ALGEBRA II
ALGEBRA UND ZAHLENTHEORIE
PROSEMINAR WS 2014/15

1. Let $n \geq 2$. Determine the unit group and the set of zero-divisors of $\mathbb{Z}/n\mathbb{Z}$ an.

2. Let R be a Euclidean domain. Show that R is a principal ideal domain.

3. Let R be a ring and $I \triangleleft R$ an ideal. Desribe the ideals in the factor ring R/I.

4. Every noetherian domain is atomic.

5. Every principal ideal domain is factorial (use Lemma 1.5!).

6. A finite monoid is an abelian group, and a finite domain is a field.

7. Let H be a GCD-monoid. Then every $x \in \mathsf{q}(H)$ has a unique representation in the form $x = a^{-1}b$ where $a, b \in H$ and $\mathrm{GCD}(a, b) = H^{\times}$. Moreover, the classes $[a]_{\simeq}$ and $[b]_{\simeq}$ are uniquely determined by x.

8. Let $R = \mathbb{Z}[\sqrt{-5}]$, $a = 6$ and $b = 2(1 + \sqrt{-5})$. Then $\mathrm{GGT}(a, b) = \emptyset$.

9. Let R be a domain and $a \in R^{\bullet}$. Then a is a prime element if and only if aR is a prime ideal.

Let R be a commutative ring.

10. Find all simple abelian groups.

11. Let M be an R-module, $\mathrm{End}_R(M)$ its endomorphism ring and $R_M = \{\lambda \cdot \mathrm{id}_M \mid \lambda \in R\} \subset \mathrm{End}_R(M)$ the ring of homotheties of M. Then $R_M \cong R/\mathrm{Ann}_R(M)$.

12. Let M be an R-module.

(a) M is simple if and only if $M = Rx$ for all $0 \neq x \in M$.
(b) Give an example of a cyclic module which is not simple.
(c) If M simple, then $\mathrm{End}_R(M)$ is a division ring.

13. Let $n \in \mathbb{N}$.

(a) $\mathrm{End}_R(R^n) \cong M_n(R)$.
(b) For every prime $p \in \mathbb{N}$ we have $\mathrm{End}_{\mathbb{Z}}((\mathbb{Z}/p\mathbb{Z})^n) \cong M_n(\mathbb{Z}/p\mathbb{Z})$.
(c) For every R-module M we have $\mathrm{End}_R(M^n) \cong M_n(\mathrm{End}_R(M))$.

Hint: $f \mapsto (p_i \circ f \circ \epsilon_j)_{1,i,j \leq n}$

14. Let $I_1, \ldots, I_n \lhd R$ be ideals of R and let M be an R-module. Then the following statements are equivalent:

(a) $M \cong R/I_1 \oplus \cdots \oplus R/I_n$.
(b) There exist cyclic submodules $C_1, \ldots, C_n \subset M$ with $\mathrm{ann}_R(C_j) = I_j$ for all $j \in [1, n]$, such that $M = \oplus_{i=1}^n C_i$.

15. Give a proof of Lemma 2.8.

16. Let M be a free R-module of rank n and N a free R-module of rank m.

1. If $\boldsymbol{u} = (u_1, \dots, u_n)$ is a basis of $M, \boldsymbol{v} = (v_1, \dots, v_m)$ a basis of N and $\varphi \in \mathrm{Hom}_R(M,N)$, then there exists a unique matrix $\mathcal{M}_{\boldsymbol{u},\boldsymbol{v}}(\varphi) \in M_{m,n}(R)$ with $(\varphi(u_1), \dots, \varphi(u_n)) = (v_1, \dots, v_m)\mathcal{M}_{\boldsymbol{u},\boldsymbol{v}}(\varphi)$.
2. For every $A \in M_{m,n}(R)$, the map $\theta_A \colon R^n \to R^m$ with $\theta_A(x) = Ax$ is an R-module homomorphism.
3. The map $\kappa_{\boldsymbol{u}} \colon R^n \to M$ with $\kappa_{\boldsymbol{u}}(\boldsymbol{\lambda}) = \sum\limits_{i=1}^{n} \lambda_i u_i$ is an R-module isomorphism ($\kappa_{\boldsymbol{u}}$ ist die Koordinatenabbildung!).
4. The map
$$\mathcal{M}_{\boldsymbol{u},\boldsymbol{v}} \colon \begin{cases} \mathrm{Hom}\ _R(M,N) & \to \quad M_{m,n}(R) \\ \varphi & \mapsto \quad \mathcal{M}_{\boldsymbol{u},\boldsymbol{v}}(\varphi) \end{cases}$$
is an R-module isomorphism.

