Topics in algebra

September 21, 2015

Remark. This is the live-texed notes of Topics in algebra course held by Mátyás Domokos at CEU in the fall trimester of 2014. Every error and typo in the text is mine.

Topics:

1. Non-commutative Rings
2. Basics of Representations of Groups
3. Commutative Algebra
4. Hilbert syzygy theorem
5. Lie algebras (Poincaré-Birkhoff-Witt theorem)

First Lecture, 30th of September

1 Non-commutative Rings

1.1 Simple rings

Remark 1.1. The motivation of this topic lies mainly in Representation Theory and in Commutative algebra. Therefore, on first sight (not knowing the previous two topics) it may seem a bit unmotivated.

Assumptions: A ring in this course will mean a not necessarily commutative ring with a unit element. We also assume that a commutative domain has at least two elements (i.e. $1 \neq 0$). Besides, every module is a left module, unless stated otherwise.

Definition 1.2. A ring R is called *simple*, if its only ideals are $\{0\}$ and R itself.

Definition 1.3. A ring R is called *primitive*, if there exists a faithful simple R-module. (Where simple means that the only submodules are $\{0\}$ and M, and faithful means that only the zero element brings everything to zero.)

Definition 1.4. The *annihilator* of M is $\operatorname{ann}_R(M) = \{r \in R \mid rm = 0 \, \forall m \in M\}$. In this language, M is faithful, if $\operatorname{ann}_R(M) = 0$. We can also define the annihilator of an element: $\operatorname{ann}_R(x) = \{r \in R \mid rx = 0\}$ which is a left ideal of R.

Remark 1.5. Clearly, $\operatorname{ann}_R(M) = \bigcap_{x \in M} \operatorname{ann}_R(x)$.

Definition 1.6. A ring R is called *prime*, if for all non-zero ideals $A, B \lhd R$ the product ideal $A \cdot B := \{\sum a_i b_i \mid a_i \in A,\ b_i \in B \ i \in \mathbb{N}\} \neq \{0\}$

Proposition 1.7. *A ring R is primitive if and only if it contains a maximal left-ideal L that contains no non-zero two-sided ideals.*

Proof. Suppose M is a simple R-module. Take any non-zero $m \in M$. Then $\{0\} \neq R \cdot m \leq M$ so – by irreducibility – $M = Rm$. Therefore, if we consider the module-homomorphism $\varphi : R \to M$, $\varphi(r) = rm$, then φ is a surjection, so $M = \mathrm{Im}\,(\varphi) \cong R/\mathrm{Ker}(\varphi) = R/\mathrm{ann}_R(m)$ i.e. $\mathrm{ann}_R(m)$ is a maximal left ideal by simplicity of M. This method assigns a maximal left ideal to a simple R-module – using a non-constructive choice: different elements can give different annihilators.

There is also an assignement in the reverse direction: if L is a maximal left ideal in R then R/L is a simple module. What is more, the annihilator of $(1 + L) \leq R/L$ is exactly L, so this is a left inverse of the previous assignment, up to isomorphism.

Moreover, $\mathrm{ann}_R(R/L)$ is a two-sided ideal of R, contained in L. Therefore, if L contains no non-zero two-sided ideal then $\mathrm{ann}_R(R/L) = 0$ so R/L is a faithful module, hence direction $\Leftarrow$ of the statement follows. For the converse, one can easily see that $\mathrm{ann}_R(R/L)$ is the biggest two-sided ideal in L. Indeed, if $A \lhd R$ and $A \subseteq L$ then $Ar \subseteq A \subseteq L$ for all $r \in R$ therefore $A \subseteq \mathrm{ann}_R(R/L)$. Taking everything into account, if the ring is primitive and M is a faithful simple module, then $\mathrm{ann}_R(m)$ is a maximal ideal (by irreducibility) and it has no non-zero two-sided ideal because its biggest two-sided ideal $\mathrm{ann}_R(M) = \mathrm{ann}_R(R/\mathrm{ann}_R(m))$ is zero by faithfulness. □

Example 1.8. Let V be an infinite dimensional vector space over a field $\mathbb{F}$. Then V is a simple faithful module of $\mathrm{End}_{\mathbb{F}}(V)$ therefore $\mathrm{End}_{\mathbb{F}}(V)$ is primitive. However, it is not simple because the set of finite-rank matrices gives a two-sided ideal.

Remark 1.9. In the commutative setup: Simpleness and primitivity are the same assumption as being a field, while primeness is equivalent to being a domain.

Proposition 1.10. *Primitivity implies primeness.*

Remark 1.11. (The converse is not true, even for commutative rings)

Proof. Let R be a primitive ring with a faithful simple R-module M. Let $A, B \lhd R$ be two non-zero ideals. Let $b \in B$ be a nonzero element. Since $\mathrm{ann}_R(M) = 0$ there exists an $m \in M$ such that $bm \neq 0$. It means that $Rbm = M$ by irreducibility. Therefore, for some nonzero $a \in A$ $aRbm \neq 0$ so $A \cdot B \supseteq aRb \neq 0$. □

Remark 1.12. Non-commutative domains (i.e. one with no zero-divisors) are prime.

Remark 1.13. Let R be a ring and $\{I_\lambda\}_{\lambda \in \Lambda}$ a family of ideals in R. Then we have a ring homomorphism

$$R \to \prod_{\lambda \in \Lambda} R/I_\lambda$$

$$r \mapsto (r + I_\lambda)_{\lambda \in \Lambda}$$

This homomorphism is injective, if $\cap_{\lambda \in \Lambda} I_\lambda = 0$. In this case, we say that R is a subdirect product of R/I_λ's.

Definition 1.14. A ring R is *semisimple* (resp. *semiprimitive*, *semiprime*) if it is the subdirect product of *simple* (resp. *primitive*, *prime*) rings.

It can be formalized in another way:

Definition 1.15. An ideal $I \lhd R$ is called *prime* (resp. *primitive*, *maximal*) if R/I is *prime* (resp. *primitive*, *simple*).

Remark 1.16. In this terminology, a ring is called semisimple (resp. semiprimitive, semiprime) if the intersection of its maximal (resp. primitive, prime) ideals are zero.

Proposition 1.17. *A ring is semiprime if and only if it has no non-zero nilpotent ideal.*

Remark 1.18. (easy exercise) The latter is equivalent to saying it has no ideal I such that $I^2 = 0$.

Proof. Suppose that for an ideal $I \lhd R$, $I^2 = 0$. For any prime ideal P we have $P \supseteq 0 = I \cdot I$. Then primeness implies $P \supseteq I$, what is true for all P, hence

$$0 \neq I \subseteq \bigcap_{P \lhd R \text{ prime}} P$$

so R is not semiprime.

Now suppose that R contains no non-zero nilpotent ideals. Take an arbitrary nonzero element $b_0 \in R$. We have to find a prime ideal $P \lhd R$ that does not contain b_0. By the assumptions, we have $(Rb_0R)^2 = Rb_0Rb_0R \neq 0$. It means that there exists some $x_0 \in R$ such that $b_1 := b_0x_0b_0$ is non-zero. Repeat this argument and obtain $b_{j+1} = b_jx_jb_j \neq 0$ for all $j \in \mathbb{N}$. This way we got a sequence $b_0, b_1, b_2, \ldots$ such that for all $i, j \in \mathbb{N}$ and $k > i, j$ there exists $z \in R$: $b_k = b_izb_j$. (It can be easily proved by induction.)

Now, let M be an ideal in R maximal with respect to the property that no element of the sequence $b_0, b_1, b_2, \ldots$ is contained in it. We need to check that M exists, but it does: the zero ideal is an element of the family of ideals with this property and the family is closed under taking the union of an ascending chain. Therefore, by Zorn's lemma, M exists.

We can show that M is prime. Suppose that $A, B \lhd R$ that properly contain M. We need to show that their product is not contained in M. By the maximality of M, both A and B contain some element of the sequence $b_0, b_1, \ldots$, let us denote them byb_i and b_j. By the above mentioned property, $0 \neq b_k = b_izb_j \in b_iRb_j \subseteq A \cdot B$ for some z. This proves the statement. □

1.2 Jacobson radical

Definition 1.19. $\operatorname{rad}(R) = \{r \in R \mid r \in \operatorname{ann}_R(M)\ \forall \text{ irreducible } R\text{-module } M\}$

Remark 1.20. There is a usual logical or set-theoretical issue about taking all irreducible modules since strictly speaking it is not a set. This formal problem is solved by the observation that an irreducible module is always cyclic (factor of R), hence we can take a set of modules (the irreducible factors of R) what contains all irreducibles, up to isomorphism.

Proposition 1.21. (Alternative definitions):

$$\operatorname{rad}(R) \overset{1)}{=} \bigcap_{Q \lhd R \text{ primitive}} Q \overset{2)}{=} \bigcap_{L \leq R \text{ maximal}} L$$

Proof. To prove the first one, we need to realize that primitive ideals are exactly the annihilators of simple R-modules: Indeed, if M is a simple$R$-module then it can be viewed as a faithful module over $R/\operatorname{ann}_R(M)$. It is easy to see that it is still simple. This proves 1). Similarly, the maximal left ideals are exactly the annihilators of non-zero elements in simple R-modules. Therefore, because a primitive ideal I is the annihilator of M for some simple R-module we get:

$$Q = \operatorname{ann}_R(M) = \bigcap_{x \in M} \operatorname{ann}_R(x) = \bigcap_{Q \leq L \leq R} L$$

and that proves 2). □

Definition 1.22. The *radical* of an R-module M can be defined analogously:

$$\operatorname{rad}(M) := \bigcap_{N \leq M \text{ maximal}} N$$

giving back the ring radical $\operatorname{rad}(R)$ for the choice $M = R$.

Theorem 1.23. *The Jacobson radical of R is exactly $\{r \in R \mid 1 - ar$ is left invertible for all $a \in R\}$.*

The required property for r can be reformulated as 'ar' has to be left quasi-regular for all $a \in R$.

Definition 1.24. An element $z \in R$ is *left quasi-regular*, if $1 - z$ is left-invertible in R.

Remark 1.25. If $a \in R$ is nilpotent, then $(1 + a + a^2 + a^3 + \dots)(1 - a) = 1 - a^n = 1$ so nilpotent elements are left and right quasi-regular. Therefore, it is a generalization of the notion of nilpotent element.

Proof. Suppose $z \in \operatorname{rad}(R)$ but az is not left quasi-regular for some $a \in R$. It means that $R \supsetneq R(1 - az)$ so it is contained in some maximal left ideal $L \supseteq R(1 - az)$. But $L \supseteq \operatorname{rad}(R)$ as well. Therefore, both $1 - az$ and az are contained in L so $1 = 1 - z + z \in L$ and that is a contradiction.

Now let Z be a left ideal in R consisting of left quasi-regular elements. Suppose on contrary that $Z \not\subseteq \operatorname{rad}(R)$ i.e. there exists a maximal left ideal $L \leq R$ such that $Z \not\subseteq L$. Then $Z + L = R$ so $z + b = 1$ for some $z \in Z$ and $b \in L$. Then $b = 1 - z$ which has a left inverse, so $L = R$ but that is a contradiction. □

Corollary 1.26.

1. $\operatorname{rad} R = 0$ *if and only if* R *is semiprimitive.*
2. $R/\operatorname{rad}(R) = 0$ *is semiprimitive.*
3. *If* R/I *is semiprimitive then* $I \supseteq \operatorname{rad}(R)$

The definition of Jacobson radical seems to be left-right sensitive so we should define separately the left and the right radical of a ring. However, in fact the two concepts coincide. To prove this, we need extra notions and statements.

Proposition 1.27. *$z \in R$ is left quasi-regular if and only if there exists some $z' \in R$ such that $z + z' - z'z = 0$. (It worth to note that this definition works for rings without 1.)*

Proof. Write the left inverse of $1 - z$ in the form of $1 - z'$. Then $1 = (1 - z')(1 - z) = 1 - z - z' + z'z$, so $z + z' - z'z = 0$. □

Let R be a ring and introduce on R a binary operation $\circ$ as $a \circ b = a + b - ab$. It turns out that $(R, \circ)$ is obviously a monoid (associative semigroup with identity element 0). But more is true:

Lemma 1.28. *If L is a left ideal in R consisting of left quasi-regular elements then $(L, \circ, 0)$ is a subgroup of the monoid $(R, \circ, 0)$.*

Proof. It is easy to check that L is closed under $\circ$. Now, take $z \in L$. We know that there exists $z' \in R$ such that $0 = z' + z - z'z = z' \circ z$. So $z' = z'z - z \in L + L = L$. However, we still have to check that z' is a two-sided inverse with respect to $\circ$. By the assumptions on $z' \in L$ being left quasi-regular, we have an element $z'' \in R$ such that $z'' \circ z' = 0$. Then z' have both a left and a right inverse in R so they have to coincide (by associativity), i.e. it is z. Or in other words, z' is indeed a two-sided inverse of z with respect to $\circ$. □

Corollary 1.29. *The left and the right Jacobson radical is the same.*

Proof. see Homework. □

1.3 Completely reducible modules

Definition 1.30. An R-module is called *completely reducible*, if for all submodules $N \leq M$ there exists an $N' \leq M$ such that $M = N \oplus N'$.

Example 1.31. A simple R-module is completely reducible. (Since it has no non-trivial submodules.)

Proposition 1.32. *Submodules and factor modules of a completely reducible module are completely reducible.*

Proof. We only prove the statement for factor modules. (The submodule case is even easier.) Let $N \leq M$ where M is completely reducible. By the assumption, we know that $N \cong M/N'$ for some N' such that $M \cong N \oplus N'$. Now, let $P \leq M/N$. If we consider the natural surjection $\eta : M \twoheadrightarrow M/N$, $m \mapsto m + N$ then we can define the preimage-module: $M \geq P_1 := \eta^{-1}(P)$. Using the assumption again, we get a submodule $Q \leq M$ such that $P_1 \oplus Q = M$. Then $\eta(Q) = Q + N$ is a complement of $P \leq M/N$. □

Second Lecture, 7th of October

Definition 1.33. A set $\{M_\lambda\}_{\lambda\in\Lambda}$ of nonzero submodules of an R-module M is *independent*, if for all $\alpha \in \Lambda$

$$M_\alpha \bigcap \sum_{\beta\in\Lambda,\, \beta\neq\alpha} M_\beta \neq 0$$

Remark 1.34. Obviously, a set of submodules is independent if and only if any of its finite subsets is independent.

Lemma 1.35. *Suppose that $\{M_\lambda\}_{\lambda\in\Lambda}$ is an independent set of non-zero submodules of M and $N \leq M$ with*

$$N \cap \sum_{\lambda\in\Lambda} M_\lambda = \{0\}$$

Then $\{M_\lambda\}_{\lambda\in\Lambda} \cup \{N\}$ is independent as well.

