \leq \sum_{j=1}^m \log^+ \max_{1 \leq i \leq n} \|x_{j,i}\|_v \tag{1}$$

for every non-archimedean place v, and

$$\log^+ \max_{1 \leq i \leq n} \|y_i\|_v \leq n_v \log(m) + \sum_{j=1}^m \log^+ \max_{1 \leq i \leq n} \|x_{j,i}\|_v \tag{2}$$

for every archimedean place v. Summing these and dividing by d, we get using $\sum_{v|\infty} n_v = d$ that

$$h'(Q) = \frac{1}{d}\sum_{v} \log^+ \max_{1\le i\le n} \|y_i\| \le$$

$$\le \frac{1}{d}\sum_{v|\infty} n_v \log(m) + \frac{1}{d}\sum_{j=1}^{m}\sum_{v} \log^+ \max_{1\le i\le n} \|x_{j,i}\|_v =$$

$$= \log(m) + \sum_{j=1}^{m} h'(P_j).$$

Claim: $\log^+(a^2) \le 2\log^+(a)$ for every $a \ge 0$, and $\log^+(\sum_{i=1}^m a_i) \le \log(m) + \sum_{i=1}^m \log^+(a_i)$ for every $a_1, \ldots, a_m \ge 0$ and $m \ge 1$. Proof: We have seen in c) that $\log^+(ab) \le \log^+(a) + \log^+(b)$. Using this for $b = a$, we get the first part. Now let $a_1, \ldots, a_m \ge 0$. Since $\log^+(\sum_{i=1}^m a_i) = \max\{0, \log \sum_{i=1}^m a_i\}$, it is enough to prove that $0 \le \log(m) + \sum_{i=1}^m \log^+(a_i)$ and $\log \sum_{i=1}^m a_i \le \log(m) + \sum_{i=1}^m \log^+(a_i)$. The first inequality is trivial. Let $a_k = \max\{a_1, \ldots, a_m\}$, where $k \in \{1, \ldots, m\}$, then

$$\log \sum_{i=1}^{m} a_i \le \log(m a_k) = \log(m) + \log(a_k) \le \log(m) + \log^+(a_k) \le$$

$$\le \log(m) + \sum_{i=1}^{m} \log^+(a_i),$$

proving the second inequality.

Proof of (1): v is non-archimedean, so $\|y_i\|_v \le \max_{1\le j\le m} \|x_{j,i}\|_v$. Let $\|x_{p,q}\|_v = \max_{i,j} \|x_{j,i}\|_v$, then $\|y_i\|_v \le \max_{1\le j\le m} \|x_{j,i}\|_v \le \|x_{p,q}\|_v$, since v is non-archimedean. So

$$\log^+ \max_{1\le i\le n} \|y_i\|_v \le \log^+ \|x_{p,q}\|_v \le \sum_{j=1}^{m} \log^+ \max_{1\le i\le n} \|x_{j,i}\|_v.$$

Proof of (2): If v is real (so $n_v = 1$): In this case $\|\cdot\|_v = |\cdot|_v$, so the triangle inequality is true for $\|\cdot\|_v$. Hence

$$\log^+ \max_{1\le i\le n} \|y_i\|_v \le \log^+ \max_{1\le i\le n} \sum_{j=1}^{m} \|x_{j,i}\|_v \le \log^+ \sum_{j=1}^{m} \max_{1\le i\le n} \|x_{j,i}\|_v \overset{\text{Claim}}{\le}$$

$$\overset{\text{Claim}}{\le} \log(m) + \sum_{j=1}^{m} \log^+ \max_{1\le i\le n} \|x_{j,i}\|_v.$$

Bitte wenden!

If v is non-real (so $n_v = 2$): In this case $\|\cdot\|_v = |\cdot|_v^2$. (Warning: the triangle inequality is true for $|\cdot|_v$, but not for $\|\cdot\|_v$! E.g. $\|1+1\|_v = \|2\|_v = 4 \not\leq 2 = \|1\|_v + \|1\|_v$.) Using the Cauchy-Schwarz inequality, we get

$$\|y_i\|_v = |y_i|_v^2 \leq \left(\sum_{j=1}^m |x_{j,i}|_v\right)^2 \leq m \sum_{j=1}^m |x_{j,i}|_v^2 = m \sum_{j=1}^m \|x_{j,i}\|_v.$$

Then

$$\log^+ \max_{1\leq i\leq n} \|y_i\|_v \leq \log^+ \left(m \max_{1\leq i\leq n} \sum_{j=1}^m \|x_{j,i}\|_v\right).$$