17. Let R be a domain with quotient field K, and let $M \subset K$ be an R-submodule. Then M is free if and only if M is cyclic.

18. Let $R = \mathbb{Z}[\sqrt{-5}]$ and $M = \langle 2, 1+\sqrt{-5} \rangle$ the R-module generated by 2 and $1+\sqrt{-5}$.

1. M is not a free R-module.
2. $M \times M$ is a free R-module of rank two.
   Hint: Show that $M \times M = \langle (2, 1+\sqrt{-5}), (1-\sqrt{-5}, 2) \rangle$.

19. Let M be an R-module.

1. If $\pi \colon M \to F$ is an R-module epimorphism onto a free module F and $(x_i)_{i \in I}$ a family in M whose image $(\pi(x_i)_{i \in I})$ is a basis of F, then
$$M = \mathrm{Ker}(\pi) \oplus \left(\oplus_{i \in I} R x_i \right).$$
Do we always have such a family $(x_i)_{i \in I}$?
2. (Basis Extension Theorem) If $N \subset M$ is a free submodule such that M/N is free, then each basis of N can be extended to a basis of M (give a precise formal formulation; the proof follows immediately from 1.).

20. Let M be a finitely generated free R-module, $N \subset M$ an R-submodule and $\varphi \in \mathrm{End}_R(M)$. If R is a field, then the following statements hold true:

1. N is free.
2. N is a direct summand of M.
3. If φ is a monomorphism, then φ is an epimorphism.
4. $\mathrm{rk}(M) = \mathrm{rk}(\mathrm{Ker}(\varphi)) + \mathrm{rk}(\mathrm{Im}(\varphi))$.

Do 1. - 4. hold true for general rings?

21. Let M be a noetherian R-module. Then $R/\mathrm{Ann}_R(M)$ is a noetherian ring.

Hint: Set $M =_R \langle x_1, \dots, x_n \rangle$; then $\mathrm{Ann}_R(M) = \bigcap_{i=1}^{n} \mathrm{Ann}_R(x_i)$; proceed by induction on n; use Theorem 2.34 to do the induction step.

22. Let R be a domain and M an R-module.

1. Then $M_{\mathrm{tor}} = \{x \in M \mid \mathrm{Ann}_R(x) \neq 0\} \subset M$ is an R-submodule (M_{tor} is called the *torsion module* of M. M is callled *R-torsion free* if $M_{\mathrm{tor}} = 0$, and M is called a *R-torsion module* if $M_{\mathrm{tor}} = M$).
2. If M is a finitely generated R-torsion module, then $\mathrm{Ann}_R(M) \neq 0$.
3. If M is R-free, then M is R-torsion free. Give an example showing that the reverse implication does not hold.

Let S be a commutative ring with $R \subset S$.

23. The set $\mathfrak{f}_{S/R} = \{a \in S \mid aS \subset R\} = \mathrm{ann}_R(S/R)$ is the largest ideal of S, which is also an ideal of R ($\mathfrak{f}_{S/R}$ is called the *conductor* of R in S).

24. If R is a domain and S a finitely generated R-module with $S \subset \mathsf{q}(R)$, then $\mathfrak{f}_{S/R} \neq \{0\}$.