Proof. Suppose indirectly, that it is not independent. Then, by Remark 1.34, there are finitely many M_{λ_i}'s for $\lambda_i \in \Lambda$ and $i = 0, \ldots, n$ such that either $\{0\} \neq \sum_{i=0}^{n} M_{\lambda_i} \cap N$ (which is impossible by the assumption $\sum_{\lambda\in\Lambda} M_\lambda \cap N = \{0\}$) or either

$$\Big(\sum_{i=1}^{n} M_{\lambda_i} + N\Big) \cap M_{\lambda_0} \neq \{0\}$$

for an appropriate numbering of the λ_i's. This means that $\sum_{i=1}^{n} m_i + n = m_0 \neq 0$ for some $m_i \in M_{\lambda_i}$, and $n \in N$. Here n cannot be zero since that would contradict the independence of the M_{λ_i}'s so $0 \neq n = m_0 - \sum_{i=1}^{n} m_i$ which is also impossible because of the assumption on N. □

Proposition 1.36. *The following are equivalent for an R-module M:*

1. *M is the direct sum of simple R-modules.*
2. *M is spanned by its simple submodules.*
3. *M is completely reducible.*

Proof. 1) ⇒ 2) is trivial.

To prove 2) ⇒ 3) suppose $M = \sum M_\lambda$ where M_λ is simple for all $\lambda \in \Lambda$ and let $N \leq M$ be an arbitrary submodule. To find its complement, – by Zorn's lemma – consider a maximal subset A of Λ among those that satisfy the following: $N \cap \sum_{\lambda\in A} M_\lambda = \{0\}$. Then if we take an arbitrary $\alpha \in \Lambda$ then– by simpleness – M_α is either in $N + \sum_{\lambda\in A} M_\lambda$ or the intersection is zero. In the first case, there is no problem. In the second case, M_α is independent of $N + \sum_{\lambda\in A} M_\lambda$ so $\{\alpha\} \cup A$ is also independent by Lemma 1.35. But that is a contradiction, meaning that $N + \sum_{\lambda\in A} M_\lambda = M$.

To get 3) ⇒ 1) Suppose that M is completely reducible. First, we prove that any non-zero completely reducible module contains a simple submodule. Indeed, take a non-zero $x \in M$ and let N be a maximal submodule of M such that $x \notin N$ (by Zorn's lemma, it exists). In M/N any non-zero submodule contains $0 \neq (x + N)$. However, M/N is also completely reducible by Proposition 1.32, so $M/N = (x + N)$. (Because if $(x + N)$ is not the whole then the complement of $(x + N)$ does not contain x and that is impossible.) Therefore, M/N is simple. Now take a complement submodule P of N in M, i.e. $N \oplus P = M$. Then $M/N \cong P$ so P is simple as well.

Therefore, if we take a maximal independent set of simple submodules $\{M_\lambda\}_{\lambda\in\Lambda}$ in M (by Zorn's Lemma), then – by the assumption – we can take its complement N' such that $N' \oplus \sum_{\lambda\in\Lambda} M_\lambda = M$. However, N also contains a simple submodule by the previous argument, so we get a contradiction. □

Proposition 1.37. *Suppose that $M = \oplus_{i=1}^{p} M_i$ where M_i is simple for all $i = 1, \dots, p$. Suppose that we can write M as $M = \oplus_{\lambda \in \Lambda} N_\lambda$ (not necessarily with finite Λ). Then $|\Lambda| = p$, and there is numbering of Λ such that $M_i \cong N_i$ for all $i = 1, \dots, p$.*

Proof. By Zorn's lemma and the previous argument, we can choose a $\Gamma_1 \subsetneq \Lambda$ such that $M_1 \oplus \bigoplus_{\gamma \in \Gamma_1} N_\gamma = M$. Then

$$M_1 \cong M / \bigoplus_{\gamma \in \Gamma_1} N_\gamma \cong \bigoplus_{\gamma \in \Lambda \setminus \Gamma_1} N_\gamma$$

where the left hand side is simple so the right hand side has to be simple as well. In other words, $|\Lambda \setminus \Gamma_1| = 1$ so we found the corresponding N. Now, using induction, we can find the full bijection between M_i's and N_α's. □

Corollary 1.38. *If $M = \oplus_{i=1}^{p} M_i$ where the M_i's simple then M is completely reducible and for any non-zero submodule or factormodule N of M there exists a subset A of $\{1, 2, \dots, n\}$ such that*

$$N \cong \oplus_{i \in A} M_i$$

Proof. A submodule or factormodule is completely reducible as well by Proposition 1.32 so it has a decomposition. The complement also has a decomposition, but by Proposition 1.37 the decomposition is unique up to permutation and isomorphism, so we got the corollary. □

1.4 Jacobson-Chevalley Density Theorem

Lemma 1.39. (Schur's lemma) *If M and N are simple R-modules, then any non-zero R-module homomorphism $M \to N$ is an isomorphism.*

Proof. Take a homomorphism $\varphi \in \mathrm{Hom}(M, N)$. Then $\mathrm{Ker}\,(\varphi) \leq M$ and $\mathrm{Im}\,(\varphi) \leq N$. $\varphi \neq 0$ so $\mathrm{Im}\,(\varphi) \neq 0$ but then by simpleness, it is the whole N, i.e. it is surjective. Similarly, $\mathrm{Ker}\,(\varphi) \neq M$ so it has to be zero. □

Corollary 1.40. *If M is a simple R-module, then $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ is a division ring (i.e. skew field).*

Theorem 1.41. (Jacobson-Chevalley Density Theorem) *A ring R is primitive if and only if R is isomorphic to a dense subring of $\mathrm{End}_D(V)$.*

Definition 1.42. Let D be a division ring and V a "vector space" over D. Then $S \subseteq \mathrm{End}_D(V)$ is *dense*, if $\forall n \in \mathbb{N}$, $\forall x_1, \dots, x_n \in V$ linearly independent over D and $\forall y_1, \dots, y_n \in V$ there exists an $s \in S$ such that $sx_i = y_i$ $(\forall i = 1, \dots, n)$.

Remark 1.43. If $\dim_D V < \infty$ then the only dense subring of $\mathrm{End}_D(V)$ is $\mathrm{End}_D(V) \cong (D^{op})^{n \times n}$ itself.

Example 1.44. Suppose that $\dim_{\mathbb{F}} V = \infty$ and $\dim_D V = n < \infty$ where D is a division ring and $\mathbb{F}$ is a field. Then $\mathrm{End}_{\mathbb{F}}(V) \supsetneq \{\text{finite rank linear transformations}\}$ is dense as well.

Proof. (of Theorem 1.41) Suppose $R \subseteq \mathrm{End}_D(V)$ is a dense subring. Then V is a faithful R-module, and it is simple since for any nonzero $x \in V$ $Rx = V$ by applying the definition of density for $n = 1$. Therefore, R is primitive, by definition.

For the converse, suppose that R is primitive then there exist a faithful, simple R-module V. Let $D = \mathrm{End}_R(V)$ which is a division ring by Schur's lemma 1.39. Then V is naturally a D-module and we have a natural $R \to \mathrm{End}_D(V)$ inclusion. (Indeed, we can see every mentioned ring as a subring of $\mathrm{End}_{\mathbb{Z}}(V)$ because $\mathrm{End}_D(V)$ is there by definition and faithfulness means that R embeds into $\mathrm{End}_{\mathbb{Z}}(V)$ as well. But if $\mathrm{End}_D(V)$ are those morphisms that commute with the elements of $\mathrm{End}_{\mathbb{Z}}(V)$ commuting with the elements of R is obviously there. Or in short, the double "commutant" contains the original ring.)

Now, take $n \in \mathbb{N}$ and linearly independent vectors $x_1, \dots x_n \in V$. These together can be considered as an element of V^n, so it is enough to prove that $R \cdot (x_1, \dots, x_n) = V^n$. Since V^n is the direct sum of simple

R-modules, it is completely reducible by Proposition 1.36. Hence, if we assume that $R \cdot V^n \lneq V^n$ then there exists a nonzero $P \leq V^n$ submodule such that $R \cdot (x_1, \ldots, x_n) \oplus P = V^n$. Let us denote by $\pi : V^n \to P$ the projection (for a chosen P splitting V^n). Then $\pi \in \mathrm{End}_R(V^n) \cong D^{n \times n}$ (see the next Lemma), in particular there exist $d_{ij} \in D$ for all $1 \leq i, j \leq n$ such that

$$\pi(x_1, \ldots, x_n) = \left(\sum_i d_{ij} x_j \right)_{i=1,\ldots,n}$$

However, $\pi(x_1, \ldots, x_n) = 0$ by the definition of π meaning that for all i the sums give $\sum_i d_{ij} x_j = 0$. Then the independence of the x_j's implies that $d_{ij} = 0$ for all i, j. i.e. $\pi = 0$ so $\mathrm{Ker}\pi = R(x_1, \ldots, x_n) = V^n$ as claimed. □

Lemma 1.45. $\mathrm{End}_R(V^n) \cong D^{n \times n}$ *where* $D = \mathrm{End}_R(V)$

Proof. By the biadditivity of the $\mathrm{Hom}(.,.)$ functor, we can see that they are isomorphic as abelian groups, so we only have to check that the multiplication works well. But it does, the straightforward details are omitted. □

Definition 1.46. An R-module M is *Artinian*, if M satisfies the descending chain condition for submodules (in short *d.c.c.* on submodules), i.e. there is no infinite, properly descending chain of submodules in M.

Or equivalently (by Zorn's lemma), every non-empty subset of submodules has a minimal element (in short: *minimum condition* on submodules).

Definition 1.47. A ring R is called *Artinian* if R is Artinian as a module over itself.

Example 1.48. Finite dimensional algebras are Artinian.

Theorem 1.49. (Wedderburn-Artin I.) *The following are equivalent for a ring R:*

1. *R is simple, Artinian*
2. *R is primitive, Artinian*
3. *R is prime, Artinian*
4. *R is isomorphic to $M_n(D)$ for some positive integer n and for some division ring D.*

Proof. The implication 1) ⇒ 2) is obvious by the characterization presented in Proposition 1.7 and 2) ⇒ 3) is true by Proposition 1.10. The direction 3) ⇒ 1) will follow from Wedderburn-Artin II, see below Corollary 1.54.

Direction 4) ⇒ 1) is an easy exercise, probably done by everyone before. For 2) ⇒ 4) suppose that R is primitive, Artinian. Then, by the density theorem, R is a dense subring of $\mathrm{End}_D(V)$ for some division ring D. If V is finite dimensional over D then by Remark 1.43 $R = \mathrm{End}_D(V) \cong \left(D^{op}\right)^{n \times n}$. Now, suppose that $\dim_D(V) = \infty$. Then take an infinite strictly ascending chain of finite dimensional subspaces of V: $V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_k \subsetneq \ldots$. Then the annihilators $L_i \leq R$ of the subspaces form a descending chain of left ideals in R which is strictly descending by density theorem 1.41. That contradicts Artinianity. □

Proposition 1.50. *If R is Artinian then the Jacobson-radical* $\mathrm{rad}\,(R)$ *of R is nilpotent, i.e. there exists an* $n \in \mathbb{N}$ *such that* $\mathrm{rad}\,(R)^n = 0$.

Proof. Consider the descending chain of left ideals $R \supseteq \mathrm{rad}\,(R) \supseteq \mathrm{rad}\,(R)^2 \supseteq \cdots \supseteq \mathrm{rad}\,(R)^n \supseteq \ldots$. By Artinianity, there exists an n such that $J := \mathrm{rad}\,(R)^n = \mathrm{rad}\,(R)^{n+1} = \ldots$. Suppose now that $J \neq 0$. Consider the following set of left ideals

$$\{L \leq R \mid L \subseteq J,\ JL \neq 0\} \neq \emptyset$$

and let M be a minimal element of it (existing by the assumed minimal condition). Let $b \in M$ such that $Jb \neq 0$ which exists by the definition of M. Then – by the minimality of M – $M = Jb$. (Indeed, $0 \neq J(Jb) = Jb \subseteq M$.) Then this also means that there exists some $z \in J$ such that $b = zb$, i.e. $(1 - z)b = 0$ but $1 - z$ is invertible, so $b = 0$ and that is a contradiction. □

Theorem 1.51. (Wedderburn-Artin II.) *The following are equivalent for a ring R:*

1. *R is semisimple, Artinian*
2. *R is semiprimitive, Artinian*
3. *R is semiprime, Artinian*
4. *There exist $n_1, \dots, n_q \in \mathbb{N}_+$ such that R is isomorphic to $M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_k}(D_k)$.*
5. *${}_RR$ is completely reducible*
6. *every R-module is completely reducible*

Third Lecture, 14th of October

Proof. 1) $\iff$ 2) follows from Wedderburn-Artin I. 2) $\Rightarrow$ 3) because primitive implies prime. 3) $\Rightarrow$ 2) because the radical of an Artinian ring is nilpotent by Proposition 1.50.

1) $\Rightarrow$ 4): By Wedderburn-Artin I, Theorem 1.49, we only need to prove that a semisimple Artinian ring is a product of simple Artinian rings.

Lemma 1.52. *Let M be an Artinian R-module, which is a subdirect sum of simple R-modules. Then M is direct sum of finitely many simple R-modules.*

Proof. The assumption means that there exists a family of morphisms $\{\varphi_\lambda : M \to M_\lambda \mid \lambda \in \Lambda, \}$ where all M_λ is simple such that $\cap_{\lambda\in\Lambda}\mathrm{Ker}\varphi_\lambda = \{0\}$. By Artinianity, there are finitely many λ's such that $\cap_{i=1}^n \mathrm{Ker}\,\varphi_{\lambda_i} = \{0\}$. So M embeds into $\oplus_{i=1}^n M_{\lambda_i}$. However, the sum is semisimple, so by Proposition 1.32 M is also a direct summand of the sum and is itself a semisimple module. □

Corollary 1.53. *If S is a semisimple ring which satisfies the descending chain condition for two-sided ideals, then S is the ring direct product of finitely many simple rings.*

Proof. Consider the ring $\mathrm{End}_{\mathbb{Z}}(S) \supseteq R := \langle x \mapsto r \cdot x,\ x \mapsto x \cdot r \mid r \in S\rangle$. Then S is naturally an R-module and the ideals of S are exactly the R-submodules of ${}_RS$. Now, we can apply Lemma 1.52 because the given assumptions imply the assumptions of the Lemma: S has d.c.c on the R-submodules and it is a semidirect product of simple rings by definition. So we get that ${}_RS$ is the module direct product of simple rings. It can be proven elementarily that it is not only an R-module direct product but the multiplication is preserved as well. □

The statement 1) $\Rightarrow$ 4) follows. Direction 4) $\Rightarrow$ 5):

$$ {}_RR \cong \oplus_{i=1}^k {}_{M_{n_i}(D_i)}M_{n_i}(D_i) \cong \oplus_{i=1}^k {}_{M_{n_i}(D_i)}\big(\oplus_{j=1}^{n_i} D_i^{n_i}\big) \cong \oplus_{i=1}^k \oplus_{j=1}^{n_i} {}_RD_i^{n_i} $$

where all the $D_i^{n_i}$'s are simple over R (because they are simple over $M_{n_i}(D_i)$ and the action is the same).

5) $\Rightarrow$ 2) will give us the equivalence of the first 5 statements. To prove this part, observe that we can choose maximal submodules that have zero intersection by complete reducibility. Namely, if $R \cong \oplus_i S_i$ as R-modules where S_i's are simple then $\oplus_{i\neq j} {}_RS_i$ is clearly a maximal left-ideal (what are the maximal R-submodules of ${}_RR$) and the intersection of them for all i is $\{0\}$. This proves that radÄ$, R = 0$ i.e. R is semiprimitive. Besides, Artinianity follows from the fact that ${}_RR$ is the direct sum of minimal left ideals L_λ for $\lambda \in \Lambda$ by complete reducibility. However, we can prove that Λ is finite since $R \ni 1 = e_1 + \cdots + e_n \in \oplus_{i=1}^n L_{\lambda_i}$ and this element generates the whole $\oplus_{\lambda\in\Lambda} L_\lambda$ so $|\Lambda| = n$. Therefore, we can see that any strictly descending chain of left ideals has length at most $n+1$ (every term is a subsum of L_{λ_i}'s) so R is Artinian.

