Mathematics 666 **Homework (due Sep. 10)** A. Hulpke

You are welcome to use a computer for any routine calculations (as long as they do not render a problem trivial), e.g. in linear algebra. (You do not need to show the calculations, but can simply quote the result.)

6) Let A be the group algebra $\mathbb{Q}S_3$ and let

$$\begin{aligned} e_1 &= \frac{1}{6}\Big(1+(2,3)+(1,2)+(1,2,3)+(1,3,2)+(1,3)\Big)\\ e_2 &= \frac{1}{6}\Big(1-(2,3)-(1,2)+(1,2,3)+(1,3,2)-(1,3)\Big)\\ e_3 &= \frac{1}{3}\Big(2-(1,2,3)-(1,3,2)\Big)\end{aligned}$$

a) Show that $1 = e_1 + e_2 + e_3$, and $e_i^2 = e_i$, $e_i e_j = 0$ for $1 \le i, j \le 3$, $i \ne j$.
Hint: In GAP, you can calculate in the group algebra in the following way:

```
gap> A:=GroupRing(Rationals,SymmetricGroup(3));;
gap> b:=BasisVectors(Basis(A));
[ (1)*(), (1)*(2,3), (1)*(1,2), (1)*(1,2,3), (1)*(1,3,2), (1)*(1,3) ]
gap> e1:=1/6*(b[1]+b[3]+b[6]+b[2]+b[4]+b[5]);
```

b) Verify (by explicit calculation. Note that a basis is sufficient) that for all i and for all $a \in A$ we have that $ae_i = e_i a$.
Your solution to parts a) and b) can be simply a transcript of GAP calculations.
c) We set $A_i = Ae_i = \{a \cdot e_i \mid a \in A\}$. Show that A_i is an A-module by right multiplication with elements of A and that $A_A = A_1 \oplus A_2 \oplus A_3$ is a decomposition of A_A as a direct sum of A modules. (We will see later in the course that there always is such a decomposition, and that there is exactly one summand for each irreducible representation. The e_i are called central, orthogonal idempotents.)

7) Consider the group algebra $\mathbb{Q}S_3$. We have seen in class that S_3 has (at least) three inequivalent irreducible representations, in dimensions 1, 1, and 2.
a) For each (type of) irreducible representation, find (e.g. give generators) a submodule $M <_{\mathbb{Q}S_3} \mathbb{Q}S_3$ of the regular module, such that the quotient is isomorphic to the respective module.
b) Show that there are two (different) submodules $M_1, M_2 <_{\mathbb{Q}S_3} \mathbb{Q}S_3$ of the regular module, whose quotient is isomorphic to the 2-dimensional representation.
c) Construct (e.g. by intersecting the submodules you have found) a composition series for the regular module and conclude that S_3 has exactly three irreducible representations.

8) Let $i = \sqrt{-1}$ and $G = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\rangle$ be the quaternion group of order 8. (You can create it in GAP as

```
Group([ [ [ 0, 1 ], [ -1, 0 ] ], [ [ E(4), 0 ], [ 0, -E(4) ] ] ])
```

for example and ask for its `Elements`.)
a) Construct an irreducible representation of G over the real numbers, acting on a 4-dimensional vectorspace $V \cong \mathbb{R}^4$.
(**Hint:** Use an $\mathbb{R}$-basis of $\mathbb{C}$ to get an $\mathbb{R}$-basis of $\mathbb{C}^2$. To show that no 2-dimensional submodule exists, consider images of a nonzero vector (a, b, c, d) in this subspace under different elements of G, and show that they will yield a basis of at least a 3-dimensional subspace.)
b) Determine the endomorphism ring $\mathrm{End}_{\mathbb{R}G}(V)$.
(**Hint:** The elements of $\mathrm{End}_{\mathbb{R}G}(V)$ are 4×4 matrices that commute with the generators of G. Use this to deduce conditions on their entires. Then show that every matrix fulfilling these conditions commutes with G.)
c) By Schur's lemma $\mathrm{End}_{\mathbb{R}G}(V)$ must be a division ring. Can you identify it?

9) Let $M \in \mathrm{GL}_n(\mathbb{C})$. We consider M as the image of a generator in a representation of the infinite cyclic group. Let $V = \mathbb{C}^n$ be the module associated to this representation. Show that V is a cyclic module (i.e. it is generated as a module by a single vector) if and only if the characteristic polynomial of M equals the minimal polynomial of M.

10) (*Wedderburn's little theorem*) We want to prove that every finite division ring is a field.
For this, consider a minimal counterexample A. Let $Z(A) = \{a \in A \mid ab = ba \forall b \in A\}$.
a) Indicate why $Z(A)$ is a field and A a vector space over $Z(A)$ of finite dimension n. Setting $q = |Z(A)|$ we thus have $|A| = q^n$
b) Consider the class equation for the multiplicative group

$$|A^*| = q^n - 1 = q - 1 + \sum_r \frac{q^n - 1}{|C_{A^*}(r)|}$$

with r running over representatives of the non-central classes. Show that $C_{A^*}(r) \cup \{0\}$ is a field and thus $|C_{A^*}(r)| = q^m - 1$ for $m < n$.
c) Deduce that $\Phi_n(q) \mid q - 1$ where Φ_n is the n-th cyclotomic polynomial.
d) Show that for $q \in \mathbb{Z}$, $q \geq n$ and ζ a primitive n-th root of unity we have that $|q - \zeta| > |q - 1|$, leading to a contradiction.