25. If R is a noetherian domain and $\mathfrak{f}_{S/R} \neq \{0\}$, then S is a finitely generated R-module.

26. Suppose that S is a finitely generated R-module and R is a noetherian ring. Then S is a noetherian ring.

Note: the Theorem of Eakin-Nagata provides a converse: if S is a finitely generated R-module and S a noetherian ring, then R is a noetherian ring.

27. Let M be a non-zero R-module. Then the following statements are equivalent:
(a) M is indecomposable.
(b) 0 and 1 are the only idempotents of $\mathrm{End}_R(M)$.
Hint: If $f \in \mathrm{End}_R(M) \setminus \{0,1\}$ is idempotent, then $M = f(M) \oplus \mathrm{Ker}(f)$.

28. Let I, J be non-principal ideals of R such that $I+J=R$. Then $I \oplus J \cong R \oplus (I \cap J)$. Compare the statement with Theorem 2.50.

Hint: Let $a \in I$ and $b \in J$ with $a+b=1$. Show that $\varphi\colon I \oplus J \to R \oplus (I \cap J)$, defined by $(x,y) \mapsto (x+y, bx-ay)$ and $\psi\colon R \oplus (I \cap J) \to I \oplus J$, defined by $(r,s) \mapsto (ar+s, br-s)$ are inverse to each other.

29. Let $R = \mathbb{Z}$, $n \in \mathbb{N}_{\ge 2}$ and $n = p_1 \cdot \ldots \cdot p_r$ with $r \in \mathbb{N}$ and $p_1, \ldots, p_r \in \mathbb{P}$. Then

$$\mathbb{Z}/n\mathbb{Z} \supset p_1\mathbb{Z}/n\mathbb{Z} \supset p_1p_2\mathbb{Z}/n\mathbb{Z} \supset \ldots \supset p_1 \cdot \ldots \cdot p_{r-1}\mathbb{Z}/n\mathbb{Z} \supset 0$$

is a composition series with composition factors $(\mathbb{Z}/p_1\mathbb{Z}, \ldots, \mathbb{Z}/p_r\mathbb{Z})$, and this give a further proof of the Fundamental Theorem of Arithmetic in $\mathbb{Z}$.

30. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}/27\mathbb{Z}$. Find a composition series of M.

31. If M is a finitely generated R-module and N a noetherian R-module, then the R-module $\mathrm{Hom}_R(M,N)$ is noetherian. Give an example that even for vector spaces the assumption that M is finitely generated cannot be dropped.

32. (Example 16, continued). Let M be a free R-module of rank n, $\boldsymbol{u} = (u_1, \ldots, u_n)$ a basis of M, N a free R-module of rank m, $\boldsymbol{v} = (v_1, \ldots, v_m)$ a basis of N, and let $\varphi \in \mathrm{Hom}_R(M,N)$.

(a) If $\boldsymbol{u}'$ is a further basis of M and $\boldsymbol{v}'$ a further basis of N, then there exist matrices $S \in \mathrm{GL}_n(R)$ and $T \in \mathrm{GL}_m(R)$ such that $\boldsymbol{u}' = \boldsymbol{u}S$, $\boldsymbol{v}' = \boldsymbol{v}T$, and we have $\mathcal{M}_{\boldsymbol{u}',\boldsymbol{v}'}(\varphi) = T^{-1}\mathcal{M}_{\boldsymbol{u},\boldsymbol{v}}(\varphi)S$.
(b) Two matrices $A, B \in M_{m,n}(R)$ are called *equivalent* (Notation, $A \sim B$) if there exist matrices $U \in \mathrm{GL}_m(R)$ and $V \in \mathrm{GL}_n(R)$ such that $B = UAV$. Then $\sim$ is an equivalence relation on $M_{m,n}(R)$, and the equivalence class of $\mathcal{M}_{\boldsymbol{u},\boldsymbol{v}}(\varphi)$ is uniquely determined by φ.
(c) If P is a free R-module with basis $\boldsymbol{w} = (w_1, \ldots, w_q)$ and $\psi \in \mathrm{Hom}_R(N,P)$, then $\mathcal{M}_{\boldsymbol{u},\boldsymbol{w}}(\psi \circ \varphi) = \mathcal{M}_{\boldsymbol{v},\boldsymbol{w}}(\psi)\mathcal{M}_{\boldsymbol{u},\boldsymbol{v}}(\varphi)$.