6) $\Rightarrow$ 5) is trivial. Conversely, for any R-module M we can take a generating map: $R^\alpha \to M$, or in other words $M = \sum_{x\in M} Rx$. Here, $Rx \cong R/\mathrm{ann}_R(x)$ which is a factor module of the completely reducible R-module ${}_RR$. Hence, Rx is also completely reducible by Proposition 1.32. Then M is the sum of its simple submodules and by Proposition 1.36 we get that M is completely reducible as well. □

Corollary 1.54. *Prime Artinian implies primitive Artinian i.e.* 3) ⇒ 2) *in Wedderburn-Artin I. 1.49.*

Remark 1.55. Suppose that $R = \prod_{i=1}^{q} M_{n_i}(D_i)$ and denote by S_i the simple R-modules $D_i^{n_i}$. Then

1. $S_1, \ldots, S_q$ is a complete list of irreducible R-modules. (Since every simple module is cyclic and by complete reducibility, it is a summand of R. Besides, they are non-isomorphic because their annihilators are different.)

2. n_i's and D_i's are unique because n_i is the multiplicity of S_i in ${}_RR$ and $D_i = \mathrm{End}_R(S_i)$.

Theorem 1.56. (Maschke's theorem) *The group algebra $\mathbb{F}G$ of a finite group G is semisimple if and only if* char$\mathbb{F} \not| \, |G|$.

Proof. Suppose that char$\mathbb{F} = p$ prime and $p \mid |G|$. Then we shall find a nilpotent ideal in $\mathbb{F}G$ hence it is not semisimple. Take $c := \sum_{g \in G} g \in \mathbb{F}G$. Then $ch = c$ for all $h \in G$ (short computation) so

$$c \sum a_g g = c \Big(\sum a_g \Big)$$

i.e. $\{\lambda c \mid \lambda \in \mathbb{F}\} \lhd \mathbb{F}G$. However, it is nilpotent because $cc = |G|c = 0$ by $p \mid |G|$.

Conversely, assume that char$\mathbb{F} \not| \, |G|$. Then we show that for any $0 \lneq N \lneq M$ modules we can find a direct complement N' i.e. $N \oplus N' = M$. This means that every module is completely reducible so by Wedderburn-Artin II. 1.51, $\mathbb{F}G$ is semisimple. The trick is to take an arbitrary $\mathbb{F}$-projection $\pi \in \mathrm{End}_{\mathbb{F}}(M)$ on N. The projection can be "pushed into" $\mathrm{End}_{\mathbb{F}G}(M) \leq \mathrm{End}_{\mathbb{F}}(M)$ if we average the conjugates of π i.e. take $\rho : M \to M$

$$\rho(x) = \frac{1}{|G|} \sum_{g \in G} g\pi g^{-1}(x)$$

Now, we need to show that ρ is an $\mathbb{F}G$-homomorphism and that $\mathrm{Im}\, \rho = N$. First,

$$h\rho(x) = h \frac{1}{|G|} \sum_{g \in G} g\pi g^{-1}(x) = \frac{1}{|G|} \sum_{g \in G} hg\pi(hg)^{-1}h(x) = \rho(h(x))$$

so ρ is G-equivariant i.e. it is indeed a homomorphism. Second, if $x \in M$ then $\pi g^{-1}(x) \in N$ so $g\pi g^{-1}(x) \in N$ and similarly for the sum. So Im$\rho \subseteq N$. Conversely, if $x \in N$ is arbitrary then

$$\rho(x) = \frac{1}{|G|} \sum_{g \in G} g\pi g^{-1}(x)$$

where $g^{-1}(x) \in N$ so π "does nothing": $\pi g^{-1}(x) = g^{-1}(x)$ therefore

$$\rho(x) = \frac{1}{|G|} \sum_{g \in G} gg^{-1}(x) = \frac{|G|}{|G|} x = x$$

so Imρ is the whole N. Now, $M \cong \mathrm{Im}\,(\rho) \oplus \mathrm{Ker}\,(\rho) \cong N \oplus \mathrm{Ker}\,(\rho)$ so we got the statement. □

2 Representations of finite groups

2.1 Basics of (general) group representations

Definition 2.1. By a *representation* of a group G we mean an $\mathbb{F}$-vector space V together with a group homomorphism $\rho : G \to GL(V)$.

Notation: For $v \in V$ and $g \in G$ $gv := (\rho(g))(v)$. Using this notation, the homomorphism rule means $(gh)v = g(hv)$, $1_G v = v$, $g(\lambda v + \mu w) = \lambda g(v) + \mu g(w)$ for all $v, w \in V$, $g, h \in G$ and $\lambda, \mu \in \mathbb{F}$.

Remark 2.2. The representations of a group G are in natural bijective correspondence with modules over $\mathbb{F}G$.

Corollary 2.3. *The main notions are in bijective correspondence as well, such as sub, factor, irreducible, (direct) sum or homomorphisms. Therefore, we have seen many results on group representations in the language of module theory (see Theorem 1.56).*

Remark 2.4. In physics, a homomorphism of representations is called intertwining operator.

Definition 2.5. The *trivial representation* is a vector space V such that $\dim_{\mathbb{F}} V = 1$ with the action $g \mapsto \mathrm{id}_V$.

Definition 2.6. Given a representation $\rho : G \to GL(V)$ we can define the *dual* representation $\rho^* : G \to GL(V)$ as for all $g \in G$, $\xi \in V^*$ and $v \in V$ we define

$$\big(\rho^*(g)(\xi)\big)(v) = \xi(g^{-1}v)$$

Definition 2.7. Given two representations ρ_1, ρ_2 we can define the *product* of the two representation $\rho_1 \cdot \rho_2 : G \to GL(V_1 \otimes V_2)$ by $(\rho_1 \cdot \rho_2)(g)(v \otimes w) = gv \otimes gw$.

Remark 2.8. Here, we got a reminder on tensor product of vector spaces that I skipped because of pure laziness. Excuse me. The mentioned notions were:

1. the construction,
2. universality,
3. uniqueness by universality,
4. base of the product from the bases of the original spaces (generating system by construction, independence by universality)

For details, see (for example) Steven Roman: Advanced Linear algebra (Springer, 2000, GTM 135)

Fourth Lecture, 21th of October

Remark 2.9. After this, we can describe what the product of two representations mean. Let ρ_1 and ρ_2 be two representations. Then we can define

$$\beta_g : V_1 \times V_2 \to V_1 \otimes V_2$$

$$(v_1, v_2) \mapsto \rho_1(g)(v_1) \otimes \rho_2(g)(v_2)$$

This is bilinear so – by universality – there exists a unique map through the tensor product: $A : V_1 \otimes V_2 \to V_1 \otimes V_2$ such that $A \circ \otimes = \beta$. From now on, we use the notation $\rho_1 \cdot \rho_2(g) := A$.

This way, we got a map $G \to \mathrm{End}_{\mathbb{F}}(V_1 \otimes V_2)$. However, we can easily get that it is multiplicative because $\rho_1\rho_2(gh)$ acts the same way on rank 1 tensors (i.e. element of the form $v \otimes w$) as $\rho_1\rho_2(g) \circ \rho_1\rho_2(h)$ acts. If the action is the same on this generating system, then it is the same on the whole vector space. Moreover, multiplicativity means that we have a unit element $\rho_1\rho_2(1)$ and inverse-pairs mapped to inverse-pairs so it is in fact a $G \to \mathrm{Aut}_{\mathbb{F}}(V_1 \otimes V_2)$ map.

Lemma 2.10. Schur's lemma revisited:

1. Schur's lemma I: *A non-zero morphism between irreducible representations of group representations is an isomorphism.*
2. Schur's lemma II: *Let $\rho : G \to GL(V)$ is a finite dimensional irreducible representation over an algebraically closed base field $\mathbb{F}$. Then the G-equivariant $V \to V$ linear maps are $\lambda \mathrm{id}_V$ ($\lambda \in \mathbb{F}$).*

Proof. The first one is a trivial consequence of the original Schur's lemma on modules. To get the second, suppose $T : V \to V$ is linear and $T \circ \rho(g) = \rho(g) \circ T$ for all $g \in G$. Take an eigenvalue λ of T in $\mathbb{F}$. Note that $S := T - \lambda \mathrm{id}_V$ is also a $V \to V$ G-module homomorphism. However, $\mathrm{Ker} S \neq \{0\}$ so by the first part $S = 0$. It means that $T = \lambda \cdot \mathrm{id}_V$. □

Corollary 2.11. *Finite dimensional irreducible representations over an algebraically closed field of an Abelian group are one dimensional.*

Proof. Suppose that G is abelian, $\rho : G \to GL(V)$ is a finite dimensional irreducible representation over $\mathbb{F}$. However, $\rho(y) \cdot \rho(x) = \rho(yx) = \rho(xy) = \rho(x) \cdot \rho(y)$ i.e. $\rho(y)$ is G-equivariant for each $y \in G$ so by Schur's lemma II (2.10), $\rho(y) = \lambda_y \mathrm{id}_V$ for some $\lambda_y \in \mathbb{F}$. This holds for all $y \in G$ so every group element operates on V by scalar multiplications. Therefore, every subspace is invariant so irreducibility implies that $\dim_{\mathbb{F}} V = 1$. □

Example 2.12. Algebraic closedness is necessary: $G = C_3 = \{1, g, g^2\}$ can be represented in two real dimensions by $g \mapsto$rotation by $\frac{2\pi}{3}$. This is a 2 dimensional irreducible representation. Finite dimensionality is also necessary.

Remark 2.13. If G has some extra topological / differential geometric structure then it would make sense to consider only that representations that are compatible with that extra structure in some sense. In this case a fruitful idea is to consider the set $\{G \to \mathbb{F} \mid \text{compatible with our actual structure}\}$. This is a vector space by pointwise operations. However, by $G \circlearrowright G$ actions, this can be made into a G-module.

Important $G \circlearrowright G$ actions are left or right multiplication. A related action is $G \times G \to \mathrm{Perm}(G)$, $(g_1, g_2)(x) = g_1 x g_2^{-1}$. How do we get G-modules by these?

Definition 2.14. Suppose that $\sigma : G \to \mathrm{Sym}(X)$ is an action of G on X. Then by this, we can construct a representation $\tilde{\sigma} : G \to GL(\mathrm{Fun}(X, \mathbb{F}))$ where $\mathbb{F}$ is a field by the formula

$$\tilde{\sigma}(g) \ : \ \mathrm{Fun}(X, \mathbb{F}) \ni f \mapsto \big(x \mapsto f(g^{-1}x)\big)$$

So we got a representation of G on $\mathrm{Fun}(X, \mathbb{F})$.

Definition 2.15. A special case of the previous construction is the *two-sided regular representation*:

$$\mathrm{Reg} : G \times G \to GL(\mathrm{Fun}(G, \mathbb{F}))$$

$$(g_1, g_2)(f) = \big(x \mapsto f(g_1^{-1} x g_2)\big)$$

By composing from the right by $\eta_1 : G \to G \times G$, $g \mapsto (g, 1)$ or $\eta_2 : G \to G \times G$, $g \mapsto (1, g)$ one can get the *left* and the *right regular representation*

$$\mathrm{Reg} \circ \eta_1 : G \to GL(\mathrm{Fun}(G, \mathbb{F})) \qquad \mathrm{Reg} \circ \eta_2 : G \to GL(\mathrm{Fun}(G, \mathbb{F}))$$

$$g(f) = \big(x \mapsto f(g^{-1}x)\big) \qquad g(f) = \big(x \mapsto f(xg)\big)$$

Now, the goal is to prove that any irreducible representation is a subrepresentation of the one-sided regular representation. (Without any assumption on G). To get this, we first define the product of representations of two different group:

Definition 2.16. Let G_1 and G_2 two groups and $\rho_i : G_i \to GL(V_i)$ is a representation for each $(i = 1, 2)$. Then we can define the *product representation*:

$$\rho_1 \otimes \rho_2 : G_1 \times G_2 \to GL(V_1 \otimes V_2)$$

$$(g_1, g_2) \mapsto \big(v_1 \otimes v_2 \mapsto g_1 v_1 \otimes g_2 v_2\big)$$

Theorem 2.17. *Suppose that $\mathbb{F}$ is algebraically closed and $\rho_i : G_i \to GL(V_i)$ are finite dimensional irreducible representations of G_i for $i = 1, 2$. Then $\rho_1 \otimes \rho_2$ is an irreducible representation of $G_1 \times G_2$.*

Proof. Let $\eta_1 : G_1 \to G_1 \otimes G_2$ be $g_1 \mapsto (g_1, 1)$ and $\eta_2 : G_2 \to G_1 \otimes G_2$ be $g_2 \mapsto (1, g_2)$. By these we can consider $V_1 \otimes V_2$ as a G_1 and a G_2-module as well by $(\rho_1 \otimes \rho_2) \circ \eta_i$.

Lemma 2.18. *Any minimal G_1-invariant subspace in $V_1 \otimes V_2$ is of the form $V_1 \otimes f = \{v \otimes f \mid v \in V_1\}$ for some $f \in V_2$.*

Proof. Such subspace is clearly invariant and by $(\rho_1 \otimes \rho_2) \circ \eta_1|_{V_1 \otimes f} \cong \rho_1$ it is indeed irreducible. To get that these are the only one: take a basis $f_1, \dots, f_n$ of V_2. Then $V_1 \otimes V_2 \cong \oplus_{j=1}^n V_1 \otimes f_j$ as G_1-modules. Therefore, $(\rho_1 \otimes \rho_2) \circ \eta_1 \cong \rho_1 + \dots + \rho_1$ so it is a finite sum of irreducible representations. (In other words, the representation is semisimple.) Let V be a minimal nonzero G_1-invariant subspace in $V_1 \otimes V_2$. If we take an arbitrary $v \in V$ then

$$v = \pi_1(v) \otimes f_1 + \dots \pi_n(v) \otimes f_n$$

where π_i's are projections to V_1 defined in an obvious way. By Schur's lemma II, 2.10, if we fix a G-invariant isomorphism $\pi : V \to V_1$ then for every other π_i there exists a $\lambda_i \in \mathbb{F}$ such that $\pi_i = \lambda_i \pi$. Therefore

$$v = \pi_1(v) \otimes f_1 + \dots \pi_n(v) \otimes f_n = \lambda_1 \pi(v) \otimes f_1 + \dots \lambda_n \pi(v) \otimes f_n = \pi(v) \otimes (\lambda_1 f_1 + \dots + \lambda_n f_n)$$

for all $v \in V$ and that was the statement. □

Let us get back to the proof of the theorem. Take a non-zero $G_1 \times G_2$-invariant subspace $W \leq V_1 \otimes V_2$. Let $U \subseteq W$ be a minimal G_1-invariant subspace. By the Lemma, $U = V_1 \otimes f$ for some nonzero $f \in V_2$. Now let us define $S := \{h \in V_2 \mid V_1 \otimes h \subseteq W\} \subseteq V_2$. This is a G_2-invariant subspace which is nonzero since $f \in S$. Therefore, S must be the full space, so we got the statement. □

2.2 Spaces of Matrix elements

Definition 2.19. Let $\rho : G \to GL(V)$ be a finite dimensional representation. Choose a basis $e := e_1, \dots, e_n \in V$. Then $\big(\rho(g)\big)_e \in \mathbb{F}^{n \times n}$ such that the (i, j)-th entry of it is the i-th coordinate of $\rho(g)(e_i)$. In another notation we consider the functions:

$$\rho_{i,j} : G \to \mathbb{F} \qquad g \mapsto (i, j)\text{-th entry of } \big(\rho(g)\big)_e$$

(In other words, identify $GL(V)$ with $GL(\mathbb{F}^n)$ by the choice of e.)

