Representation theory

Prof. Hendrik Lenstra*

Do not hand in solutions to problems that you consider trivial (unless too few are left). Do hand in the solutions to the hardest problems you can actually solve.

Theorem 1 (Frobenius, 1901)**.** *Let G be a group acting transitively on a finite set X such that for all $\sigma \in G \setminus \{1\}$ one has $\#\{x \in X : \sigma x = x\} \leq 1$. Then*

$$N = \{1\} \cup \{\sigma \in G : \forall x \in X : \sigma x \neq x\}$$

is a (normal) subgroup of G.

A group G is called a *Frobenius group* if an X and an action as in the theorem exist with $\#X \geq 2$ and the additional property that there are $\sigma \in G \setminus \{1\}$ and $x \in X$ with $\sigma x = x$; also, N is called the *Frobenius kernel* of G, and $\#X$ is called the *degree*.

Exercise L.1. Let G, X, N be as in the theorem of Frobenius, with $n = \#X \geq 2$.

(a) Prove: $\#N = n$.

(b) Suppose N is a subgroup. Prove: N is normal, and N acts transitively on X.

(c) Prove: $\#G = nd$ for some divisor d of $n - 1$.

Exercise L.2. Show by means of an example that the condition that X is finite cannot be omitted from Frobenius' theorem.

Exercise L.3. (a) Let R be a ring, $I \subset R$ a left ideal of finite index, and H a subgroup of the group R^* of units of R such that for all $a \in H \setminus \{1\}$ one has $R = (a-1)R + I$. Prove that $X = R/I$ and $G = \{\sigma : X \to X :$ there exist $a \in H$, $b \in R$: for all $x \in R : \sigma(x \bmod I) = (ax + b \bmod I)\}$ satisfy the conditions of Frobenius' theorem. What is N?

(b) Show how to recover the examples D_n (n odd) from (a).

*Exercises from lectures at Vrije Universiteit (Free University) Amsterdam, Fall 2010, by Gabriele Dalla Torre, gabrieledallatorre@gmail.com

Exercise L.4. (a) Apply Exercise L.3 to the subring $R = \mathbb{Z}[i, j]$ of the division ring $\mathbb{H} = \mathbb{R} + \mathbb{R} \cdot i + \mathbb{R} \cdot j + \mathbb{R} \cdot ij$ of quaternions to construct a Frobenius group G of order $8 \cdot 9$ and degree 9 such that G contains the quaternion group $Q = \langle i, j \rangle$ of order 8.

(b) Apply Exercise L.3 to $R = \mathbb{Z}[i, (1 + i + j + ij)/2]$ to construct a Frobenius group of order $24 \cdot 25$ and degree 25 that contains Q.

Exercise L.5*. Can you think of an example of a Frobenius group whose Frobenius kernel is non-abelian?

Exercise L.6. (a) Let R be a ring. Prove that there is a unique ring homomorphism $\mathbb{Z} \to R$.

(b) Let M be an abelian group. Prove that M has a unique $\mathbb{Z}$-module structure.

Exercise L.7 Chinese reminder theorem. (a) Let R be a commutative ring, $t \in \mathbb{Z}_{\geq 2}$, and let $I_1, \ldots, I_t$ be ideals of R such that for any two distinct indices i, j one has $I_i + I_j = R$. Prove that $\bigcap_{i=1}^t I_i = \prod_{i=1}^t I_i$, and show that the ring $R/\prod_{i=1}^t I_i$ is isomorphic to the product ring $\prod_{i=1}^t R/I_i$.

(b) Let the commutativity assumption on R in (a) be dropped, and interpret "ideal" to mean "two-sided ideal". Show how one can replace the product ideal by a suitable sum of product ideals so that the statements in (a) remain correct.

Exercise L.8. Let R be a ring, M an R-module, and $x \in M$. Write $\operatorname{Ann} x = \{r \in R : rx = 0\}$ (the *annihilator* of x), and $Rx = \{rx : r \in R\} \subset M$.

(a) Prove that $\operatorname{Ann} x$ is a left ideal of R, that Rx is a sub-R-module of M, and that there is an isomorphism $R/\operatorname{Ann} x \cong Rx$ of R-modules.