Links:
Österreichische Mathematische Gesellschaft: http://www.oemg.ac.at
Deutsche Mathematiker Vereinigung: https://dmv.mathematik.de/
European Mathematical Society: http://www.euro-math-soc.eu/
American Mathematical Society: http://www.ams.org/home/page
MathSciNet: http://www.ams.org/mathscinet
https://zbmath.org/: Zentralblatt
Number Theory Web: http://www.numbertheory.org/
Commutative Algebra Web: http://www.commalg.org/

33. Let M be an R-module, F a free R-module, and $g\colon M \to F$ be an R-epimorphism. Then there exists an R-monomorphism $\psi\colon F \to M$ such that $g \circ \psi = \mathrm{id}_F$, and for every such ψ we have $M = \mathrm{Ker}(g) \oplus \mathrm{Im}(\psi)$.

34. Let M be a free R-module with basis $(u_i)_{i\in I}$. For $i \in I$, let $u_i^* \in \mathrm{Hom}_R(M, R)$ denote the unique R-homomorphism satisfying $u_i^*(u_j) = \delta_{i,j}$ for all $j \in I$.

1. Then $(u_i^*)_{i\in I}$ is R-linear independent.
2. If I is finite, then $(u_i^*)_{i\in I}$ is an R-basis of $\mathrm{Hom}_R(M, R)$. In this case $(u_i^*)_{i\in I}$ is called the dual basis with respect to $(u_i)_{i\in I}$.

35.

1. If M is a finitely generated R-module and $N \subsetneq M$ a submodule, then there exists a maximal submodule $N' \subsetneq M$ with $N \subset N'$.
2. The $\mathbb{Z}$-module $\mathbb{Q}$ has no maximal submodules.

36. Let S be a commutative ring, $f\colon R \to S$ a ring homomorphism, and $Q \subset S$ a prime ideal.

1. $f^{-1}(Q) \subset R$ is a prime ideal.
2. If f is surjective and Q a maximal ideal, then $f^{-1}(Q) \subset R$ is maximal. Give an example that the conclusion does not hold without the assumption that f is surjective.

37. The following statements are equivalent:

(a) $|\max(R)| = 1$.
(b) $R \setminus R^\times \subset R$ is an ideal.

38. Let $p \in \mathbb{P}$ and $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \,|\, x = \frac{a}{s} \text{ mit } a \in \mathbb{Z},\ s \in \mathbb{N} \text{ and } p \nmid s\}$.

1. $\mathbb{Z}_{(p)}$ is a principal ideal domain.
2. $p\mathbb{Z}_{(p)}$ is the only nonzero prime ideal of $\mathbb{Z}_{(p)}$, $\mathbb{Z}_{(p)}^\times = \mathbb{Z}_{(p)} \setminus p\mathbb{Z}_{(p)}$ and $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p$.
3. Every $u \in \mathbb{Z}_{(p)} \setminus \{0\}$ has a unique representation $u = p^n \epsilon$ with $n \in \mathbb{N}$ and $\epsilon \in \mathbb{Z}_{(p)}^\times$.
4. $\mathbb{Z} = \bigcap_{q\in\mathbb{P}} \mathbb{Z}_{(q)}$.

39. Let $I \triangleleft R$ be an ideal with $I = {}_R\langle a_1, \ldots, a_k\rangle$. Then $I^{nk} \subset {}_R\langle a_1^n, \ldots, a_k^n\rangle$ for all $n \in \mathbb{N}$.