By the above choice we can define

$$M(\rho) := \mathrm{Span}_{\mathbb{F}}\{\rho_{i,j} \mid 1 \leq i, j \leq n = \dim V\} \leq \mathrm{Fun}(G, \mathbb{F})$$

the *space of matrix elements* of the representations of ρ.

Remark 2.20. Note that it is does not depend on the choice of basis: let $f := f_1, \dots, f_n$ be another basis in V and let $S := \big((f_j)_e\big)_{j=1,\dots,n} \in \mathbb{F}^{n \times n}$. Then for a $v \in V$ we have

$$(v)_f = S^{-1} \cdot (v)_e$$

hence $\big(\rho(g)\big)_f = S^{-1}\big(\rho(g)\big)_e S$. In a totally basis-free terminology, for a finite dimensional representation $\rho : G \to GL(V)$, $M(\rho)$ consists of the functions $\big(g \mapsto \xi(gv)\big) \in \mathrm{Fun}(G, \mathbb{F})$ for all possible $v \in V$ and $\xi \in V^*$.

Lemma 2.21. *$M(\rho)$ is a $G \times G$ invariant subspace in $\mathrm{Fun}(G, \mathbb{F})$. What is more, if $\mathbb{F}$ is algebraically closed and ρ is irreducible then $\mathrm{Reg}_{M(\rho)} \cong \rho^* \otimes \rho$ where $\mathrm{Reg}_{M(\rho)} : G \times G \to GL(M(\rho))$ is $(g_1, g_2) \mapsto \mathrm{Reg}(g_1, g_2)|_{M(\rho)}$.*

Proof. Let $\mu : V^* \otimes V \to M(\rho) \subseteq \mathrm{Fun}(G, \mathbb{F})$ be $\xi \otimes v \mapsto \big(x \mapsto \xi(xv)\big)$. Now, choose a basis $e_1, \dots, e_n$ of V and take the corresponding dual basis ε_i such that $\varepsilon_i(e_j) = \delta_i^j$. This way the previous function can be written as

$$\mu : \xi \otimes v \mapsto \big(x \mapsto (\xi)_\varepsilon^T (\rho(x))_e (v)_e\big) \in M(\rho)$$

This shows that μ is a non-zero linear map because $\mu(\varepsilon_i \otimes e_j) = \rho_{ij}$ and it also shows that μ is surjective.

However, μ is also $G \times G$ equivariant because

$$\mu\big((\rho^* \otimes \rho)(g,h)(\xi \otimes v)\big) = \mu(g\xi \otimes hv) = \Big(x \mapsto g\xi(xhv)\Big) = \Big(x \mapsto \xi(g^{-1}xhv)\Big) = \mathrm{Reg}(g,h)\Big(x \mapsto \xi(xv)\Big)$$

It is clear that if ρ is irreducible then ρ^* is irreducible as well. Moreover, we have just seen that the product of two irreducible representations is an irreducible representation of the product. So a non-zero map from $V^* \otimes V$ has to be injective. Therefore, it is an isomorphism. □

Corollary 2.22. *Let Right-reg* $= \mathrm{Reg} \circ \eta_2$ *be the right regular representation. Then*

$$\textit{Right-reg}_{M(\rho)} \cong \rho + \rho + \cdots + \rho$$

where there are $\dim V$ *summands on the right hand side. (Similarly, for left regular representation)*

Proof. $M(\rho) \cong V^* \otimes V = \sum_{i=1}^n \varepsilon_i \otimes V$ where $\varepsilon_1, \dots, \varepsilon_n \in V^*$. □

Remark 2.23. The above mentioned argument works over an arbitrary (e.g. not necessarily finite) group for finite dimensional representations.

Corollary 2.24. *The subspaces* $M(\rho)$ *(as* ρ *ranges the isomorphism classes of irreducible representations of* G*) are linearly independent in* $\mathrm{Fun}(G, \mathbb{F})$ *so*

$$\bigoplus_{\rho \in \mathrm{Irrep}(G)} M(\rho) \subseteq \mathrm{Fun}(G, \mathbb{F})$$

Proof. $G \times G$ acts irreducibly and pairwise non-isomorphicly on the $M(\rho)'s$ because if $M(\rho) \cong M(\rho')$ as $G \times G$-modules then they are isomorphic as G-modules as well. However, then both sides are direct sums of ρ's and ρ''s respectively so $\rho \cong \rho'$. Linear independence follows from this because if $M(\rho) \cap \sum_{\rho \neq \rho'} M(\rho') \neq 0$ then we get contradiction by considering both sides of the intersection as G-modules (not as $G \times G$-modules): By irreducibility of $M(\rho)$, the intersection must be $M(\rho)$ itself if it is nonzero, but this would mean that ρ is a subrepresentation of $\sum_{\rho \neq \rho'} M(\rho')$ hence $\rho \cong \rho'$ for some ρ' by complete reducibility. That is a contradiction. □

Theorem 2.25. *If* G *is finite,* $\mathbb{F}$ *is algebraically closed and* $\mathrm{char}\,\mathbb{F} \not| \, |G|$ *then* $\mathrm{Fun}(G, \mathbb{F}) = \oplus_{i=1}^n M(\rho_i)$ *when* ρ_i *is a complete list of representatives of the isomorphism classes of the irreducible representations of* G*.*

Proof. By the theorem above, we only need to prove that $M(\rho_i)$'s span $\mathrm{Fun}(G, \mathbb{C})$. For this, let us denote the characteristic functions of the group elements by $e_g \in \mathrm{Fun}(G, \mathbb{F})$ and denote the corresponding basis $\{e_g \,|\, g \in G\}$ by e. It is enough to prove that $e_g \in \sum_{i=1}^n M(\rho_i) = \oplus_{i=1}^n M(\rho_i)$ for all $g \in G$. First, we only state that $e_g \in M(\text{Right-reg})$. Indeed, for an arbitrary $x \in G$ we can write

$$e_g(x) = e_g(1 \cdot x) = \big(\text{Right-reg}(x) \cdot e_g\big)(1) = \Big(\big(\text{Right-reg}(x)\big)_e\Big)_{1,g}$$

so $e_g(x)$ is nothing but the $(1,g)$-th of the matrix of Right-reg(x) expressed in the basis e. This prove$e_g \in M(\text{Right-reg})$.

To see $M(\text{Right-reg}) \subseteq \sum_{i=1}^n M(\rho_i)$, note that by Maschke's Theorem 1.56 and the assumptions, $\mathbb{F}G$ is semisimple hence all of its representations are completely reducible (by Proposition 1.36). In particular, the representation Right-reg too: we have Right-reg $= \oplus \rho_i^{\alpha_i}$ for some $\alpha_i \in \mathbb{N}$. Hence, $M(\text{Right-reg}) = M(\oplus \rho_i^{\alpha_i}) \subseteq \sum M(\rho_i)$. (For further clarification, see the next remark.) Therefore, $\mathrm{Fun}(G, \mathbb{F}) \subseteq M(\text{Right-reg}) \subseteq \oplus_{i=1}^n M(\rho_i)$. □

Remark 2.26. In the previous proof we used the following observation:

Let $\rho : G \to GL(V)$ be a representation and take an invariant subspace $W \subseteq V$. Fix a basis $e_1, \dots, e_k$ in W (in short e') and extend it by $e_{k+1}, \dots, e_n$ (in short e'') to get a basis e in V. Then $e_{k+1}+W, \dots, e_n+W \in V/W$ is of course a basis of V/W. In this case, we get a matrix-decomposition:

$$\big(\rho(g)\big)_e = \begin{pmatrix} \big(\rho_W(g)\big)_{e'} & * \\ 0 & \big(\rho_{V/W}(g)\big)_{e''} \end{pmatrix}$$

In a suitable basis, the matrix elements of ρ_W and $\rho_{V/W}$ are containing the matrix elements of ρ. Therefore, $M(\rho_W)$, $M(\rho_{V/W}) \subseteq M(\rho)$.

Moreover, if W has an invariant direct complement U in V, i.e. $V = W \oplus U$ then in a suitable basis $\big(\rho(g)\big)_e$ is block diagonal (because $* = 0$ in the above matrix) with blocks $\big(\rho_W(g)\big)_e$ and $\big(\rho_{V/W}(g)\big)_e = \big(\rho_U(g)\big)_e$. In such a basis the set of non-zero matrix elements of ρ is the union of the sets of non-zero matrix elements appearing in ρ_W and ρ_U. Therefore, $M(\rho) = M(\rho_W) + M(\rho_U)$, in particular, $M(\rho^\alpha) = M(\rho)$ for any $\alpha \in \mathbb{N}$.

2.3 Character theory

Theorem 2.27. *Let G be a finite group and $\mathbb{F}$ be an algebraically closed field. Then the number of non-isomorphic finite-dimensional irreducible representations is the same as the number of conjugacy classes of G.*

Proof. The plan is to realize both numbers as a dimension of some subspace of $\mathrm{Fun}(G, \mathbb{C})$. Let $\rho : G \to GL(V)$ be an irreducible representation. Then

$$M(\rho) \overset{G\times G}{\cong} V^* \otimes V \overset{G\times G}{\cong} \mathrm{End}_{\mathbb{F}}(V)$$

where the first isomorphism is seen in Lemma 2.21 and the latter is the usual identification $\xi \otimes v \mapsto (w \mapsto \xi(w)v)$ (linearly extended to the whole $V^* \otimes V$). The $G \times G$-module structure on $\mathrm{End}_{\mathbb{F}}(V)$ is given by $(g, h)(A) = \rho(h) \cdot A \cdot \rho(g^{-1})$. Before proceeding, we need another definition:

Definition 2.28. The *central functions* (or *class functions*) $\mathrm{Cent}(G, \mathbb{F}) \subseteq \mathrm{Fun}(G, \mathbb{F})$ are defined as

$$\mathrm{Cent}(G, \mathbb{F}) := \{f : G \to \mathbb{F} \mid \forall g, x \in G : \ f(x) = f(gxg^{-1})\}$$

In other words, $f \in \mathrm{Cent}(G, \mathbb{F})$ if and only if $\mathrm{Reg}(g, g)f = f$ for all $g \in G$. I.e. this is the fixed point set under the action $G \hookrightarrow G \times G \overset{\mathrm{Reg}}{\to} \mathrm{End}_{\mathbb{F}}(\mathrm{Fun}(G, \mathbb{F}))$.

Now, we can try to find the central functions inside $\mathrm{End}_{\mathbb{F}}(V) \cong M(\rho) \subseteq \mathrm{Fun}(G, \mathbb{F})$. These are exactly the transformations such that $\rho(g) \cdot A \cdot \rho(g^{-1}) = A$ for all $g \in G$, namely the module endomorphisms. By Schur's lemma 2.10, we know that this is true only for $\lambda \cdot \mathrm{Id}_V$ for $\lambda \in \mathbb{F}$. So we got that

$$M(\rho) \cap \mathrm{Cent}(G, \mathbb{F}) = \{\lambda \cdot \mathrm{Id}_V \mid \lambda \in \mathbb{F}\}$$

using the identification $\mathrm{End}_{\mathbb{F}}(V) \cong M(\rho)$.

Example 2.29. An example for such a central function is the character of a representation $\rho : G \to GL(V)$ namely $\mathrm{ch}_\rho : G \to \mathbb{F}$, $x \mapsto \mathrm{Tr}(\rho(x))$.

Remark 2.30. In fact, we proved above that $M(\rho) \cap \mathrm{Cent}(G, \mathbb{F}) = \mathbb{F} \cdot \mathrm{ch}_\rho$ for any non-zero irreducible representation $\rho : G \to GL(V)$. This follows from that $\mathrm{ch}_\rho$is an element of the 1-dimensional space $M(\rho) \cap \mathrm{Cent}(G, \mathbb{F})$ or by the fact that the above isomorphism $\mathrm{End}_{\mathbb{F}}(V) \to M(\rho)$ is given by the formula $A \mapsto \big(x \mapsto \mathrm{Tr}(A \cdot \rho(x)\big)$. Note that the argument before the example works even without the assumption of $|G| < \infty$, we only need the finite-dimensionality of V and the algebraic closedness of the field.

Corollary 2.31. *Let G be a finite group and $\mathbb{F}$ be an algebraically closed field. Assume that* $\operatorname{char}\mathbb{F} \not| |G|$. *Let $\rho_1, \dots \rho_q$ be a complete list of irreducible representation. Then $\{\mathrm{ch}_{\rho_i} \mid i = 1, \dots, q\}$ is an $\mathbb{F}$-vector space basis of* $\mathrm{Cent}(G, \mathbb{F})$.

Proof. Use theorem 2.25 that states $\mathrm{Fun}(G, \mathbb{F}) = \oplus_{i=1}^{q} M(\rho_i)$. Then any $f \in \mathrm{Cent}(G, \mathbb{F}) = \oplus_{i=1}^{q}\big(M(\rho_i) \cap \mathrm{Cent}(G, \mathbb{F})\big)$ can be decomposed as $f = f_1 + \dots + f_q$. However, by the previous observation that $M(\rho_i) \cap \mathrm{Cent}(G, \mathbb{F})$ is one dimensional i.e. $f_i = \lambda_i \cdot \mathrm{ch}_{\rho_i}$ so we got the statement of the corollary. □

Back to the proof of theorem 2.27: One can easily notice that $\dim_{\mathbb{F}}\mathrm{Cent}(G, \mathbb{F})$ is the number of conjugacy classes in G (since the functions on G fixed under conjugation with every group element are exactly the functions that are constant along cnojugacy classes). So Corollary 2.31 gives us the statement. □

Corollary 2.32. *If* $\mathrm{char}\mathbb{F} = 0$ *and G is a finite group and ρ, ψ are finite dimensional representations of G such that* $\mathrm{ch}_\rho = \mathrm{ch}_\psi$. *Then $\rho \cong \psi$.*

Proof. By Maschke's theorem 1.56: $\rho \cong \sum_{i=1}^{q} m_i\rho_i$ for some $m_i \in \mathbb{N}$. Then the character of ρ is $\sum_{i=1}^{q} m_i\mathrm{ch}_{\rho_i}$. However, ch_{ρ_i}'s are linearly independent. Therefore, the decomposition of $\mathrm{ch}_\rho = \mathrm{ch}_\psi$ determines the coefficients m_i so it basically determines the decomposition of ρ and ψ as well. □

2.4 Unitary case

Assumption: From now on, $\mathbb{F} = \mathbb{C}$.