(b) We call M *cyclic* (as an R-module) if there exists $x \in M$ with $M = Rx$. Prove: M is cyclic if and only if there exists a left ideal $I \subset R$ with $M \cong R/I$.

Exercise L.9. (a) Let R be a domain, i. e. a commutative ring with $1 \neq 0$ without zero-divisors, and let M be an R-module. A *torsion element* of M is an element $x \in M$ with $\operatorname{Ann} x \neq \{0\}$ (see Exercise L.8). Prove that the set M_{tor} of torsion elements is a submodule of M.

(b) Give an example of a ring R and an R-module M for which $\{x \in M : \operatorname{Ann} x \neq \{0\}\}$ is not a submodule of M.

Exercise L.10. Let k be a field, and denote by R the ring $\{\left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right) : a, b, c \in k\}$ of lower-triangular 2×2-matrices over k. In this exercise all R-modules are described.

(a) Let V and W be k-vector spaces, and let $f \colon V \to W$ be a k-linear map. Prove that the group $V \oplus W$ is an R-module with multiplication $\left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right) \cdot (v, w) = (av, b \cdot f(v) + cw)$ (for $a, b, c \in k$, $v \in V$, $w \in W$).

(b) Prove that, up to isomorphism, any R-module is obtained as in (a).

Exercise L.11. Let $\mathbb{Q}[X]$ be the polynomial ring in one indeterminate X over the field $\mathbb{Q}$ of rational numbers, and let M be the $\mathbb{Q}$-vector space consisting of all sequences $(a_i)_{i=0}^{\infty} = (a_0, a_1, a_2, \ldots)$ of elements a_i of $\mathbb{Q}$. Make M into a $\mathbb{Q}[X]$-module by putting

$$X \cdot (a_0, a_1, a_2, \ldots) = (a_1, a_2, a_3, \ldots).$$

Let $(F_i)_{i=0}^{\infty} = (F_0, F_1, F_2, \ldots) = (0, 1, 1, 2, 3, 5, 8, 13, \ldots)$ be the sequence of *Fibonacci numbers*, defined by $F_0 = 0$, $F_1 = 1$, $F_{i+2} = F_{i+1} + F_i$ $(i \geq 0)$. Prove that $\operatorname{Ann}\big((F_i)_{i=0}^{\infty}\big)$ is the $\mathbb{Q}[X]$-ideal generated by $X^2 - X - 1$.

Exercise L.12. Let A be one of the groups $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/12\mathbb{Z}$, and let B be one of the groups $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/18\mathbb{Z}$. To which 'known' group is $\operatorname{Hom}_{\mathbb{Z}}(A, B)$ isomorphic? Motivate all your nine answers.

Exercise L.13. Let R, S, T be rings, let M be an R-S-bimodule, and let N be an R-T-bimodule. Exhibit an S-T-bimodule structure on the group ${}_R\operatorname{Hom}(M, N)$ of R-linear maps $M \to N$.

Exercise L.14. Let R_1 and R_2 be rings, and let R be the ring $R_1 \times R_2$. Let L_i and M_i be R_i-modules, for $i = 1, 2$, and define the R-modules L and M by $L = L_1 \times L_2$ and $M = M_1 \times M_2$. Prove that there is a bijective map $\operatorname{Hom}_{R_1}(L_1, M_1) \times \operatorname{Hom}_{R_2}(L_2, M_2) \to \operatorname{Hom}_R(L, M)$ sending the pair (f_1, f_2) to the map $f \colon L \to M$ defined by $f(x_1, x_2) = (f_1(x_1), f_2(x_2))$ (for $x_1 \in L_1$, $x_2 \in L_2$).

Exercise L.15. Let $G = \langle \sigma \rangle$ be a group of order 2, and let $\mathbb{Z}[G]$ be the group ring of G over the ring $\mathbb{Z}$ of integers. For a $\mathbb{Z}[G]$-module M, write $M_+ = \{x \in M : \sigma x = x\}$ and $M_- = \{x \in M : \sigma x = -x\}$. Prove: for every $\mathbb{Z}[G]$-module M there is an exact sequence

$$0 \to L \to M_+ \oplus M_- \to M \to N \to 0$$

of $\mathbb{Z}[G]$-modules, where the middle arrow sends (x, y) to $x + y$, and where L and N are $\mathbb{Z}[G]$-modules with $L = L_+ = L_-$ and $N = N_+ = N_-$.