40. Let M be an R-module and $I \subset \mathcal{J}(R)$ an ideal ($\mathcal{J}(R)$ is the Jacobson radical).

1. If M is finitely generated and $IM = M$, then $M = 0$.
2. If $N \subset M$ is a submodule such that M/N is finitely generated and $M = N + IM$, then $M = N$.

41. If R is a commutative ring and $\Sigma \subset \operatorname{spec}(R)$ is a chain, then

$$\mathfrak{a} = \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p} \quad \text{und} \quad \mathfrak{b} = \bigcap_{\mathfrak{p} \in \Sigma} \mathfrak{p}$$

prime ideals of R.

42. Let $R = \mathbb{Z}$ and $I \subset R$ an ideal. Determine $\mathcal{V}(I)$.

43. Let K be a field and $0 \ne I \lhd K[X]$. By Theorem 3.18 there are $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathcal{P}(I)$ with $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \subset I$. Give an interpretation of these deals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$?

44. Let R be a commutative ring with $R \ne 0$. Then the following statements are equivalent :

(a) R has precisely one prime ideal.
(b) Every element is either a unit or nilpotent.

Give an example of such a ring!

45. Let R be an artinian commutative ring.

1. $\mathcal{J}(R)$ equals the set of all nilpotent elements.
2. R has only finitely many maximal ideals.
   Hint: $\Omega = \{\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n \mid n \in \mathbb{N}, \mathfrak{m}_i \in \max(R)\}$ has a minimal element.

46. Let R_1 and R_2 be commutative rings, $R = R_1 \times R_2$, and $I \subset R$ a subset.

1. I is an ideal of R if and only if $I = I_1 \times I_2$ with $I_j \subset R_j$ is an ideal for $j \in [1, 2]$.
2. Suppose that $I = I_1 \times I_2 \lhd R$.
   (a) $R/I \cong R_1/I_1 \times R_2/I_2$.
   (b) $I \in \operatorname{spec}(R)$ if and only if
   $\Big(I_1 = R_1 \text{ and } I_2 \in \operatorname{spec}(R_2)\Big)$ or $\Big(I_2 = R_2 \text{ and } I_1 \in \operatorname{spec}(R_1)\Big)$.

47. For $p \in \mathbb{P}$ let

$$\mathbb{Z}(p^\infty) = \left\{ \frac{m}{p^k} + \mathbb{Z} \mid m \in \mathbb{Z}, k \in \mathbb{N} \right\} \subset \mathbb{Q}/\mathbb{Z}\,.$$

1. $\mathbb{Q}/\mathbb{Z} = \bigoplus_{p \in \mathbb{P}} \mathbb{Z}(p^\infty)$.
2. $\mathbb{Z}(p^\infty)$ is an artinian but not a noetherian $\mathbb{Z}$-module.
   Hint: Show that every proper subgroup is finite.

48. Let R be a commutative ring and A an R-algebra (e.g, a polynomial ring over R, a matrix ring over R, or a semigroup algebra).

1. If $I \subset A$ is a left ideal, then I is an R-submodule.
2. If R is noetherian (artinian) and A a finitely generated R-module, then A is left noetherian (left artinian). In particular, every finite dimensional K-algebra over a field K is an artinian ring.

49. A commutative ring R is called reduced if 0 is the only nilpotent element. Give an example of a reduced ring.

1. If $I \lhd R$ is a radical ideal, then R/I is reduced.
2. Let L/K be a field extension, $n \in \mathbb{N}$ and $V \subset L^n$ a K-variety. The K-algebra $K[V] := K[\boldsymbol{X}]/\mathcal{J}(V)$ is called the coordinate ring of the variety V. Show that the ring $K[V]$ is reduced.

50. Let R be a commutative ring and $I \lhd R$ an ideal.

1. If R is noetherian and I a radical ideal, then I is the intersection of finitely many minimal prime ideals lying over I.
2. If $I = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$ with prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{q}_s$, $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ and $\mathfrak{q}_k \not\subset \mathfrak{q}_l$ for all $i \neq j \in [1, r]$ and all $k \neq l \in [1, s]$, then $\{\mathfrak{p}_1, \ldots \mathfrak{p}_r\} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_s\}$.