Definition 2.33. Let V be a finite-dimensional vector space over $\mathbb{C}$. A *scalar-product* β on V is a $\frac{1}{2} - 1$ linear positive definite Hermitian form on V, (sometimes it is called sesqui-linear) i.e. $\beta : V \times V \to \mathbb{C}$ is

1. $\mathbb{C}$-linear in the second argument,
2. $\beta(x, y) = \overline{\beta(y, x)}$ (this is called Hermitianity. By these two, β is conjugate-linear or half-linear in the first argument)
3. $\beta(x, x) \geq 0$ with equality only if $x = 0$. (by 2. $\beta(x, x)$ is always real, but we even require it to be positive on nonzero vectors. It is called positive definiteness.)

Usual notation: $\beta(x, y) = \langle x, y\rangle$.

Definition 2.34. Let V be a finite-dimensional $\mathbb{C}$-vector space with a fixed scalar product $\langle ., .\rangle$. Then we can define

$$\mathrm{End}_{\mathbb{C}}(V) \supseteq U(V) := \{A \in \mathrm{End}_{\mathbb{C}}(V) \mid \langle Ax, Ay\rangle = \langle x, y\rangle \ \forall x, y \in V\}$$

In the case of $V = \mathbb{C}^n$ we get

$$GL_n(\mathbb{C}) \supseteq U_n(\mathbb{C}) = \{A \in \mathbb{C}^{n\times n} \mid A^*A = I\}$$

where A^* is the transpose of the element-wise conjugate of A.

Remark 2.35. The real version of it is the orthogonal group:

$$GL_n(\mathbb{R}) \supseteq O_n(\mathbb{R}) := \{A \in \mathbb{R}^{n\times n} \mid A^TA = I\}$$

Lemma 2.36. *Let $\rho : G \to GL(V)$ be a finite-dimensional complex representation of a finite group G. There exists a scalar product $\langle ., .\rangle$ on V such that $\rho(G) \subseteq U(V)$.*

Proof. Let β be an arbitrary such product on V. Define $\langle x, y\rangle := \sum_{g\in G} \beta(gx, gy)$. It is straightforward to check that it is a scalar product and it is clearly G-invariant. □

Corollary 2.37. *A finite dimensional complex representation of a finite group is completely reducible.*

Proof. Let $\rho : G \to GL(V)$ be a representation. Take an invariant scalar product on V, so $\rho(G) \subseteq U(V)$. Let W be an invariant subspace in V. Then $V = W \oplus W^\perp$ as $\mathbb{F}$-vector spaces where $W^\perp$ is the orthogonal complement of W with the given invariant scalar product. What is more, $W^\perp$ is also an invariant subspace because for $x \in W^\perp$ and for arbitrary $g \in G$ and $w \in W$ we get

$$\langle gx, w\rangle = \langle g^{-1}gx, g^{-1}w\rangle = \langle x, g^{-1}w\rangle = 0$$

because $g^{-1}w \in W$. So we got the theorem. □

Lemma 2.38. *Let $\rho : G \to GL(V)$ be a finite dimensional complex irreducible representation of a group G. Then up to scalar multiple there can be only one G-invariant scalar product on V.*

Proof. Suppose $\langle .,. \rangle$ is a G-invariant scalar product on V and let $e_1, \dots, e_n$ be an orthonormal basis in V. Then we, in principle, identified V with $\mathbb{C}^n$ and $(x, y) \mapsto \langle x, y\rangle$ with $(x, y) \mapsto (x)_e^* \cdot (y)_e$. Let β be a (possibly different) G-invariant scalar product on V. Then there exists a $B \in \mathbb{C}^{n\times n}$ such that $\beta(x, y) = x^*By$. However, in this case

$$x^*By = \beta(x, y) = \beta(gx, gy) = x^*\rho(g)^*B\rho(g)y$$

for all $x, y \in \mathbb{C}^n$. So $B = \rho(g)^*B\rho(g) = \rho(g)^{-1}B\rho(g)$ because $\rho(g)^* = \rho(g)^{-1}$ by unitarity. Therefore, $\rho(g)B = B\rho(g)$ so – By Schur's lemma 2.10 – we got that $B = \lambda \cdot I_n$. □

Lemma 2.39. *Let $\rho : G \to GL(V)$ be a finite dimensional complex representation of a group G. If G acts irreducibly and non-isomorphicly on two invariant subspaces U and $W \leq V$ then $U \perp W$ with respect to any invariant scalar product.*

Remark 2.40. Note that we did not assume the finiteness of G here.

Proof. If there is no such scalar product then we did not state anything. So let $\langle .,. \rangle$ be an invariant scalar product on V. Consider the decomposition $V = W \oplus W^\perp$. Let us denote by π the projection $\pi : V \to W \leq W \oplus U$ by "projecting on the first coordinate". It is clear that $\ker \pi = W^\perp$. Since W and $W^\perp$ are both G-invariant subspaces and π is G-equivariant because elementwise it is given as $gv = gw + gw' \overset{\pi}{\mapsto} gw$.

Now, consider $\pi|_U : U \to W$. It is a G-equivariant linear map and $\rho_U \ncong \rho_W$ so by Schur's lemma I (2.10) we get that $\pi = 0$. Therefore $U \subseteq \ker\pi = W^\perp$. By counting dimensions, we get the statement. □

Let G be a finite group and let $\rho^{(1)}, \dots, \rho^{(q)}$ be the irreducible representations of G over $\mathbb{C}$, i.e. $\rho^{(k)} : G \to GL(V_k)$. Let us denote by $n_k = \dim_{\mathbb{C}} V_k$. In each V_k take an invariant scalar product (this is essentially unique by Lemma 2.38) and take an orthonormal basis in V_k with respect to the invariant scalar product. Let $\rho_{ij}^{(k)}(g)$ be the (i, j)-th matrix element of $\rho^{(k)}(g)$.

Definition 2.41. On the space $\mathrm{Fun}(G, \mathbb{C})$ there is a natural $G \times G$-invariant scalar product:

$$\langle f, h\rangle := \frac{1}{|G|}\sum_{g\in G} \overline{f(g)}h(g)$$

Theorem 2.42. $\{\rho_{ij}^{(k)} \mid , k \leq q, i \leq n_k, j \leq n_k\}$ *is an orthogonal basis in* $\mathrm{Fun}(G, \mathbb{C})$. *Moreover,* $\langle \rho_{ij}^{(k)}, \rho_{ij}^{(k)}\rangle = \frac{1}{n_k}$ *for all* k, i, j.

In short, the unitary matrix elements of the irreducible representations of G constitute an orthonormal basis in $\mathrm{Fun}(G, \mathbb{C})$.

Remark 2.43. It is the finite group-theoretic version of the Peter-Weyl theorem in harmonic analysis.

Proof. $G \times G$ acts irreducibly and pairwise non-isomorphically on the spaces $M(\rho^{(k)})$ hence by Lemma 2.39 $M(\rho^{(k)}) \perp M(\rho^{(l)})$ for all $k \neq l$.

Now, to simplify the notation, let $\rho = \rho^{(k)}$, $\rho_{ij} = \rho_{ij}^{(k)}$, $V = V_k$, $n = n_k$ and let $e_1, \dots, e_n$ be an orthonormal basis in V with respect to an invariant scalar product $[.,.]$ on V. Now, we can consider the $G \times G$-module isomorphism:

$$\eta:\ \mathrm{End}_{\mathbb{C}}(V)\to M(\rho)$$
$$A\mapsto \big(x\mapsto \mathrm{Tr}(A\cdot\rho(x)\big)$$

On the space $\mathrm{End}_{\mathbb{C}}(V)$ there is a natural $G\times G$-invariant scalar product $(A,B)\overset{\beta}{\to}\mathrm{Tr}(A^*B)$ for $A,B\in\mathrm{End}_{\mathbb{C}}(V)$. With respect to this scalar product E_{ij}'s give an orthonormal basis.

By the above isomorphism η we can get an induced scalar product $(f,h)\mapsto\beta(\eta^{-1}(f),\eta^{-1}(h))$ on $M(\rho)$. However, by Lemma 2.38, the invariant scalar product is unique up to scalar multiple so there exists a $\lambda\in\mathbb{C}$ such that

$$\beta\big(\eta^{-1}(f),\eta^{-1}(h)\big)=\lambda\langle f,h\rangle$$

Besides,

$$\eta(E_{ij})=\big(x\mapsto\mathrm{Tr}(E_{ij}^*\rho(x))\big)=\big(x\mapsto\mathrm{Tr}(E_{ji}\rho(x))\big)=\rho_{ij}(x)$$

therefore we got that

$$\langle\rho_{ij},\rho_{kl}\rangle=\begin{cases}\frac{1}{\lambda} & \text{if } (i,j)=(k,l)\\ 0 & \text{else}\end{cases}$$

where λ does not depend on i,j,k,l. Now, we only have to show that $\lambda=\dim V$.

$$\frac{n}{\lambda}=\sum_{i=1}^{n}\langle\rho_{ij},\rho_{ij}\rangle=\sum_{i=1}^{n}\frac{1}{|G|}\sum_{g\in G}\overline{\rho_{ij}(g)}\rho_{ij}(g)=\frac{1}{|G|}\sum_{g\in G}\sum_{i=1}^{n}\overline{\rho_{ij}(g)}\rho_{ij}(g)=\frac{1}{|G|}\sum_{g\in G}1=1$$

where we used that $\rho(g)$ is a unitary matrix so its rows and columns have length one. □

Corollary 2.44. *The characters* $\mathrm{ch}_{\rho^{(1)}},\dots,\mathrm{ch}_{\rho^{(q)}}$ *is an orthonormal basis in* $\mathrm{Cent}(G,\mathbb{C})$.

Proof.

$$\langle\mathrm{ch}_{\rho^{(k)}},\mathrm{ch}_{\rho^{(l)}}\rangle=\Big\langle\sum_{i=1}^{n_k}\rho_{ii}^{(k)},\sum_{j=1}^{n_l}\rho_{jj}^{(l)}\Big\rangle=\sum_{i=1}^{n_k}\sum_{j=1}^{n_l}\langle\rho_{ii}^{(k)},\rho_{jj}^{(l)}\rangle=\begin{cases}n_k\frac{1}{n_k}=1 & \text{if } k=l\\ 0 & \text{else}\end{cases}$$

□

Corollary 2.45. *Let* ρ *be a finite dimensional complex representation of a finite group* G*. Then*

1. $\rho\cong\sum_{i=1}^{q}\langle\mathrm{ch}_{\rho^{(k)}},\mathrm{ch}_{\rho}\rangle\rho^{(k)}$
2. ρ *is irreducible if and only if* $\langle\mathrm{ch}_{\rho},\mathrm{ch}_{\rho}\rangle=1$

Proof. The first is the straightforward consequence of Corollary 2.44. The second one can be deduced by taking the decomposition $\rho=\sum_i m_i\rho^{(i)}$ so one gets that $\langle\mathrm{ch}_{\rho},\mathrm{ch}_{\rho}\rangle=\sum_i m_i^2$. □

Sixth Lecture, 4th of November

Definition 2.46. *Character table:* Let G be a finite group, $\rho_1,\dots,\rho_q$ be a complete list of irreducible representations of G. Denote their characters by $\chi_i:=\mathrm{ch}_{\rho_i}$. Denote the conjugacy classes of G by $\mathcal{C}_1,\dots,\mathcal{C}_q$ (Note that we already proved in Theorem 2.27 that the number of conjugacy classes and the number of irreducible representations are the same.)

We use the following notation if e is a conjugacy class then $\chi_i(\mathcal{C}):=\chi_i(x)$ for arbitrary $x\in\mathcal{C}$. We know that characters are conjugacy invariant so this is a definition. Now, the character table of G is a $q\times q$ matrix over $\mathbb{C}$ such that its (i,j)-th entry is $\chi_i(\mathcal{C}_j)$.

Remark 2.47. The first row is: $\chi_i(1)=\dim_{\mathbb{C}}(V)$ and the first column is conventionally corresponding to the trivial representation so $\chi_1(\mathcal{C}_j)=1$ for all $j=1,\dots,q$.

Example 2.48. For character tables:

1. Let $G = \langle g \mid g^3 = 1 \rangle$. Then the character table is

$$\begin{bmatrix} & \{1\} & \{g\} & \{g^2\} \\ \hline \text{triv} & 1 & 1 & 1 \\ \chi_2 & 1 & \omega & \omega^2 \\ \chi_3 & 1 & \omega^2 & \omega \end{bmatrix}$$

2. Let $G = S_3 \cong D_3$. Then the character table is the following:

$$\begin{bmatrix} & \{\text{id}\} & \{(123),(321)\} & \{(12),(23),(13)\} \\ \hline \text{triv} & 1 & 1 & 1 \\ \text{sign} & 1 & 1 & -1 \\ D_3 & 2 & -1 & 0 \end{bmatrix}$$

Remark 2.49. We can reinterpret the orthonormality of characters in the terms of the character table:

$$\delta_i^j = \langle \chi_i, \chi_j \rangle = \frac{1}{|G|} \sum_{k=1}^{q} \overline{\chi_i(\mathcal{C}_k)} \chi_j(\mathcal{C}_k) \cdot |\mathcal{C}_k| = \sum_{k=1}^{q} \sqrt{\frac{|C_k|}{|G|}} \chi_i(\mathcal{C}_k) \sqrt{\frac{|C_k|}{|G|}} \chi_j(\mathcal{C}_k)$$

so if M stands for the character table, then let us introduce another $q \times q$ matrix N that is a modified version of M: divide every column by $\sqrt{\frac{|C_k|}{|G|}}$. By this we get the following:

Proposition 2.50. *$N \cdot N^* = I$ i.e. the rows of N form an orthonormal basis with respect to the usual scalar product of $\mathbb{C}^q$.*

Corollary 2.51. *$N^* \cdot N = I$ by simple linear algebra. This can be expanded:*

$$\sum_{i=1}^{q} \overline{\chi_i(\mathcal{C}_k)} \chi_i(\mathcal{C}_l) = \begin{cases} 0 & \text{if } k \neq l \\ \frac{|G|}{|\mathcal{C}_k|} & \text{if } k = l \end{cases}$$

This system of equations is called the Second Orthogonality Relation. (Pretty useful to compute explicit character tables.)

2.5 Integrality

Definition 2.52. Let R be an integral domain ($1 \in R$ commutative that has no zero-divisors). Let $S \leq R$ be a unital subring. Then $\alpha \in R$ is *integral* over S if there exists a monic polynomial $f \in S[x]$ such that $f(\alpha) = 0$.

Lemma 2.53. *Let S be a unital subring of R and $\alpha \in R$. Then the following are equivalent:*

1. *α is integral over S*
2. *There exists a subring $T \leq R$ such that $S \subseteq T \subseteq R$ such that $\alpha \in T$ and T is a finitely generated S-module.*

Proof. Direction 1) $\Rightarrow$ 2): If α is integral then we can take a polynomial $f(x) = x^n + \sum_{j=0}^{n-1} a_j x^j$ such that $f(\alpha) = 0$. Then by $T := \sum S\alpha^i$ we get a subset such that $S \subseteq T \subseteq R$ that is clearly finitely generated over S. So we only have to see that it is a subring, but by the relation $f(\alpha) = 0$ i.e. $\alpha^n = -\sum_{j=0}^{n-1} a_j \alpha^j$ it is indeed closed under multiplication.

