Homework 12

The homeworks are due on the Thursday of the week after the assignment was posted online[1]. Please hand in your homework at the beginning of the tutorial or bring it to the lecture on Thursday morning. You can work on and submit your homework in groups of two. Please staple your pages and write your names and matriculation numbers on the first page.

Problem 34 (10 pts.)

Let $L \subset \mathbb{R}^n$ be a lattice of full rank (here we work with the standard inner product $\langle x, y\rangle = \sum_{i=1}^n x_i y_i$ on $\mathbb{R}^n$.)

a) Show that there is a matrix $A \in \mathrm{GL}_n(\mathbb{R})$ such that $L = A\mathbb{Z}^n$.

b) Show that if $L = A\mathbb{Z}^n$, then the dual lattice L' of L is given by $L' = A^*\mathbb{Z}^n$, where $A^* = (A^T)^{-1}$.

Solution. a) Let $v_1, \ldots, v_n \in \mathbb{R}^n$ be a basis of L, that is,

$$L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$$

and the v_i are linearly independent. Write $v_i = (v_{1,i}, v_{2,i}, \ldots, v_{n,i})^T \in \mathbb{R}^n$ and put

$$A = (v_1, v_2, \ldots, v_n) \in \mathbb{R}^{n\times n},$$

that is, the vectors v_i form the columns of A. Since the v_i are linearly independent, we have $A \in \mathrm{GL}_n(\mathbb{R})$. Moreover, if

$$x = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n \in L$$

with $a_i \in \mathbb{Z}$, then

$$x = A \cdot a$$

with $a = (a_1, a_2, \ldots, a_n)^T \in \mathbb{Z}^n$. Certainly, we also have $A\mathbb{Z}^n \subset L$, so that we can conclude $A\mathbb{Z}^n = L$.

b) We have $\lambda \in L'$ if and only if $\langle \lambda, y\rangle \in \mathbb{Z}$ for all $y \in L$ and this is equivalent to $\langle \lambda, Ax\rangle \in \mathbb{Z}$ for all $x \in \mathbb{Z}^n$. Since A^T is the dual of A with respect to $\langle\cdot,\cdot\rangle$, we have

$$\langle \lambda, Ax\rangle = \langle A^T\lambda, x\rangle.$$

We certainly have $\langle A^T\lambda, x\rangle \in \mathbb{Z}^n$ for all $x \in \mathbb{Z}^n$ if and only if $A^T\lambda \in \mathbb{Z}^n$, because clearly this is sufficient and it is easily seen to be necessary by taking $x = e_i$ the ith standard basis vector. We have $A^T\lambda \in \mathbb{Z}^n$ if and only if $\lambda \in (A^T)^{-1}\mathbb{Z}^n$, proving the claim. □

[1] This assignment is due Thursday, 16.01.20.

Problem 35 (10 pts.)

In this problem we prove some properties of Dirichlet characters that were already mentioned or used in class.

a) Show that the set G of Dirichlet characters $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}$ modulo m is a group with respect to multiplication.

b) Show that $|G| = \varphi(m)$.

c) Show that

$$\sum_{n \pmod m} \chi(n) = \begin{cases} \varphi(m) & \text{if } \chi = \chi^0, \\ 0 & \text{otherwise,} \end{cases}$$

where χ^0 denotes the trivial character modulo m.

Hints: For $\chi \neq \chi^0$, there exists $k \in \mathbb{Z}$ with $\gcd(k, m) = 1$, such that $\chi(k) \neq 1$. Then multiply the sum above by $\chi(k)$.

Solution. Parts a) and b) are easy to check and can be found in any number theory book, therefore we omit their full proofs here. As some hints for part b), it is easy to see that $\chi(1) = 1$. Further, by the fundamental theorem of finite abelian groups, the group of units $(\mathbb{Z}/m\mathbb{Z})^\times$ splits into a direct product of cyclic groups of the form $\mathbb{Z}/p_i^{h_i}\mathbb{Z}$, where $\prod h_i = \varphi(m)$ and p_i are primes dividing $\varphi(m)$. It is then easy to see that any character χ is uniquely defined on the generators of these cyclic groups, and that there will be in total exactly $\prod h_i = \varphi(m)$ possibilites for χ. c) If $\chi = \chi^0$, the claim is trivial. Otherwise, the claim follows again easily on noting that

$$\sum_{n \pmod m} \chi(n) = \sum_{n \pmod m} \chi(kn) = \chi(k) \sum_{n \pmod m} \chi(n),$$

since $(k, m) = 1$. Alternatively, by the observation from part b), the sum in question will equals the sum of all the $\varphi(m)$-th roots of unity, which is zero. $\square$

Problem 36 (10 pts.)