Can you find an example of a $\mathbb{Z}[G]$-module M for which L and N are both non-zero?

Exercise L.16. Let A be the abelian group $\prod_p \mathbb{Z}/p\mathbb{Z}$, and let B be the subgroup $\bigoplus_p \mathbb{Z}/p\mathbb{Z}$ of A; in both cases, p ranges over the set of primes. Let C be the abelian group A/B.

(a) Prove: for each positive integer n, the map $C \to C$ sending x to nx is bijective.

(b) Prove: the group C has a module structure over the field $\mathbb{Q}$ of rational numbers.

Exercise L.17. Let A be the ring $\prod_p \mathbb{F}_p$ with componentwise ring operations, the product ranging over all prime numbers p.

(a) Prove that A contains $\mathbb{Z}$ as a subring.

(b) Let $R = \{a \in A: \text{ there exists } n \in \mathbb{Z},\ n \neq 0, \text{ such that } na \in \mathbb{Z}\}$. Prove that R is a subring of A, and that there is an exact sequence of abelian groups

$$0 \to \bigoplus_p \mathbb{F}_p \to R \to \mathbb{Q} \to 0.$$

Does this sequence split?

Exercise L.18. Let R be a ring. The *opposite* ring R^{opp} has the same underlying additive group as R, but with multiplication $*$ defined by $a*b = ba$, for $a, b \in R^{\text{opp}}$.

(a) Prove that, for every positive integer n and every commutative ring A, the ring $M(n, A)$ of $n \times n$-matrices over A is isomorphic to its opposite.

(b) * Is every ring isomorphic to its opposite? Give a proof or a counterexample.

Exercise L.19. Let I be an infinite set, for each $i \in I$ let R_i be a non-zero ring, and let R be the product ring $\prod_{i \in I} R_i$. Construct an R-module M that is not isomorphic to an R-module of the form $\prod_{i \in I} M_i$, with each M_i being an R_i-module and $R = \prod_{i \in I} R_i$ acting componentwise on $\prod_{i \in I} M_i$.

Exercise L.20. (This exercise counts for two). Prove the structure theorem for finitely generated modules over a principal ideal domain.

Exercise L.21. Let R be a ring. In class we defined two R-modules to be *Jordan-Hölder isomorphic* if they have isomorphic chains of submodules. Prove that this is an equivalence relation on the class of all R-modules.

Exercise L.22. Are $\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/75\mathbb{Z})$ and $\mathbb{Z} \times (\mathbb{Z}/14\mathbb{Z})$ Jordan-Hölder isomorphic as $\mathbb{Z}$-modules? Motivate your answer.

Exercise L.23. Are $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ Jordan-Hölder isomorphic as $\mathbb{Z}$-modules? Motivate your answer.

Exercise L.24. Let R be a ring, and let M be an R-module of finite length with composition series $(M_i)_{i=0}^{l(M)}$. 'The' *semisimplification* M_{ss} of M is the R-module

$$M_{\text{ss}} = \bigoplus_{i=1}^{l(M)} (M_i/M_{i-1}).$$

Prove: M and its semisimplification are Jordan-Hölder isomorphic.

Exercise L.25. Let R be a ring, let K, L, M, N be R-modules, and let $f\colon K \to L$, $g\colon L \to M$, $h\colon M \to N$ be R-linear maps such that $h \circ g \circ f = 0$ (the zero map). Construct an exact sequence

$$0 \to \ker f \to \ker(g \circ f) \to \ker g \to \big(\ker(h \circ g)\big)/\operatorname{im} f \to$$

$$(\ker h)/\operatorname{im}(g \circ f) \to \operatorname{cok} g \to \operatorname{cok}(h \circ g) \to \operatorname{cok} h \to 0$$

of R-modules, where ker denotes kernel, im denotes image, and cok denotes cokernel.

This result is often called the *snake lemma.* Can you see why?