Direction 2) $\Rightarrow$ 1): Suppose that $\alpha \in T$ where T is a finitely generated unital subring. Let us take a finite S-generator system of T: $e_1, \ldots, e_n$. Then α "acts" on T by left multiplication, namely $\alpha \cdot e_i = \sum_{j=1}^{n} a_{ij} e_j$ for some $a_{ij} \in S$, $i, j = 1, \ldots, n$. (These coefficients may be highly non-unique.) By the matrix $((a_{ij}))$ we

can define the monic polynomial that will prove the integrality of α: let $f = \det(x \cdot I_n - A) \in S[x]$. (The elements of $A = ((a_{ij}))$ are in S so $f \in S[x]$.)

By the definition it is clear that f is monic so we only have to prove that $f(\alpha) = 0$. By linear algebra we know that $f(\alpha) \cdot z = f(A) \cdot z$ for all $z \in T$. However, by the Cayley-Hamilton theorem $f(A) = 0$, so $f(\alpha) \cdot z = 0$. But T is a domain so $f(\alpha) = 0$. □

Corollary 2.54. *Let $S \subseteq R$ be a unital subring. Then $\{\alpha \in R \mid \alpha$ is integral over $R\}$ is a subring of R.*

Proof. Fix an α and β that are integral over S. By the above lemma, we have to find a finitely S-generated subring $W \leq R$ such that $\alpha \pm \beta \in W$ and $\alpha \cdot \beta \in W$. So, by the above lemma again, take a finitely S-generated unital subring $T \leq R$ such that $\alpha \in T$ and a similar subring U such that $\beta \in U$. Then $W = \mathrm{Span}_S\{tu \mid t \in T, u \in U\}$ satisfies the above conditions. □

Remark 2.55. The above defined set $\{\alpha \in R \mid \alpha$ is integral over $R\}$ in the case $R = \mathbb{C}$ and $S = \mathbb{Z}$ is called *algebraic integers*.

Fact 2.56. *The character values of a finite group are algebraic integers.*

Proof. $\rho(g)^{|G|} = \mathrm{id}_V$ for an arbitrary representation $\rho : G \to GL(V)$. So the complex eigenvalues of $\rho(g)$ are $|G|$-th roots of the unity. □

Lemma 2.57. *Let $\chi = \mathrm{ch}_\rho$ where $\rho : G \to GL(V)$ is an arbitrary irreducible representation of a finite group G. Let $\mathcal{C}$ be a conjugacy class of G. Then $\frac{\chi(\mathcal{C})}{\chi(1)}|\mathcal{C}|$ is an algebraic integer.*

Proof. Let $\mathcal{C}_1, \ldots, \mathcal{C}_q$ be the conjugacy classes in G. Take the basis $c_k = \sum_{g \in C_k} g$ of the subspace of central elements of $\mathbb{C}G$. Then $c_i c_j = \sum_k m_{ijk} c_k$. These coefficients can be explicitly computed: take an arbitrary $x \in C_k$

$$m_{ijk} = |\{(y, z) \in C_i \times C_j \mid yz = x\}| \in \mathbb{Z}$$

However, c_k is a central element, so – by Schur's lemma 2.10 – $\rho(c_k)$ is a scalar transformation because of the irreducibility of V. So take the trace:

$$\mathrm{Tr}(\rho(c_k)) = \chi(c_k) = \sum_{g \in C_k} \chi(g) = |\mathcal{C}|\chi(c_k)$$

therefore the elements of the diagonal in the scalar matrix corresponding to $\rho(c_k)$ are exactly $\frac{\chi(\mathcal{C})}{\chi(1)}|\mathcal{C}| =: b_j$. By $c_i c_j = \sum_k m_{ijk} c_k$ (where c_i's are scalar matrices) we clearly get that $b_i b_j = \sum_k m_{ijk} b_k$ for all i, j where one should not forget that $m_{ijk} \in \mathbb{Z}$. This means that $\mathrm{Span}_{\mathbb{Z}}(1, b_i \mid i)$ is a finitely $\mathbb{Z}$-generated subring of $\mathbb{C}$ so by Lemma 2.53 we got that b_i's are algebraic integers. □

Corollary 2.58. *Let $\rho : G \to GL(V)$ be an irreducible complex representation of a finite group G. Then* $\dim V \mid |G|$.

Proof.

$$1 = \langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{k=1}^{q} \overline{\chi(\mathcal{C}_k)} \chi(\mathcal{C}_k) |\mathcal{C}_k|$$

$$\frac{|G|}{\chi(1)} = \sum_{k=1}^{q} \overline{\chi(\mathcal{C}_k)} \frac{\chi(\mathcal{C}_k)|\mathcal{C}_k|}{\chi(1)} \in \text{algebraic integers}$$

Therefore $\frac{|G|}{\chi(1)} \in \mathbb{Q} \cap \{\text{algebraic integers}\} = \mathbb{Z}$. □

Proposition 2.59. *Let $\chi := \mathrm{ch}_\rho$ a character of an irreducible complex representation $\rho : G \to GL(V)$ of a finite group G. Let $\mathcal{C}$ be a conjugacy class in G such that* $\mathrm{hcd}(|\mathcal{C}|, \dim(V)) = 1$. *Then for all $g \in \mathcal{C}$ either $\chi(g) = 0$ or $\chi(g) \in \mathbb{C} \cdot \mathrm{id}_V$.*

Proof. By the assumption, there exist $l, m \in \mathbb{Z}$ such that $l \cdot |\mathcal{C}| + m\chi(1) = 1$. Then

$$\frac{\chi(g)}{\chi(1)} = l \cdot \frac{\chi(\mathcal{C})}{\chi(1)}|\mathcal{C}| + m\chi(g)$$

i.e. we get that $\frac{\chi(g)}{\chi(1)}$ is an algebraic integer because it is a sum of algebraic integers. It would be enough to prove that its absolute value is also in $\mathbb{Q}$ and that will imply the statement. That is not a realizable idea, but something like that will happen with the help of some elementary Galois theory.

We know that $\chi(g) = \sum_{j=1}^{n} \omega_j$ where ω_j's are roots of 1 and $n = \dim V$. Take the field $\mathbb{F} = \mathbb{Q}(\omega_1, \ldots, \omega_n)$ i.e. the field extension by ω_j's. $\mathbb{F} \mid \mathbb{Q}$ is a Galois extension (known) so we can take the Galois group $H := \mathrm{Aut}(\mathbb{F} : \mathbb{Q})$. Take $s \in H$ arbitrarily. Then

$$s(\chi(g)) = \sum_{j=1}^{n} s(\omega_j)$$

$$|s(\chi(g))| \leq \sum_{j=1}^{n} |s(\omega_j)| = n$$

because $s(\omega_j)$'s are roots of unity, and equality happens only if all the ω_j's are the same. In that case $\rho(g) \in \mathbb{C} \cdot \mathrm{id}_V$ so we are trying to get that either equality holds or $\chi(g) = 0$.

We know (it is obvious) that $s \in H$ brings algebraic integers into algebraic integers, and the product of them is also an algebraic integer. Therefore,

$$\prod_{s \in H} \frac{s(\chi(g))}{\chi(1)} \in \mathbb{F}^H \cap \{\text{algebraic integers}\} = \mathbb{Q} \cap \{\text{algebraic integers}\} = \mathbb{Z}$$

However, all the terms in the product have $|z| \leq 1$. So either $z = 0$ or $|z| = 1$. So we got that for all $g \in G$ either $\chi(g) = 0$ or $\left|\frac{\chi(g)}{\chi(1)}\right| = 1$ and that was the statement. □

Theorem 2.60. *The size of the conjugacy class in a non-abelian simple group is never a positive power of a prime.*

Proof. Assume indirectly that $|\mathcal{C}| = p^k$. By the orthogonality of the rows of the character table, we get

$$0 = \sum_{i=1}^{q} \chi_i(1)\chi_i(\mathcal{C}) = 1 + \sum_{i=2}^{q} \chi_i(1)\chi_i(\mathcal{C})$$

Now we take a few observations before rearranging the above equation.

1. Since G is simple ρ_i's are all faithful (on G), i.e. $G \cong \rho_i(G)$.
2. $G_\rho = \{g \in G \mid \rho(g) \in \mathbb{C} \cdot \mathrm{id}_V\} \lhd G$ for any representation $|G|$. Therefore, $G_\rho = \{1\}$ for all representations because G is simple.
3. By the previous proposition, we get that either $p \mid \chi_i(1)$ or $\chi_i(\mathcal{C}) = 0$

Therefore we can exclude those summands such that $p \nmid \chi_i(1)$. So we get

$$-\frac{1}{p} = \sum_{i : p \mid \chi_i(1)} \frac{\chi_i(1)}{p}\chi_i(\mathcal{C}) \in \{\text{algebraic integers}\}$$

which is a contradiction. □

Goal: To prove Burnside's two prime theorem

Proposition 2.61. *A p-group has nontrivial center.*

Proof. If G acts on itself by conjugation then the orbits are exactly the conjugacy classes. By the orbit-stabilizer theorem, the orbits have prime-power size. However, the orbit of 1 has only one element. Therefore, there have to be another 1-element orbit because else 1 plus p powers cannot yield the p-power $|G|$. □

Corollary 2.62. *A finite p-group is solvable.*

Theorem 2.63. *If $|G| = p^\alpha q^\beta$ where p, q are primes and $\alpha, \beta \in \mathbb{N}$ then G is solvable.*

Proof. Let us take a minimal (with respect to $|G|$) counterexample. Then at least one of the composition factors of G (for an arbitrary composition series) is a counterexample as well. By minimality, this composition series has length one i.e. G must be non-abelian simple.

Let P be a Sylow p-subgroup of G and take an element $z \in Z(P)$. Then $C_G(z) \supseteq P$ so $|G : C_G(z)| =$ |conjugacy class of z| $\mid q^\beta$. However, this is a contradiction to Theorem 2.60. □

Example 2.64. $G = S_4$. The conjugacy classes contain the elements that have the same cycle-decomposition. The sizes of the classes are 1, 3, 8, 6 and 6 respectively. The obvious irreducible representations are the trivial and the sign representation. So we get:

$$\begin{bmatrix} & \text{id} & (ab)(cd) & (abc) & (ab) & (abcd) \\ \text{triv} & 1 & 1 & 1 & 1 & 1 \\ \text{sign} & 1 & 1 & 1 & -1 & -1 \\ ? & ? & ? & ? & ? & ? \\ ? & ? & ? & ? & ? & ? \\ ? & ? & ? & ? & ? & ? \end{bmatrix}$$

The commutator of S_4 is A_4 so there are no more 1-dimensional representations. The dimensions of the remaining representations are known by $\sum n_i^2 = |S_4| = 24$, since the only way to write 22 as a sum of three squares is $2^2 + 3^2 + 3^2$. To get the other representations, it is a good idea to take a factor of S_4, e.g. S_3 is a factor of S_4 that can be seen by the action on the 3-element conjugacy class $(ab)(cd)$. Then we can compute the character values from the character table of S_3 and get

$$\begin{bmatrix} & \text{id} & (ab)(cd) & (abc) & (ab) & (abcd) \\ \text{triv} & 1 & 1 & 1 & 1 & 1 \\ \text{sign} & 1 & 1 & 1 & -1 & -1 \\ S_4 \to S_3 & 2 & 2 & -1 & 0 & 0 \\ ? & 3 & ? & ? & ? & ? \\ ? & 3 & ? & ? & ? & ? \end{bmatrix}$$

The fourth representation is realized by action on the vertices of the tetrahedron embedded into the 3 dimensional space (where the center of the tetrahedron is the origin). So we get

$$\begin{bmatrix} & \text{id} & (ab)(cd) & (abc) & (ab) & (abcd) \\ \text{triv} & 1 & 1 & 1 & 1 & 1 \\ \text{sign} & 1 & 1 & 1 & -1 & -1 \\ S_4 \to S_3 & 2 & 2 & -1 & 0 & 0 \\ \text{tetrahedron} & 3 & -1 & 0 & 1 & ? \\ ? & 3 & ? & ? & ? & ? \end{bmatrix}$$

where the fact that $(ab)(cd)$ corresponds to a rotation by π, (abc) corresponds to a rotation by $\frac{2\pi}{3}$ and (ab) corresponds to a reflection. $(abcd)$ has no such easy interpretation but the value can be computed by the

orthogonality relations: it's -1. The last representation is the previous one tensored by the sign, so the full character table is:

$$\begin{bmatrix} & \mathrm{id} & (ab)(cd) & (abc) & (ab) & (abcd) \\ \text{triv} & 1 & 1 & 1 & 1 & 1 \\ \text{sign} & 1 & 1 & 1 & -1 & -1 \\ S_4 \to S_3 & 2 & 2 & -1 & 0 & 0 \\ \text{tetrahedron} & 3 & -1 & 0 & 1 & -1 \\ \chi_4 \cdot \text{sign} & 3 & -1 & 0 & -1 & 1 \end{bmatrix}$$

Remark 2.65. The last representation can be interpreted by the general method: if G acts on a set X then the vector space $\mathrm{Fun}(X, \mathbb{F})$ is a natural $\mathbb{F}G$-module. The corresponding character will be the number of fixed points.

Lemma 2.66. *If G acts on X 2-transitively then the corresponding character (called permutation character) is the trivial character plus one irreducible.*

Proof. One can prove that $\langle \mathrm{ch}_\rho, \mathrm{ch}_\rho \rangle = 2$ by 2-transitivity. But $\langle \mathrm{ch}_1, \mathrm{ch}_\rho \rangle = 1$ by transitivity so the statement follows. □

Seventh Lecture, 11th of November

3 Commutative algebra

Convention: From now on, a ring means commutative ring with unit element. In addition, frequently R is a $\mathbf{k}$-algebra where $\mathbf{k}$ is a field and we also assume that $\mathbf{1}_\mathbf{k} = \mathbf{1}_R$.

Example 3.1. $\mathbb{Q} \times \mathbb{Z}$ is not a $\mathbb{Q}$-algebra in this sense.

Definition 3.2. Let R be a commutative $\mathbf{k}$-algebra. Then $z_1, \ldots, z_n \in R$ are *algebraically independent* over $\mathbf{k}$ if for any non-zero polynomial $f(x_1, \ldots, x_n) \in \mathbf{k}[x_1, \ldots, x_n]$ $f(z_1, \ldots, z_n) \neq 0$.

Equivalently, $\mathbf{k}[z_1, \ldots, z_n]$ has to be isomorphic to the polynomial ring $\mathbf{k}[x_1, \ldots, x_n]$ as a $\mathbf{k}$-algebra.

Theorem 3.3. (Noether Normalization Lemma) *Let R be a finitely generated commutative $\mathbf{k}$-algebra. Then there exist $u_1, \ldots, u_n \in R$ algebraically independent over $\mathbf{k}$ such that R is a finitely generated module (in short: finite module) over the subalgebra $\mathbf{k}[u_1, \ldots, u_n]$.*

Remark 3.4. Equivalently, R is integral over $\mathbf{k}[u_1, \ldots, u_n]$.

Proof. We prove by induction on the number m of generators of R. Assume that $R = \mathbf{k}[z_1, \ldots, z_m]$ for some $m \in \mathbb{N}$, $z_i \in R$. If z_i's are algebraically independent then there is nothing to prove.