Using the claim from c), we get the bound $\log(m) + \log^+ \max_i \sum_j \|x_{j,i}\|_v$ for the right hand side. So

$$\begin{aligned}\log^+ \max_{1\leq i\leq n} \|y_i\|_v &\leq \log(m) + \log^+ \max_{1\leq i\leq n} \sum_{j=1}^m \|x_{j,i}\|_v \leq \\ &\leq \log(m) + \log^+ \sum_{j=1}^m \max_{1\leq i\leq n} \|x_{j,i}\|_v \overset{\text{Claim}}{\leq} \\ &\overset{\text{Claim}}{\leq} 2\log(m) + \sum_{j=1}^m \log^+ \max_{1\leq i\leq n} \|x_{j,i}\|_v.\end{aligned}$$

2. Let K be a number field such that $x \in K$ and $K/\mathbb{Q}$ is Galois. We fix an embedding $K \hookrightarrow \mathbb{C}$, so we may think of K as a subfield of $\mathbb{C}$. Let $d = [K:\mathbb{Q}]$. By definition $h(x) = \frac{1}{d}\sum_v \log^+ \|x\|_v$, so $h(x) = 0 \Leftrightarrow \|x\|_v \leq 1$ for every place v of K. If x is a root of unity, then $x^N = 1$ for some $N \in \mathbb{Z}_{\geq 1}$. Then $\|x\|_v^N = \|x^N\|_v = \|1\|_v = 1$, so $\|x\|_v = 1$ for every v, hence $h(x) = 0$.

Now suppose $h(x) = 0$. Let $A = \{\alpha \in K; h(\alpha) = 0\}$. We claim that $|A| < \infty$. The statement follows from this claim, because $1, x, x^2, x^3, \ldots \in A$, so there are $i < j$ such that $x^i = x^j$, hence $x^{j-i} = 1$. Let $\alpha \in A$, then $\|\alpha\|_v \leq 1$ for every v. Let $f_\alpha(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in \mathbb{Q}[X]$ be the minimal polynomial of X over $\mathbb{Q}$. The fractional ideal (α) has a decomposition $(\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\alpha)}$, and $1 \geq \|\alpha\|_{\mathfrak{p}} = p^{-f_{\mathfrak{p}}\,\mathrm{ord}_{\mathfrak{p}}(\alpha)}$ for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, so $\mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0$. Then $(\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\alpha)} \subseteq \mathcal{O}_K$, hence $\alpha \in \mathcal{O}_K$. This means that $f_\alpha \in \mathbb{Z}[X]$. Let $f_\alpha(X) = (X-\alpha_1)\cdots(X-\alpha_r)$, then $\alpha_1, \ldots, \alpha_r \in K$ (since $K/\mathbb{Q}$ is Galois), and in fact $\alpha_1, \ldots, \alpha_r \in A$, since these are conjugates of α. So as a complex number, each α_i has absolute value at most 1. Note that $r \leq [K:\mathbb{Q}] = d$. Since $\pm a_i$ is a symmetric polynomial of $\alpha_1, \ldots, \alpha_r$, we have $|a_i| \leq 2^r \leq 2^d$. So each coefficient of $f_\alpha(X)$ is in $\{-2^d, \ldots, 2^d\}$, and $\deg(f_\alpha(X)) \leq d$, so there are at most $(2^{d+1}+1)^{d+1}$ possible polynomials that f_α can be. Each of these polynomials has at most d zeros, so $|A| \leq d(2^{d+1}+1)^{d+1} < \infty$.

Siehe nächstes Blatt!

3. We first recall the situation in Lecture 5:

- k and C are big positive integers. (It becomes clear during the proof how big these have to be.)
- $K \subseteq \mathbb{C}$ is a number field, $\alpha_1, \dots, \alpha_n \in K^\times$, $b_1, \dots, b_n \in \mathbb{Z}$, $b_n \neq 0$.
- $B \geq \max\{2, |b_1|, \dots, |b_n|\}$.
- $\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n$, where $\Lambda \neq 0$ and $|\Lambda| \leq B^{-C}$.
- $h = \lfloor \log(kB) \rfloor$, $L = \lfloor k^{\frac{n}{n+1}} \log k \rfloor$.
- $\gamma_j = \lambda_j - \frac{b_j}{b_n}\lambda_n$ for $j \in \{1, \dots, n-1\}$.
- $$\Phi(z_0, \dots, z_{n-1}) = \sum_{0 \leq \lambda_{-1} \leq h-1} \sum_{0 \leq \lambda_0, \dots, \lambda_n \leq L} p(\lambda)\Delta(z_0 + \lambda_{-1}, h, \lambda_0 + 1, 0) \prod_{j=1}^{n-1} \alpha_j^{\gamma_j z_j},$$