Poisson summation formula for finite groups. **Some definitions:** Let G be an arbitrary group. A complex-valued function f defined on G is called a *character* of G if f has the multiplicative property $f(ab) = f(a)f(b)$ for any $a, b \in G$ and if there exists some $c \in G$ with $f(c) \neq 0$. It is easy to see that if f is a character on a *finite* group G with identity e, then $f(e) = 1$ and each $f(a)$ is a root of unity. A *finite abelian* group G of order n has exactly n distinct characters. If multiplication of characters is defined by $(f_i f_j)(a) = f_i(a) f_j(a)$ for any $a \in G$, then the set of characters of G forms an abelian group of order n, which is usually denoted by $\widehat{G}$. Note that, alternatively but equivalently, $\widehat{G}$ is then the dual group of G, i.e., the set of homomorphisms $G \to S^1$ with the group law given by pointwise multiplication of functions.
If G is a finite abelian group, the *Fourier transform* of a function $f : G \to \mathbb{C}$ is the function $\widehat{f} : \widehat{G} \to \mathbb{C}$ given by

$$\widehat{f}(\chi) = \sum_{g \in G} f(g)\overline{\chi}(g).$$

One then has the *Fourier inversion formula*

$$f(x) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi(x),$$

which tells us how to recover f from its Fourier transform.

Your tasks: You **do not** need to prove anything up to here! Rather, just familiarize yourself with these notions. What you **do** need to prove is the following version of Poisson summation, and illustrate it by an example.

a) Let G be a finite abelian group and $H \subset G$ a subgroup. Show that for any function $f : G \to \mathbb{C}$ we have
$$\frac{1}{|H|} \sum_{h \in H} f(h) = \frac{1}{|G|} \sum_{\chi \in H^\perp} \widehat{f}(\chi),$$
where $H^\perp = \{\chi \in \widehat{G} : \chi = 1 \text{ on } H\}$.
Hints: You might want to use (and prove) the identities
$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \mathbf{1}_G, \\ 0 & \text{if } \chi \neq \mathbf{1}_G, \end{cases} \qquad \sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{if } g \neq 1, \end{cases}$$
and the *orthogonality relations*
$$\sum_{g \in G} \chi_1(g)\overline{\chi}_2(g) = \begin{cases} |G| & \text{if } \chi_1 = \chi_2, \\ 0 & \text{if } \chi_1 \neq \chi_2, \end{cases} \qquad \sum_{\chi \in \widehat{G}} \chi_1(g)\overline{\chi}_2(g) = \begin{cases} |G| & \text{if } g_1 = g_2, \\ 0 & \text{if } g_1 \neq g_2. \end{cases}$$
Try to prove that if $\delta_g : G \to \{0, 1\}$ is given by $\delta_g(x) = 1$ if $x = g$, and $\delta_g(x) = 0$ otherwise, then
$$\delta_g(x) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \overline{\chi}(g)\chi(x).$$
To prove the Poisson summation formula for f, it is then enough to verify it for δ_g.

b) Let $G = \mathbb{Z}/8\mathbb{Z}$ and $f : G \to \mathbb{C}$ be given by $f(0) = f(4) = 5$, $f(1) = f(5) = 3$ and $f(2) = f(3) = f(6) = f(7) = 1$. Compute the values $\widehat{f}(n)$.

Solution. a) Clearly every function $f : G \to \mathbb{C}$ can be written as a linear combination of delta-functions,
$$f = \sum_{g \in G} f(g)\delta_g,$$
therefore it is enough to verify the Poisson summation for δ_g. We distinguish two cases: If $g \in H$, then one needs to show that
$$\frac{1}{|H|} = \frac{1}{|G|} \sum_{\chi \in H^\perp} \widehat{\delta}_g(\chi) = \sum_{\chi \in H^\perp} \overline{\chi}(g),$$
which follows on checking the easy facts that $H^\perp \cong \widehat{(G/H)}$, $\widehat{G}/H^\perp \cong \widehat{H}$ and, in particular, that $|H^\perp| = [G : H]$. If $g \notin H$, then we need to show that
$$\sum_{\chi \in H^\perp} \widehat{\delta}_g(\chi) = \sum_{\chi \in H^\perp} \overline{\chi}(g) = 0.$$

But since certainly $g \neq 1$, then we know that $\sum_{\chi \in \widehat{G}} \chi(g) = 0$. Pick any $h \in H$, $h \neq 1$. Then $g^{-1}h \neq 1$, and $\sum_{\chi \notin H^\perp} \chi(g)\chi(g^{-1}h) = \sum_{\chi \notin H^\perp} \chi(h) = 0$, hence also $\sum_{\chi \notin H^\perp} \chi(g) = 0$, from where the conclusion follows.
b) By writing a cyclic group in the form $\mathbb{Z}/m\mathbb{Z}$, one can write an isomorphism with the character (dual) group explicitly:
Every (Dirichlet) character has the form $\chi_k : j \mapsto e^{2\pi i jk/m}$ for a unique $k \in \mathbb{Z}/m\mathbb{Z}$. The Fourier transform of a function $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ can then be regarded as a function not on $(\widehat{\mathbb{Z}/m\mathbb{Z}})$, but on $\mathbb{Z}/m\mathbb{Z}$:

$$\widehat{f}(k) := \sum_{j \in \mathbb{Z}/m\mathbb{Z}} f(j)\overline{\chi}_k(j) = \sum_{j \in \mathbb{Z}/m\mathbb{Z}} f(j)e^{-2\pi i jk/m}.$$

On the values $0, 1, \ldots, 7$, the Fourier transform $\widehat{f}$ takes then, in order, the values: $20, 0, 8 + 4i, 0, 4, 0, 8 - 4i, 0$. $\square$