Otherwise, there exists a nonzero polynomial $F = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdot \ldots x_n^{i_n}$ such that $F(z_1, \ldots, z_n) = 0$. The problem is this F can be non-monic in every variable so our goal is to find a monic 1-variable polynomial and a suitable generating set that give a nontrivial relation. The trick is to take a "change of variables" of F where x_i's are translated by a large power of other x_i's. So take a positive integer C greater than any of the exponents appearing in F. Now, define the following:

$$v_1 := z_1, \quad v_2 := z_2 - z_1^C, \quad \ldots \quad v_i := z_i - z_1^{C^{i-1}} \quad \ldots \quad v_m = z_m - z_1^{C^{m-1}}$$

This change is invertible so $R = \mathbf{k}[v_1, \ldots, v_m]$. What is more, we can express the original monomials in z with v's:

$$z_1^{i_1} \cdot \ldots \cdot z_m^{i_m} = v_1^{i_1} \cdot \ldots \cdot (v_i + v_1^{C^{i-1}}) \cdot \ldots \cdot (v_m + v_1^{C^{m-1}}) = v_1^{i_1 + i_2 C + \cdots + i_m C^{m-1}} + \text{lower degree terms}$$

Therefore,

$$0 = F(z_1, \ldots, z_m) = G(v_1, \ldots, v_m)$$

where G is the polynomial we get from F by the above change of variables so

$$G(x_1,\dots,x_m) = a_{i_1,\dots,i_m} x_1^{i_1+i_2C+\dots+i_mC^{m-1}} + +\text{lower degree terms}$$

where $i_1,\dots,i_n$ is the greatest index in the anti-lexicographic order, i.e. it is the highest degree terms of G. By the assumption $0 \neq a_{i_1\dots,u_m} \in \mathbf{k}$ so we can divide by it. Then v_1 is integral over $\mathbf{k}[v_2,\dots,v_m]$.

By the induction hypothesis $S = \mathbf{k}[v_2,\dots,v_m]$ has a subalgebra P that is isomorphic to a polynomial algebra and S is finite over P. Then R is finite over P and we got the theorem. □

3.1 Transcendence degree

Definition 3.5. If $A \subseteq B$ is a commutative domain then $b \in B$ is *algebraic* over A if there exists a nonzero $f \in A[x]$ such that $f(b) = 0$.

Definition 3.6. Let R be a commutative $\mathbf{k}$-algebra. Then $r_1,\dots,r_n \in R$ is a *transcendence generating system* of R over $\mathbf{k}$ if R is algebraic over $\mathbf{k}[r_1,\dots,r_n]$.

An algebraically independent transcendence generating system is called *transcendence basis* of R over $\mathbf{k}$.

Definition 3.7. The *transcendence degree* $\mathrm{tr.deg}_{\mathbf{k}}(R)$ of R over $\mathbf{k}$ is the cardinality of a transcendence basis.

Fact 3.8. *It does not depend on the choice of the basis.*

Remark 3.9. The proof goes by proving the analog of the Exchange property. In this topic it is called Steinitz's Exchange Lemma.

Corollary 3.10. *The m in the Noether Normalization Lemma is unique, i.e. it is* $\mathrm{tr.deg}_{\mathbf{k}}(R)$.

3.2 Weak Nullstellensatz

Definition 3.11. Let $\mathbb{C}[x_1,\dots,x_n] \supseteq S$ and denote by $\mathcal{V}(S)$ the *common zero locus* of the elements of S. It is clear that $\mathcal{V}(S) = \mathcal{V}\big((S)\big)$. Therefore, it is enough to consider the $\mathcal{V}$'s of ideals. However, – by the Basissatz – every ideal is finitely generated so it is enough to consider $\mathcal{V}\big((f_1,\dots,f_n)\big)$'s. The following theorem describes an important property of these sets.

Theorem 3.12. *Let $f_1,\dots,f_d \in \mathbb{C}[x_1,\dots,x_n]$ and $f \in \mathbb{C}[x_1,\dots,x_n]$ such that f vanishes identically on $\mathcal{V}(f_1,\dots,f_d)$. Then there exists a positive integer N and polynomials $h_1,\dots,h_d \in \mathbb{C}[x_1,\dots,x_n]$ with*

$$f^N = \sum h_i f_i \in \mathbb{C}[x_1,\dots,x_n]$$

Lemma 3.13. *Let F be a field and let $R \subseteq F$ be a subring such that F is a finite R-module. Then R is a field.*

Proof. Take a nonzero $a \in R$. By the assumption $a^{-1} \in R$ is integral over R so there exists a $b_1,\dots,b_n \in R$ such that

$$(a^{-1})^n + b_1(a^{-1})^{n-1} \cdots + b_{n-1}a^{-1} + b_n = 0$$

multiply this by a^{n-1}:

$$a^{-1} = -b_1 - b_2a - \cdots - b_na^{n-1}$$

so $a^{-1} \in R$. □

Lemma 3.14. *Let $A \subseteq B$ be commutative domains, where B is a finitely generated as an algebra over A. (This is a lot less than assuming that B is finite as an A-module.) Assume that B is algebraic over A. Then there exists an $s \in A\backslash\{0\}$ such that $B[s^{-1}] \subseteq \mathrm{Frac}(B)$ is a finite $A[s^{-1}]$-module.*

Proof. By the assumptions, we can take elements $b_1, \ldots, b_n$ such that $B = A[b_1, \ldots, b_n]$. Then there exist nonzero $f_i \in A[x]$ such that $f_i(b_i) = 0$ (for all i). Let s be the product of the leading coefficients of f_i's. Clearly b_i's are integral over $A[s^{-1}]$. □

Lemma 3.15. (Zariski lemma) *Let* $\mathbf{k}$ *be a subfield of* F*. If* F *is a finitely generated* $\mathbf{k}$*-algebra then* $\dim_{\mathbf{k}} F < \infty$.

Proof. If F is algebraic over $\mathbf{k}$ then we are done. (In that case algebraic is the same as integrality so then F is finite over $\mathbf{k}$.) Suppose F is not algebraic. So let $z_1, \ldots, z_n$ be $\mathbf{k}$-algebra generators such that for some positive $n \leq m$, and $z_1, \ldots, z_n$ are algebraically independent over $\mathbf{k}$ and $z_{n+1}, \ldots, z_m$ are algebraic over $A = \mathbf{k}[z_1, \ldots, z_n]$. By the previous Lemma 3.14, there exists an $f \in \mathbf{k}[x_1, \ldots, x_n]$ such that for $s = f(z_1, \ldots, z_n)$ we have $F[s^{-1}] = F$ is integral over $A[s^{-1}]$. Therefore, by Lemma 3.13 $A[s^{-1}]$ is a field. However, this would mean that $\mathbf{k}[x_1, \ldots, x_n, \frac{1}{f(x_1, \ldots, x_n)}]$ is a subfield of $\mathbf{k}(x_1, \ldots, x_n)$ which is a contradiction (this would mean that for every polynomial $p \in \mathbf{k}[x_1, \ldots, x_n]$ we have $\frac{1}{p} = \frac{h}{f^d}$ for some h so $f^d = hd$ what would mean that there are only finitely many irreducible polynomials over $\mathbf{k}$ which is impossible). □

Remark 3.16. This lemma is also a corollary of the Noether Normalization Lemma 3.3

Definition 3.17. Let $ev_a : \mathbf{k}[x_1, \ldots, x_n] \to \mathbf{k}$ be the *evaluation homomorphism* $f \mapsto f(a_1, \ldots, a_n)$ at a point $a = (a_1, \ldots, a_n) \in \mathbf{k}^n$. Then

$$\mathrm{Ker}(ev_a) = \{f \mid f(a) = 0\} \lhd R[x_1, \ldots, x_n]$$

is a maximal.

Example 3.18. $\mathrm{Ker}(ev_a) = (x_1 - a_1, \ldots, x_n - a_n)$.

Theorem 3.19. (Weak Nullstellensatz) *If* $\mathbf{k}$ *is algebraically closed then the only maximal ideals in* $\mathbf{k}[x_1, \ldots, x_n]$ *are the ideals of the form* $(x_1 - a_1, \ldots, x_n - a_n)$ *for some* $(a_1, \ldots, a_n) \in \mathbf{k}^n$.

Proof. Take a maximal ideal M in $\mathbf{k}[x_1, \ldots, x_n]$ and consider $F = \mathbf{k}[x_1, \ldots, x_n]/M$. It is a field because M was maximal and it is a finitely generated $\mathbf{k}$-algebra (indeed, $x_i + M$'s generate it). By Lemma 3.15, F is a finite field extension of $\mathbf{k}$. This can happen only if $F = \mathbf{k}$ because $\mathbf{k}$ is algebraically closed. So every x_i's image is some $a_i \in \mathbf{k}$ under the factorization homomorphism. This gives the statement. □

3.3 Nullstellensatz

Lemma 3.20. *Let* S *be a* $\mathbf{k}$*-subalgebra of* R *where* R *is a finitely generated* $\mathbf{k}$*-algebra. Let* M *be a maximal ideal in* R*. Then* $M \cap S$ *is a maximal ideal in* S.

Remark 3.21. Without the assumption of "finitely generated"-ness, it is not true.

Proof. By Lemma 3.15 the factor ring R/M is a finite field extension of $\mathbf{k}$. Therefore, any $\mathbf{k}$-subalgebra T of F is in fact a subfield. In particular $S/M \cap S \subseteq R/M$ is a subfield as well so $M \cap S$ is a maximal ideal in S. □

Proposition 3.22. *The Jacobson radical of a finitely generated* $\mathbf{k}$*-algebra consists of nilpotent elements.*

Proof. Let R be a $\mathbf{k}$-algebra and take an $a \in \operatorname{rad} R$. By the previous Lemma, $\operatorname{rad}(R) \subseteq \operatorname{rad}(R[x])$. Hence, by a characterization of the Jacobson radical: $1 - ax \in R[x]$ is invertible. Therefore, there exist $c_0, \ldots, c_n \in R$ such that

$$(1 - ax)(c_0 + c_1 x^1 + \ldots c_n x^n) = 1 \in R[x]$$

Then one gets that $c_{i+1} - ac_i = 0$ for all $i = 0, \ldots n-1$ and by the main term $-ac_n = 0$. By substitution on gets that $a^{n+1} = 0$. Conversely, a nilpotent element generates a nilpotent ideal so by the generalities about Jacobson radical we get that it is in $\operatorname{rad} R$. □

Corollary 3.23. *For a finitely generated* $\mathbf{k}$*-algebra there exists some integer* d *such that* $\big(\operatorname{rad}(R)\big)^d = \{0\}$.

Proof. By the Hilbert Basis Theorem $\mathbf{k}[x_1, \dots, x_n]$ is Noetherian and we have a natural surjection $\mathbf{k}[x_1, \dots, x_n] \to R = \mathbf{k}[r_1, \dots, r_n]$ so the second is Noetherian as well. In particular $\operatorname{rad} R = Ra_1 + \cdots + Ra_n$ for some $a_1, \dots, a_n \in \operatorname{rad} R$. Let $n_i \in \mathbb{N}$ be such that $a_i^{n_i} = 0$. Then $n = 1 + \sum_{i=1}^{n}(n_i - 1)$ is such an integer that $(\operatorname{rad} R)^n = \{0\}$ by the pigeon-hole principle. □

Definition 3.24. Let $\mathbf{k}$ be an algebraically closed field. For a subset $X \subseteq \mathbf{k}^n$ the *vanishing ideal*

$$\mathcal{I}(X) := \{f \in \mathbf{k}[x_1, \dots, x_n] \mid f|_X \equiv 0\} \lhd \mathbf{k}[x_1, \dots, x_n]$$

It is a candidate for the inverse map of $\mathcal{V}$ seen in Definition 3.11. However, that is not totally true.

Definition 3.25. For an ideal $I \lhd R$ of an arbitrary commutative ring $\sqrt{I}$ stands for

$$\{f \in R \mid \exists n \in \mathbb{N}\ f^n \in I\}$$

called the *radical* of I.

In these terms, we can restate the Nullstellensatz:

Theorem 3.26. (Hilbert's Nullstellensatz) *Let* $\mathbf{k}$ *be an algebraically closed field. For any ideal* $I \lhd \mathbf{k}[x_1, \dots, x_n] =: R$ *we have*

$$\mathcal{I}\big(\mathcal{V}(I)\big) = \sqrt{I}$$

Proof. $\supseteq$ is trivial, by the definitions. To see the reverse, first let's understand the formula on the left:

$$\mathcal{I}(\mathcal{V}(I)) = \bigcap_{a \in \mathcal{V}(I)} \mathcal{I}\big(\{a\}\big) = \bigcap_{a \in \mathcal{V}(I)} \operatorname{Ker}(ev_a)$$

which means – by the Weak Nullstellensatz 3.19:

$$\mathcal{I}(\mathcal{V}(I)) = \bigcap \{M \mid R \rhd M \text{ maximal}, M \supseteq I\}$$

However, by the map $\eta : R \to R/I$ we can express this:

$$\eta^{-1}\Big(\operatorname{rad}\big(R/I\big)\Big) = \bigcap \{M \mid R \rhd M \text{ maximal}, M \supseteq I\}$$

by the definition of the radical. However, the previous Proposition 3.22 says that $\operatorname{rad}(R/I) = \{f \in R/I \mid f \text{ is nilpotent}\}$. Therefore,

$$\eta^{-1}\Big(\operatorname{rad}\big(R/I\big)\Big) = \Big\{f \in R \mid f^n \in I\Big\} = \sqrt{I}$$

and that was the statement.

Eighth Lecture, 18th of November □

Proposition 3.27. *Let* R *be a commutative ring. Then*

$$\operatorname{Nil}(R) = \bigcap_{P \lhd R \text{ prime}} P \subseteq \operatorname{rad}(R)$$

Moreover, if R *is Noetherian then* $\operatorname{Nil}(R)$ *is nilpotent.*

Proof. Indeed, $R/\operatorname{Nil}(R)$ contains no nilpotent elements so it contains no nilpotent ideals. Therefore, $R/\operatorname{Nil}(R)$ is semiprime so

$$\bigcap_{P \lhd R/\operatorname{Nil}(R) \text{ prime}} P = \{0\}$$

This yields the first equality. Besides, it is clear that $\operatorname{Nil}(R) \subseteq \operatorname{rad}(R)$ since the latter is the intersection of maximal ideals and every maximal ideal is prime. The Noetherian case follows from the fact that in a Noetherian ring, every ideal if finitely generated. □

Remark 3.28. If R is a finitely generated $\mathbf{k}$-algebra then $\operatorname{Nil}(R) = \operatorname{Rad}(R)$. (We have seen this implicitly last week 3.22)

3.4 Localization

Definition 3.29. Let R be a commutative ring, $S \subseteq R$ be a *multiplicative* subset (i.e. $1 \in S$, $0 \notin S$ and $s, t \in S \Rightarrow st \in S$). Then the *localization* of R with respect to S is

$$R[S^{-1}] = \left\{ \frac{a}{s} \mid a \in R,\ s \in S \right\}$$

where $\frac{a}{s}$ is an equivalence class $\big[(a, s)\big]$ in $R \times S$ with respect to the equivalence relation

$$(a, s) \sim (b, t) \iff \exists u \in S :\ u(at - bs) = 0 \in R$$

One can easily verify that it is indeed an equivalence relation.

$R[S^{-1}]$ can be endowed with a ring structure: the addition is defined as

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

and the multiplication via

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

The proof that these are well-defined and satisfy the ring axioms is straightforward hence omitted.

The ring $R[S^{-1}]$ is even an R-module because of the canonical ring homomorphism:

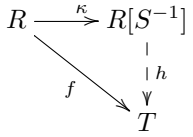
$$\kappa : R \to R[S^{-1}]$$

$$a \mapsto \frac{a}{1}$$

It is again omitted that it is indeed a homomorphism.