  where $p(\lambda) \in K$, not all zero, such that $H(p(\lambda)) = e^{h(p(\lambda))} \leq c_1^{hk}$ for all λ for some constant $c_1 > 1$ (here c_1 depends only on K, n, $\alpha_1, \dots, \alpha_n$). So in particular $|p(\lambda)| \leq c_1^{hk}$.
- $m_0, \dots, m_{n-1} \in \mathbb{Z}_{\geq 0}$ such that $m_0 + \cdots + m_{n-1} < k$.
- $D_0 = \frac{d}{dz_0}$, $D_j = (\log \alpha_j)^{-1} \frac{d}{dz_j}$ for $j \in \{1, \dots, n-1\}$.
- $f(z) = \frac{1}{m_0!} D_0^{m_0} D_1^{m_1} \cdots D^{m_{n-1}} \Phi(z_0, \dots, z_{n-1})|_{z_0 = \cdots = z_{n-1} = z}$.
- $g(z) = \sum_\lambda p(\lambda)\Delta(z + \lambda_{-1}, h, \lambda_0 + 1, m_0) \left(\prod_{j=1}^{n-1} \gamma_j^{m_j}\right) \left(\prod_{j=1}^{n} \alpha_j^{\lambda_j z}\right)$.

Recall that $\Delta(z, k) = \frac{(z+1)\cdots(z+k)}{k!}$ and $\Delta(z, k, l, m) = \frac{1}{m!}(\frac{d}{dz})^m(\Delta(z, k)^l)$. We have proved in the lecture that $|\Delta(z, k, l, m)| \leq e^{(|z|+k)l}$.

Calculating the differentials in the definition of $f(z)$, we get that

$$f(z) = \sum_\lambda p(\lambda)\Delta(z + \lambda_{-1}, h, \lambda_0 + 1, m_0) \left(\prod_{j=1}^{n-1} \gamma_j^{m_j}\right) \left(\prod_{j=1}^{n-1} \alpha_j^{\gamma_j z}\right). \tag{3}$$

The number of terms in the sum is at most $h(L+1)^{n+1} \leq h(2L)^{n+1} \leq (hk)^{n+1} \leq c_2^{hk}$. We will give a bound for every term. First of all, $|p(\lambda)| \leq c_1^{hk}$ and

$$|\Delta(z + \lambda_{-1}, h, \lambda_0 + 1, m_0)| \leq e^{(|z+\lambda_{-1}|+h)(\lambda_0+1)} \leq e^{(|z|+2h)(L+1)} \leq e^{4(hk+L|z|)} \leq \\ \leq c_3^{hk+L|z|}.$$

Bound for $\left|\prod_{j=1}^{n-1} \gamma_j^{m_j}\right|$: If $j \in \{1, \dots, n-1\}$, then $|\gamma_j| = |\lambda_j - \frac{b_j}{b_n}\lambda_n| \leq L + BL \leq 2LB \leq 2kB \leq c_4^h$, therefore $\left|\prod_{j=1}^{n-1} \gamma_j^{m_j}\right| \leq (c_4^h)^{m_1 + \cdots + m_{n-1}} \leq c_4^{hk}$.

Bitte wenden!

Bound for $\left|\prod_{j=1}^{n-1} \alpha_j^{\gamma_j z}\right|$: Here we could just use the upper bound $|\gamma_j| \leq 2kB$, however this would not give a good enough bound. Instead we use that $\gamma_j = \lambda_j - \frac{b_j}{b_n}\lambda_n$:

$$\begin{aligned}\prod_{j=1}^{n-1} \alpha_j^{\gamma_j z} &= \left(\prod_{j=1}^{n-1} \alpha_j^{\lambda_j z}\right) \exp\left(-\frac{\lambda_n}{b_n} z \sum_{j=1}^{n-1} b_j \log \alpha_j\right) = \\ &= \left(\prod_{j=1}^{n-1} \alpha_j^{\lambda_j z}\right) \exp\left(-\frac{\lambda_n}{b_n} z(\Lambda - b_n \log \alpha_n)\right) = \\ &= \left(\prod_{j=1}^{n} \alpha_j^{\lambda_j z}\right) e^{-\frac{\lambda_n}{b_n}\Lambda z}\end{aligned} \tag{4}$$

Let $c_5 = \max\{|\log \alpha_1|, \ldots, |\log \alpha_n|\}$, then

$$\left|\prod_{j=1}^{n} \alpha_j^{\lambda_j z}\right| \leq e^{c_5 \lambda_j |z|} \leq e^{c_5 L|z|} \leq c_6^{L|z|}.$$

Finally $\left|e^{-\frac{\lambda_n}{b_n}\Lambda z}\right| \leq e^{L|\Lambda z|} \leq e^{L|z|}$, since $|\Lambda| \leq B^{-C} \leq 1$. So $\left|\prod_{j=1}^{n-1} \alpha_j^{\gamma_j z}\right| \leq c_6^{L|z|} e^{L|z|} \leq c_7^{L|z|}$.