51. Let L/K be a field extension, $n \in \mathbb{N}$ and $V \subset L^n$ a K-variety. Then the following statements are equivalent:

(a) V is irreducible (this means, if $V = V_1 \cup V_2$ with K-varieties V_1 and V_2, then $V = V_1$ or $V = V_2$).
(b) The vanishing ideal $\mathcal{J}(V) \subset K[\boldsymbol{X}]$ is a prime ideal.

52. Let L/K be a field extension, L algebraically closed, $n \in \mathbb{N}$ and $V = \mathcal{V}_L(\mathfrak{a}) \subset L^n$ a K-variety with $\mathfrak{a} \lhd K[\boldsymbol{X}]$.

1. V is the union of finitely many irreducible K-varieties, which do not contain each other: $V = V_1 \cup \ldots \cup V_s$
2. If $\mathcal{J}(V) = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$ with pairwise distinct minimal prime ideals lying over $\mathfrak{a}$, then $r = s$ and (after renumbering if necessary) $V_i = \mathcal{V}_L(\mathfrak{p}_i)$ for all $i \in [1, r]$.

53. Every factorial domain is integrally closed.
Hint: Consider an element $x = c^{-1}b \in \mathsf{q}(R) = K$ and an integral equation of x.

54. Let R be an integrally closed domain and $f, g \in R[X]$ relatively prime (i.e., there is no $h \in R[X] \setminus R$ such that $h \mid f$ and $h \mid g$). Then there are $p, q \in R[X]$ with $pf + qg \in R^\bullet$.
Hint: Consider the ideal $\langle f, g\rangle \lhd K[X]$ with $K = \mathsf{q}(R)$, and use Corollary 4.8.

55. Let K be a field and $\overline{K} \supset K$ an algebraic closure. A subset $C \subset \overline{K}^2$ is called an affine curve (defined over K) if there is an $f \in K[X, Y] \setminus K$ with $C = \mathcal{V}_{\overline{K}}(f)$.
If $f, g \in K[X, Y] \setminus K$ are relatively prime, then $|\mathcal{V}_{\overline{K}}(f) \cap \mathcal{V}_{\overline{K}}(g)| < \infty$ (i.e., the affine curves intersect in only finitely many points).
Hint: Consider $f, g \in R_1[Y]$ where $R_1 = K[X]$ and use 55; then consider $f, g \in R_2[X]$ and use 55. Take $(\alpha, \beta) \in \mathcal{V}_{\overline{K}}(f) \cap \mathcal{V}_{\overline{K}}(g)$.

56. Let $R \subset S$ be an integral ring extension and $Q \lhd S$ an ideal.
Then $R/(Q \cap R) \subset S/Q$ is an integral ring extension.

57. Let K be an algebraic number field, R its ring of integers, and $P \in \max(R)$.

1. There is precisely one prime $p \in \mathbb{P}$ with $p \in P$.
2. For a prime $p \in \mathbb{P}$ the following statements are equivalent:
   (a) $p \in P$.
   (b) $P \cap \mathbb{Z} = p\mathbb{Z}$.
   (c) $\mathsf{N}(P)$ is a power of p.

58. Let K be an algebraic number field with $[K : \mathbb{Q}] = n$ and R its ring of integers. Let $p \in \mathbb{P}$ and $pR = P_1^{e_1} \cdot \ldots \cdot P_g^{e_g}$ where $g, e_1, \ldots, e_g \in \mathbb{N}$ and $P_1, \ldots, P_g \in \max(R)$ are pairwise distinct. Then $\sum_{i=1}^g e_i f_i = n$ where $f_i = [R/P_i : \mathbb{Z}/p\mathbb{Z}] = f_i$ for all $i \in [1, g]$.