Exercise L.26. (a) Let $n \in \mathbb{Z}_{>0}$, and let $1 \to A_1 \to A_2 \to \ldots \to A_n \to 1$ be an exact sequence of groups. Suppose that all A_i with at most one exception are finite. Prove that they are all finite, and that one has $\prod_{i=1}^n (\#A_i)^{(-1)^i} = 1$.

(b) Let $n \in \mathbb{Z}_{>0}$, and let $A_0 \to A_1 \to \ldots \to A_n \to A_0$ be an exact sequence of groups such that the kernel of the first map equals the image of the last. Suppose that all A_i with at most one exception are finite. Prove that they are all finite, that $\prod_{i=0}^n \#A_i$ is the square of some integer, and that for odd n one has $\prod_{i=0}^n (\#A_i)^{(-1)^i} = 1$.

Exercise L.27. (a) Let R be the ring from Exercise L.17. Prove that the multiplication map $R \times R \to R$ induces an isomorphism $R \otimes_{\mathbb{Z}} R \to R$.

(b) Let M be an R-R-bimodule. Prove that for all $r \in R$ and $m \in M$ one has $rm = mr$.

Exercise L.28. Let A, B, C be groups. A map $f\colon A \times B \to C$ is called *bilinear* if for all α, $\alpha' \in A$ and β, $\beta' \in B$ one has $f(\alpha\alpha', \beta) = f(\alpha, \beta) \cdot f(\alpha', \beta)$ and $f(\alpha, \beta\beta') = f(\alpha, \beta) \cdot f(\alpha, \beta')$.

(a) Suppose $f\colon A \times B \to C$ is bilinear. Prove that the subgroup of C generated by $f(A \times B)$ is abelian.

(b) Exhibit a bijection between the set of bilinear maps $A \times B \to C$ and the set of group homomorphisms $(A/[A, A]) \otimes_{\mathbb{Z}} (B/[B, B]) \to C$.

Exercise L.29. Let A and B be subgroups of a group G. Prove that the map $A \times B \to G$ sending (α, β) to the *commutator* $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}$ is bilinear (as defined in Exercise L.28) if and only if the image of this map is contained in the center of the subgroup of G generated by A and B.

Exercise L.30. Let n be an integer, A an additively written abelian group, and $n_A\colon A \to A$ the map $a \mapsto na$. Prove: $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} A \cong \operatorname{cok} n_A$.

Exercise L.31. A *torsion* group is a group of which every element has finite order. A group B is called *divisible* if for each $m \in \mathbb{Z}_{>0}$ and each $b \in B$ there exists $c \in B$ with $c^m = b$. Prove: if A and B are abelian groups such that A is torsion and B is divisible, then $A \otimes_{\mathbb{Z}} B = 0$.

Exercise L.32. Describe the group $A \otimes_{\mathbb{Z}} B$ when each of A and B is one of the following: (a) finite cyclic; (b) infinite cyclic; (c) the Klein four group; (d) the additive group $\mathbb{Q}$; and (e) $\mathbb{Q}/\mathbb{Z}$. (Be sure to cover all combinations.)

Exercise L.33. Construct a non-trivial abelian group A such that $A \otimes_{\mathbb{Z}} A = 0$. Can such a group be finitely generated?

Exercise L.34. Let A, B, C be additively written abelian groups, and let $f\colon A \times B \to C$ be a bilinear map that is also a group homomorphism. Prove that f is the zero map.

Exercise L.35. In this exercise, all tensor products are over $\mathbb{Z}$.

Is the tensor product of two finitely generated abelian groups finitely generated? Is the tensor product of two finite abelian groups finite? Give in each case a proof or a counterexample.

Exercise L.36. Suppose that A and B are non-zero finitely generated abelian groups. Prove: $A \otimes_{\mathbb{Z}} B = 0$ if and only if A and B are finite with $\gcd(\#A, \#B) = 1$.

Exercise L.37. Let k be a field, let V be the k-vector space k^2, and let $M_2(k)$ be the ring of 2×2-matrices over k. We view $M_2(k)$ as a k-vector space in the natural way. Define the map $f\colon V \times V \to M_2(k)$ by $f\big((a,b),(c,d)\big) = \left(\begin{smallmatrix} ac & ad \\ bc & bd \end{smallmatrix}\right)$.