Putting all the obtained bounds together, we get that

$$|f(z)| \leq c_2^{hk} \cdot c_1^{hk} \cdot c_3^{L|z|} c_3^{hk} \cdot c_4^{hk} \cdot c_7^{L|z|} \leq c_8^{hk+L|z|}.$$

4. We use the same notation as in the solution of exercise 3. Using equations (3) and (4) from the solution of exercise 3, we get that

$$f(l) = \sum_{\lambda} p(\lambda)\Delta(l + \lambda_{-1}, h, \lambda_0 + 1, m_0) \left(\prod_{j=1}^{n-1} \gamma_j^{m_j}\right) \left(\prod_{j=1}^{n} \alpha_j^{\lambda_j l}\right) e^{-\frac{\lambda_n}{b_n}\Lambda l}.$$

Recall that

$$g(l) = \sum_{\lambda} p(\lambda)\Delta(l + \lambda_{-1}, h, \lambda_0 + 1, m_0) \left(\prod_{j=1}^{n-1} \gamma_j^{m_j}\right) \left(\prod_{j=1}^{n} \alpha_j^{\lambda_j l}\right).$$

So

$$\begin{aligned}&f(l) - g(l) = \\ &= \sum_{\lambda} p(\lambda)\Delta(l + \lambda_{-1}, h, \lambda_0 + 1, m_0) \left(\prod_{j=1}^{n-1} \gamma_j^{m_j}\right) \left(\prod_{j=1}^{n} \alpha_j^{\lambda_j l}\right) \left(e^{-\frac{\lambda_n}{b_n}\Lambda l} - 1\right).\end{aligned}$$

Siehe nächstes Blatt!

We have seen in the solution of exercise 3, that the number of terms in the sum is at most c_2^{hk}, and

$$\left|p(\lambda)\Delta(l+\lambda_{-1},h,\lambda_0+1,m_0)\left(\prod_{j=1}^{n-1}\gamma_j^{m_j}\right)\left(\prod_{j=1}^{n}\alpha_j^{\lambda_j l}\right)\right| \leq$$
$$\leq c_1^{hk}c_3^{hk+Ll}c_4^{hk}c_6^{Ll} \leq c_9^{hk+Ll}.$$

Since $l < hk^{\frac{1}{2(n+1)}}(\log k)^{-1}$, we have here $Ll \leq k^{\frac{n}{n+1}}(\log k)\cdot hk^{\frac{1}{2(n+1)}}(\log k)^{-1} \leq hk$, thus $c_9^{hk+Ll} \leq c_{10}^{hk}$.

Now we only need to bound $\left|e^{-\frac{\lambda_n}{b_n}\Lambda l}-1\right|$. For this we use the bound $|e^z-1| \leq |z|e^{|z|}$, which was proved in the lecture. Now $z = -\frac{\lambda_n}{b_n}\Lambda l$, so $|z| \leq B^{-C}Ll \leq B^{-C}hk$. Here $hk \leq k\log(kB) \leq B^{C/4}$ for a big enough C (depending on K, n, $\alpha_1,\ldots,\alpha_n$, and also on k), and then $|z| \leq B^{-\frac{3}{4}C} \leq 1$. So

$$\left|e^{-\frac{\lambda_n}{b_n}\Lambda l}-1\right| = |e^z-1| \leq |z|e^{|z|} \leq e|z| \leq eB^{-\frac{3}{4}C}$$

for a big enough C.

Putting all the bounds together, and using $hk \leq k\log(kB)$, we get that

$$|f(l)-g(l)| \leq c_2^{hk}c_{10}^{hk}eB^{-\frac{3}{4}C} \leq e^{c_{11}hk}B^{-\frac{3}{4}C} \leq (kB)^{c_{11}k}B^{-\frac{3}{4}C}.$$

If C is big enough (depending on K, n, $\alpha_1,\ldots,\alpha_n$, and also on k), then $(kB)^{c_{11}k} \leq B^{\frac{1}{4}C}$, thus $|f(l)-g(l)| \leq B^{-\frac{1}{2}C}$.