(a) Prove that f is k-bilinear, and that the image of f consists of the set of 2×2-matrices over k of rank at most 1.

(b) Prove that the pair $\big(M_2(k), f\big)$ is a tensor product of V and V over k, as defined in class.

(c) Prove that not every element of $V \otimes_k V$ is of the form $x \otimes y$, with x, $y \in V$.

Exercise L.38. Let A and B be abelian groups.

(a) Prove: if at least one of A and B is cyclic, then every element of $A \otimes_{\mathbb{Z}} B$ is of the form $x \otimes y$, with $x \in A$, $y \in B$.

(b) Suppose A is finitely generated. Prove: A is cyclic if and only if every element of $A \otimes_{\mathbb{Z}} A$ is of the form $x \otimes y$, with x, $y \in A$.

Exercise L.39. Let A be an additively written abelian group. For $n \in \mathbb{Z}$, we write $nA = \{nx : x \in A\}$. Let $a \in A$.

(a) Prove: the element $a \otimes a$ of $A \otimes_{\mathbb{Z}} A$ equals 0 if there exists $n \in \mathbb{Z}$ with $na = 0$ and $a \in nA$.

(b) Is the statement in (a) valid with "if" replaced by "only if"? Give a proof or a counterexample.

Exercise L.40. Let S be a finite simple group. By an *S-degree* we mean a function that assigns to each finite separable field extension $k \subset l$ a positive rational number $[l:k]_S$ such that the following two axioms are satisfied:

(i) if $k \subset l$ is a Galois extension with a simple group G, then one has $[l:k]_S = [l:k]$ if $G \cong S$, and $[l:k]_S = 1$ if $G \ncong S$;

(ii) one has $[m:k]_S = [m:l]_S \cdot [l:k]_S$ whenever $k \subset l$ and $l \subset m$ are finite separable field extensions.

Prove that there exists a unique S-degree.

In the following three problems we let the S-degree $[l:k]_S$ of a finite separable field extension $k \subset l$ be as in the previous exercise.

Exercise L.41. Let $k \subset l$ be a finite separable field extension. Prove that, as S ranges over all finite simple groups up to isomorphism, all but finitely many of the numbers $[l:k]_S$ are equal to 1, and that one has

$$[l:k] = \prod_S [l:k]_S.$$

Exercise L.42. Let $k \subset l$ be a finite separable field extension. We call $k \subset l$ *solvable* if the Galois group of the Galois closure of $k \subset l$ is solvable.

(a) Prove: if $k \subset l$ is solvable, then one has $[l:k]_S = 1$ for every non-abelian finite simple group S.

(b) Suppose that $[l:k] = 5$, and that $k \subset l$ is not solvable. Determine $[l:k]_S$ for all finite simple groups S.

Exercise L.43. Let $k \subset l$ be a finite separable field extension.

(a) Suppose that m is a finite Galois extension of k inside some overfield of l, with $m \cap l = k$. Prove that for all finite simple groups S one has $[m \cdot l : m]_S = [l : k]_S$.

(b) Is the converse of Exercise L.42(a) true? Give a proof or a counterexample.

Exercise L.44. (This exercise counts for two). Let M be a $\mathbb{Z}$-module. Prove the following facts.

(a) The module M is semisimple if and only if every $x \in M$ has finite square-free order.

(b) The module M is injective if and only if it is divisible.

(c) The module M is projective if and only if it is free over $\mathbb{Z}$.

(d) If M satisfies two of the previous three properties, then $M = \{0\}$.

Exercise L.45. Let R be a ring. An R-module M is said to be of *finite length* if for some $t \in \mathbb{Z}_{\geq 0}$ it has a chain $\{0\} = M_0 \subset M_1 \subset \ldots \subset M_t = M$ of submodules for which each of the modules M_i/M_{i-1} $(0 < i \leq t)$ is simple.

(a) Two pairs (M, M') of (N, N') of R-modules of finite length are called *equivalent* if $M \oplus N'$ is Jordan-Hölder isomorphic to $M' \oplus N$ (see Exercise L.21). Prove that this is indeed an equivalence relation.

(b) We write $G_{\mathrm{fl}}(R)$ for the set of equivalence classes of the equivalence relation from (a). If M, M' are R-modules of finite length, then $[M, M'] \in G_{\mathrm{fl}}(R)$ denotes the class of the pair (M, M'), and we write $[M] = [M, \{0\}]$. Prove that there is a unique operation $+$ on $G_{fl}(R)$ that makes $G_{fl}(R)$ into an abelian group and satisfies the rules $[M] + [M'] = [M \oplus M']$ and $[M, M'] = [M] - [M']$ for any two R-modules M, M' of finite length.

Exercise L.46. Let R be a ring, and let $G_{fl}(R)$ be the abelian group defined in the previous exercise.

(a) Let $\mathcal{S}$ be a set of simple R-modules such that each simple R-module is isomorphic to exactly one element of $\mathcal{S}$. Prove that $([S])_{S\in\mathcal{S}}$ is a $\mathbb{Z}$-basis for $G_{fl}(R)$.

(b) Suppose R is a field. Prove: $G_{fl}(R) \cong \mathbb{Z}$ (as groups).

Exercise L.47. (a) Suppose that R is a ring that, when viewed as a module over itself, is of finite length. Prove that an R-module is finitely generated if and only if it is of finite length. Prove also that the group $G_{fl}(R)$ from Exercise L.45 is finitely generated.

(b) Prove that there is a group isomorphism from $G_{fl}(\mathbb{Z})$ with the multiplicative group $\mathbb{Q}^*_{>0}$ of positive rational numbers that, for each finite abelian group M, sends $[M]$ to $\#M$. Prove also that $G_{fl}(\mathbb{Z})$ is not finitely generated.

Exercise L.48. Let R be a semisimple ring, and let M, N be two finitely generated R-modules. Prove: M is isomorphic to N if and only if $[M] = [N]$ in $G_{fl}(R)$, the notation being as in Exercise L.45.

Exercise L.49. Let k be a field, let G be a group, and let M, N be $k[G]$-modules.

(a) Prove that the k-vector space structure on $M \otimes_k N$ can in a unique way be extended to a $k[G]$-module structure on $M \otimes_k N$ such that for all $\sigma \in G$, $x \in M$, $y \in N$ one has $\sigma(x \otimes y) = (\sigma x) \otimes (\sigma y)$.

(b) Prove that the k-vector space structure on $\mathrm{Hom}_k(M, N)$ can in a unique way be extended to a $k[G]$-module structure on $\mathrm{Hom}_k(M, N)$ such that for all $\sigma \in G$, $x \in M$, $f \in \mathrm{Hom}_k(M, N)$ one has $(\sigma f)(x) = \sigma f(\sigma^{-1}x)$.

Exercise L.50. Let k, G be as in the previous exercise. For a $k[G]$-module M, we write M^G for the k-vector space $\{x \in M : \text{for all } \sigma \in G \text{ one has } \sigma x = x\}$, and we write M_G for the k-vector space $M/\sum_{\sigma\in G}(\sigma - 1)M$. Let now M, N be $k[G]$-modules, and let $M \otimes_k N$ and $\mathrm{Hom}_k(M, N)$ be $k[G]$-modules as in the previous exercise.

(a) Prove: $\mathrm{Hom}_{k[G]}(M, N) = \mathrm{Hom}_k(M, N)^G$.

(b) Show how one can make M into a right $k[G]$-module by putting $x\sigma = \sigma^{-1}x$ for $\sigma \in G$, $x \in M$. Conclude that one define the k-vector space $M \otimes_{k[G]} N$. Prove also that $M \otimes_{k[G]} N$ is isomorphic to $(M \otimes_k N)_G$.

Exercise L.51. Let k, G be as in the previous exercise, and let M be a $k[G]$-module. Let $(e_i)_{i\in I}$ be a basis for M as a k-vector space. Prove that each of $(\sigma \otimes e_i)_{\sigma\in G, i\in I}$ and $(\sigma \otimes \sigma e_i)_{\sigma\in G, i\in I}$ forms a basis for $k[G] \otimes_k M$ as a k-vector space, and that $k[G] \otimes_k M$ is free when viewed as a $k[G]$-module (as in Exercise L.49).

Exercise L.52. Let k be a field and let G be a finite group.

(a) Prove that the abelian group $G_{fl}(k[G])$ from Exercise L.45 has a unique $\mathbb{Z}$-bilinear operation $\cdot \colon G_{fl}(k[G]) \times G_{fl}(k[G]) \to G_{fl}(k[G])$ such that for any two

$k[G]$-modules M, N of finite length one has $[M] \cdot [N] = [M \otimes_k N]$, where $M \otimes_k N$ is a $k[G]$-module as in Exercise L.49.

(b) Prove that the operation $\cdot$ from (a) makes $G_{fl}(k[G])$ into a commutative ring. This ring is called the *representation ring* of G over k, notation: $\mathcal{R}_k(G)$.

Exercise L.53. Let G be a finite abelian group, and let k be an algebraically closed field of characteristic not dividing $\#G$. Put $\hat{G} = \mathrm{Hom}(G, k^*)$. Prove that the representation ring $\mathcal{R}_k(G)$ is, as a ring, isomorphic to the group ring $\mathbb{Z}[\hat{G}]$.

Exercise L.54. (This exercise counts for two.) Denote by S_3 a non-abelian group of order 6. Let k be an algebraically closed field of characteristic not dividing 6. In this exercise we "compute" the representation ring $\mathcal{R}_k(S_3)$ as a ring.

(a) Prove that S_3 has three pairwise non-isomorphic irreducible representations over k: the trivial representation k, another one-dimensional representation coming from the sign map $S_3 \to \{1, -1\} \subset k^*$, and a two-dimensional representation.

(b) Write 1, ϵ, t (respectively) for the classes in $\mathcal{R}_k(S_3)$ of the three representations mentioned in (a). Prove that 1, ϵ, t form a basis of $\mathcal{R}_k(S_3)$ over $\mathbb{Z}$ and that 1 is the unit element of $\mathcal{R}_k(S_3)$.

(c) Express ϵ^2, ϵt and t^2 on the $\mathbb{Z}$-basis 1, ϵ, t.

(d) Determine all ring homomorphisms $\mathcal{R}_k(S_3) \to \mathbb{Z}$, and prove that $\mathcal{R}_k(S_3)$ is isomorphic to the subring $\{(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} : a \equiv b \bmod 2,\ b \equiv c \bmod 3\}$ of the ring $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ (with component-wise ring operations).

Exercise L.55. (This exercise also counts for two.) Choose a non-abelian group G of order 8, and let k be an algebraically closed field of characteristic different from 2. Describe $\mathcal{R}_k(G)$ as a subring of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, by proceeding as in the previous exercise.

Exercise L.56. (The converse of *Maschke's theorem.*) Let G be a finite group and let k be a field of characteristic dividing $\#G$. Prove that the ring $k[G]$ is not semisimple. (*Hint*: construct a short exact sequence of $k[G]$-modules that does not split.)

Exercise L.57. Let k be a field, let V, W be two finite-dimensional k-vector spaces, and let $f \in \mathrm{End}_k V$, $g \in \mathrm{End}_k W$. Prove: $\mathrm{Tr}(f \otimes g) = \mathrm{Tr}(f) \cdot \mathrm{Tr}(g)$. Here Tr denotes trace, and $f \otimes g$ is viewed as an element of $\mathrm{End}_k(V \otimes_k W)$.

Exercise L.58. Let k be a field. For a k-vector space V, write $V^\dagger$ for the dual k-vector space $\mathrm{Hom}_k(V, k)$.

Let V, W be two finite-dimensional k-vector spaces. Exhibit an isomorphism $V^\dagger \otimes_k W^\dagger \cong (V \otimes_k W)^\dagger$ of k-vector spaces. Your isomorphism should be $k[G]$-linear if G is a group for which V, W carry $k[G]$-structures; here the $k[G]$-module structures on the duals and on the tensor products are as in Exercise L.49, with G acting trivially on k.

Exercise L.59. Let G be a finite group, let k be an algebraically closed field of characteristic zero, and let M, N be finitely generated $k[G]$-modules. Suppose that for each $\sigma \in G$, there is an isomorphism between M and N when viewed as modules over the subring $k[\langle\sigma\rangle]$ of $k[G]$. Prove that M and N are isomorphic as $k[G]$-modules.

Exercise L.60. Denote by Q_8 the quaternion group of order 8.

(a) Prove: $\mathbb{C}[Q_8] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times M(2, \mathbb{C})$ (as rings).

(b) Denote by $\mathbf{R}$ the field of real numbers and by $\mathbb{H}$ the division ring of quaternions. Exhibit a ring isomorphism $\mathbf{R}[\mathbf{Q_8}] \cong \mathbf{R} \times \mathbf{R} \times \mathbf{R} \times \mathbf{R} \times \mathbb{H}$.

Exercise L.61. Let A_4 be the alternating group of order 12.

(a) Determine positive integers $n_1, \ldots, n_t$ such that $\mathbb{C}[A_4] \cong \prod_{i=1}^{t} M(n_i, \mathbb{C})$ (as rings).

(b) Describe all simple $\mathbb{C}[A_4]$-modules.

Exercise L.62. Let G be a finite group.

(a) Let k be a field, let M be a $k[G]$-module with $\dim_k M = 1$, and let N be a simple $k[G]$-module. Prove: the $k[G]$-module $M \otimes_k N$ is simple.

(b) Let $\mathbb{C}$ be the field of complex numbers. Prove: G is abelian if and only if for any two simple $\mathbb{C}[G]$-modules M and N the $\mathbb{C}[G]$-module $M \otimes_{\mathbb{C}} N$ is simple.

Exercise L.63. Let k be field. An *ordering* of k is a subset $P \subset k^*$ that is closed under addition and multiplication, with the property that for each $a \in k^*$ one has either $a \in P$ or $-a \in P$, but not both. Suppose that k has an ordering.

(a) Prove: $\operatorname{char} k = 0$.

(b) Prove: for every index set I the field $k(X_i : i \in I)$ of rational functions in the indeterminates X_i, $i \in I$, has an ordering.

Exercise L.64. Let k be field, with algebraic closure $\bar{k}$. A theorem of Artin and Schreier (1927) implies that for each $\rho \in \operatorname{Aut}_k \bar{k}$ of order 2 the set $P_\rho = \{\alpha \cdot \rho\alpha : \alpha \in \bar{k}^*\} \cap k^*$ is an ordering of k, as defined in the previous exercise. In addition, the map from the set of conjugacy classes of elements of order 2 in $\operatorname{Aut}_k \bar{k}$ to the set of orderings of k that sends the class of ρ to P_ρ is *bijective*. You may use these results in this exercise.

(a) Let K be an algebraically closed field. Prove: K has an automorphism of order 2 if and only if $\operatorname{char} K = 0$.

(b) Let K be an algebraically closed field, and let ρ be an automorphism of order 2 of K. Suppose that $t \in \mathbb{Z}_{\geq 0}$ and $\alpha_1, \ldots, \alpha_t \in K$ satisfy $\sum_{i=1}^{t} \alpha_i \cdot \rho(\alpha_i) = 0$. Prove: $\alpha_i = 0$ for each i.

(c) Let K and ρ be as in (b). Prove that for every root of unity $\zeta \in K$ one has $\rho(\zeta) = \zeta^{-1}$.

Exercise L.65. Let k be an algebraically closed field of characteristic zero, and let G be a finite group. For a finitely generated $k[G]$-module M, denote by $M^\dagger$ the $k[G]$-module $\mathrm{Hom}_k(M, k)$.

(a) Prove that the following two assertions about G are equivalent: (i) for every finitely generated $k[G]$-module M one has $M^\dagger \cong_{k[G]} M$; and (ii) every element of G is conjugate to its inverse.

(b) Suppose G has odd order, and $G \neq 1$. Prove that there exists an irreducible $k[G]$-module M with $M^\dagger \ncong_{k[G]} M$.

Exercise L.66. Prove that every finite group G can be embedded as a subgroup in a finite group H with the property that each element of H is conjugate to its inverse.