Remark 3.30. Note that the above κ is not necessarily injective. In fact, $\ker \kappa = \{a \in R \mid \exists s \in S :\ sa = 0\}$. Even so, the notation $J \cap R := \kappa^{-1}(J)$ is used for the ideal $J \lhd R[S^{-1}]$ supported by the natural intuition that κ is "usually" an embedding.

Proposition 3.31. *The localization of R with respect to a multiplicative set S is universal in the following sense: if $f : R \to T$ is any ring homomorphism such that $f(s) \subseteq T^\times$ then f factors through κ i.e. there exists a unique $h : R[S^{-1}] \to T$ such that $f = h \circ \kappa$. In diagram:*



has to be commutative.

Remark 3.32. The following basic facts help to relate the ideal-structure of R and $R[S^{-1}]$:

1. If $J \lhd R[S^{-1}]$ then $J = (J \cap R)R[S^{-1}] := \kappa(\kappa^{-1}(J)) \cdot R[S^{-1}]$ by the defining property of an ideal.
2. If $I \lhd R$ then $I \cdot R[S^{-1}] \cap R = (I : S) := \{a \in R \mid \exists s \in S,\ sa \in I\} \supseteq I$ obviously.
3. $I \cdot R[S^{-1}] = R[S^{-1}]$ if and only if $I \cap S = \emptyset$. To prove this note that $I \cdot R[S^{-1}]$ is an ideal in $R[S^{-1}]$ and an ideal is the whole ring if and only if it contains 1.

Proposition 3.33. *Every ideal in $R[S^{-1}]$ is of the form $I \cdot R[S^{-1}]$ for some $I \lhd R$. In other words, the map*

$$\psi : \mathrm{Ideals}(R) \to \mathrm{Ideals}(R[S^{-1}])$$

$$I \mapsto IR[S^{-1}]$$

is surjective. Moreover, ψ induces a bijection when restricted to the sets

$$\psi : \{P \lhd R \mid P \text{ is prime},\ P \cap S = \emptyset\} \longleftrightarrow \{Q \lhd R[S^{-1}] \mid Q \text{ is prime}\}$$

Proof. The surjectivity follows from the first part of the previous remark. To get the second part note that for a prime ideal Q we have $Q = (Q \cap R) \cdot R[S^{-1}]$ by again the first remark. Here $Q \cap R := \kappa^{-1}(Q)$ is prime because it is the preimage of a prime ideal.

To get injectivity, consider a prime ideal P of R that has $P \cap S = \emptyset$. Then the image $\psi(P) = PR[S^{-1}]$ is an ideal in $R[S^{-1}]$ such that $(P \cdot R[S^{-1}]) \cap R = P$ so ψ is in fact injective. We only need to prove that the image of ψ is in fact $\{Q \lhd R[S^{-1}] \mid Q \text{ is prime}\}$ and not bigger.

Let $P \lhd R$ be a prime ideal such that $P \cap S = \emptyset$. This latter property ensures that $\psi(P) \neq R[S^{-1}]$ by the third part of the previous remark. Besides, it is prime because if

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \in \psi(P)$$

then $\frac{ab}{1} \in \psi(P)$ is true as well. Hence, there exists a $z \in S$ such that $zab \in P$. But $z \notin P$ by $S \cap P = \emptyset$ so $ab \in P$ which implies $a \in P$ or $b \in P$. Therefore, either $\frac{a}{s} \in P$ or $\frac{b}{t} \in P$ and that proves the statement. $\square$

Remark 3.34. A short verbal conclusion is that there are more elements in $R[S^{-1}]$ but less prime ideals.

Example 3.35. Let A be a commutative ring and $P \lhd A$ a prime ideal. Set $S := A \backslash P$. This is a multiplicative set.

Notation: In the above setup $A_p := A[S^{-1}]$.

Remark 3.36. A_p is a local ring since $A_p \backslash PA_p = A_p^\times$ and if the non-unit elements in a ring constitute an ideal then the ring is local and this ideal is the unique maximal ideal of the ring.

Notation: $\mathrm{Spec}(A) := \{P \lhd A \mid P \text{ is prime}\}$ stands for the prime spectrum of A.With slight abuse of notation $\mathrm{Spec}(A[S^{-1}]) = \{P \in \mathrm{Spec}(A) \mid P \cap S = \emptyset\}$ with the identification induced by ψ.

3.5 Localization of modules

Definition 3.37. Let M be an A-module (where A is a commutative ring) and $S \subseteq A$ be a multiplicative set. Then

$$M[S^{-1}] := \left\{ \frac{m}{s} \mid m \in M,\ s \in S \right\} / \sim$$

where $\sim$ is the following equivalence relation:

$$\frac{m}{s} = \frac{n}{t} \iff \exists u \in S :\ v(tm - ns) = 0 \in M$$

It can be endowed with an $A[S^{-1}]$-module structure by the multiplication

$$\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}$$

It is straightforward to check that it is indeed a definition.

Proposition 3.38. *Localization is an exact covariant functor from the category of A-modules to the category of $A[S^{-1}]$-modules.*

Proof. To prove that it is functorial we have to define it on the morphisms (in a composition-preserving way). Given $f : M \to N$ let

$$f[S^{-1}] : M[S^{-1}] \to N[S^{-1}]$$
$$\frac{m}{s} \to \frac{f(m)}{s}$$

It is easy to check that $(g \circ f)[S^{-1}] = g \circ [S^{-1}] \circ f[S^{-1}]$.

To verify exactness, note that $[S^{-1}]$ brings monomorphisms into monomorphisms and epimorphisms into epimorphisms. So it is enough to prove that

$$(M/N)[S^{-1}] \cong M[S^{-1}]/N[S^{-1}]$$

with the induced map of the natural surjection $M[S^{-1}] \to (M/N)[S^{-1}]$. However, it is clear that the kernel is indeed zero because if $(M/N)[S^{-1}] \ni \frac{\overline{m}}{s} = 0$ then $\frac{\overline{m}}{s} = 0$ as well so $\exists t \in S$ such that $t\overline{m} = 0$. Therefore $tm = n \in N$ hence $\frac{m}{s} = \frac{1}{s}\frac{m}{1} = \frac{1}{s}\frac{n}{t} \in N[S^{-1}]$. □

3.6 Associated primes

Definition 3.39. Let M be an A-module. Then $P \in \mathrm{Spec}(A)$ is an *associated prime* of M if there exists a nonzero $x \in M$ such that $P = \mathrm{ann}(x) \lhd A$.

An element $a \in A$ is a *zero-divisor* on M if there exists a nonzero $x \in M$ such that $ax = 0$.

The set of all associated primes of M is denoted by $\mathrm{Ass}(M)$. While the *support* of M is

$$\mathrm{Supp}(M) := \{P \in \mathrm{Spec}(A) \mid P \supseteq \mathrm{Ann}(M)\}$$

which is exactly the set of primes such that $M_P \neq 0$ because if any murderer of M is not in the prison P then it can kill everyone i.e. $M_P = 0$ so P "does not support" M.

Remark 3.40. Trivially $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$ because if P is an associated prime, i.e. $P = \mathrm{ann}(x)$ for some $x \in M$ then x is in safety i.e. $M_P \ni \overline{x} \neq 0$.

Proposition 3.41. *Let A be a Noetherian ring and M be a non-zero module. Then*

1. *Every maximal element of the family $\mathcal{F} = \{\mathrm{ann}(x) \mid 0 \neq x \in M\}$ is a prime ideal. (In particular, $\mathrm{Ass}(M) \neq \emptyset$).*
2. *The zero-divisors of M is exactly $\cup_{P \in \mathrm{Ass}(M)} P$.*

Proof. Suppose that $\mathrm{ann}(x)$ is a maximal element in $\mathcal{F}$ and that $ab \in \mathrm{ann}(x)$. If $b \notin \mathrm{ann}(x)$ then $0 = (ab)x = a(bx)$ implies that $a \in \mathrm{ann}(bx) \supseteq \mathrm{ann}(x)$. By the maximality of $\mathrm{ann}(x)$ we get that $\mathrm{ann}(bx) = \mathrm{ann}(x)$ i.e. $a \in \mathrm{ann}(x)$ and then $\mathrm{ann}(x)$ is prime.

To prove the second statement, note that the $P \in \mathrm{Ass}(M)$ contain only zero-divisors. Conversely, suppose that $a \in A$ is a zero-divisor on M. So there exists a nonzero $x \in M$ such that $a \in \mathrm{ann}(x)$. Consider the following subset of $\mathcal{F}$:

$$\mathcal{F}' = \{\mathrm{ann}(y) \mid a \in \mathrm{ann}(y),\ y \neq 0\} \subseteq \mathcal{F}$$

This is nonzero since $\mathrm{ann}(x) \in \mathcal{F}'$ and it is closed under taking union. Therefore – by Zorn's lemma we can take a maximal element $\mathrm{ann}(z) \in \mathcal{F}'$ where $z \neq 0$. This $\mathrm{ann}(z)$ is obviously maximal in $\mathcal{F}$ too so – by the first part of the proof – it is a prime ideal and $a \in \mathrm{ann}(z) \in \mathrm{Ass}(M)$. □

Remark 3.42. Let P be a prime ideal. Then for the A-module A/P we have $\mathrm{Ass}(A/P) = \{P\}$ because P is prime so A/P is a domain.

Lemma 3.43. *If $N \leq M$ then $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N)$*

Proof. Suppose that $P \in \mathrm{Ass}(M)$ so $P = \mathrm{ann}(x)$ for some nonzero $x \in M$. Then

$$M \supseteq Ax \cong A/\mathrm{ann}(x) = A/P$$

so for any $y \in Ax\backslash\{0\}$ we have $\mathrm{ann}(y) = P$ by the previous Remark 3.42. Now, there are two cases: Either $Ax \cap N \neq \{0\}$ or it is zero.

In the first case there exists a nonzero $y \in N \cap Ax$ so $\mathrm{ann}(y) = P$ what means $P \in \mathrm{Ass}(N)$. In the second case $Ax \cap N = \{0\}$ so the natural surjection

$$\eta : M \to M/N$$

$$m \mapsto m + N$$

restricts to Ax as an injection i.e. $\eta : Ax \hookrightarrow M/N$. This means that for any nonzero $y \in \eta(Ax) \subseteq M/N$ we have $\mathrm{ann}(y) = P$ so $P \in \mathrm{Ass}(M/N)$. □

Proposition 3.44. *Let A be a Noetherian ring and M be a finitely generated A-module. Then there exists a chain*

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$$

of modules such that $M_i/M_{i-1} \cong A/P_i$ for some prime ideals $P_i \in \mathrm{Spec}(A)$.

Proof. By Proposition 3.41 there exists a $P_1 \in \mathrm{Ass}(M)$ such that $P_1 = \mathrm{ann}(x)$. Then immediately we got $M_1 := Ax$ for which

$$M_1/M_0 = M_1 = Ax \cong A/P_1$$

This argument can be iterated and by the Noetherian property of A we have the ascending chain condition on M so the procedure finishes in finitely many steps. □

Proposition 3.45. *Let $S \subseteq A$ be a multiplicative set.*

1. *Let N be an $A[S^{-1}]$-module (by $A \to A[S^{-1}]$ it is also an A-module). Then $\mathrm{Ass}_{A[S^{-1}]}(N) = \mathrm{Ass}_A(N)$ where we used the identification $\mathrm{Spec}(A[S^{-1}]) \hookrightarrow \mathrm{Spec}(A)$ seen in Proposition 3.33.*
2. *If A is Noetherian and M is an A-module then*

$$\mathrm{Ass}(M[S^{-1}]) = \mathrm{Ass}(M) \cap \mathrm{Spec}(A[S^{-1}])$$

with the identification $\mathrm{Ass}(M[S^{-1}]) \leftrightarrow \{P \in \mathrm{Ass}(M) \mid P \cap S = \emptyset\}$.

Proof. The first equality holds because

$$P = \mathrm{ann}_{A[S^{-1}]}\Big(\frac{x}{s}\Big) = \mathrm{ann}_{A[S^{-1}]}\Big(\frac{x}{1}\Big) = \mathrm{ann}_A(x) \cdot A[S^{-1}]$$

and $\mathrm{ann}(x) = P \cap A$ so the identification yields the equality.

To see the containment $\supseteq$ in the second statement consider a prime ideal $P \in \mathrm{Ass}(M) \cap \mathrm{Spec}(A[S^{-1}])$. Then $P \cap S = \emptyset$ and $P = \mathrm{ann}_A(x)$ for some nonzero $x \in M$. Now, if

$$\frac{a}{s} \cdot \frac{x}{1} = 0 \in M[S^{-1}] \qquad \text{i.e.} \qquad \exists t \in S : \ tax = 0$$

then – by $t \notin P = \mathrm{ann}_A(x)$ – $a \in P$. So

$$\mathrm{ann}_{A[S^{-1}]}\Big(\frac{x}{1}\Big) = P \cdot A[S^{-1}]$$

Conversely, if $P \in \mathrm{Ass}(M[S^{-1}])$ i.e. $P = \mathrm{ann}_{A[S^{-1}]}\Big(\frac{x}{1}\Big)$ for some $x \in M$ then take $\mathfrak{p} := P \cap A$. (For this, $P = \mathfrak{p}A[S^{-1}]$ by Proposition 3.33). Since A is Noetherian there exists an ideal-generating system

$\mathfrak{p} = (a_1, \dots, a_n) \lhd A$. For these $a_i \frac{x}{1} = 0$ holds $(i = 1, \dots, n)$ so for all there exists a $t_i \in S$ such that $t_i a_i x = 0$. Now, set

$$t := \prod_{i=1}^{n} t_i$$

For this element we have $a_i \in \operatorname{ann}(tx)$ by definition so $\operatorname{ann}_A(tx) \supseteq \mathfrak{p}$. However,

$$\operatorname{ann}_A(tx) \subseteq \operatorname{ann}_{A[S^{-1}]}\Big(\frac{tx}{1}\Big) = P \subseteq A$$

so $\operatorname{ann}_A(tx) \subseteq P \cap A = \mathfrak{p}$. This means that $\operatorname{ann}_A(tx) = \mathfrak{p}$ so $\mathfrak{p} \in \operatorname{Ass}(M)$. □

Theorem 3.46. *Let A be a Noetherian ring and M be a finitely generated A-module. Then*

1. $\operatorname{Ass}(M)$ *is finite*
2. *the minimal elements of* $\operatorname{Supp}(M)$ *belong to* $\operatorname{Ass}(M)$.

Proof. The first statement follows from Proposition 3.44 which says that every module has composition series and from Lemma 3.43 that states that Ass works well with module extensions so the prime ideals corresponding to the composition series fully describes $\operatorname{Ass}(M)$.

For the second statement let $P \in \operatorname{Supp}(M)$ be a minimal prime ideal. Then

$$\emptyset \overset{3.41}{\neq} \operatorname{Ass}(M_P) \overset{3.45}{=} \operatorname{Ass}(M) \cap \operatorname{Spec}(A_P) \overset{\text{triv.}}{\subseteq} \{P\}$$

so $P \in \operatorname{Ass}(M)$. □

3.7 Primary ideals

Definition 3.47. Let A be a commutative ring. The ideal $J \lhd A$ is a *primary ideal* if all zero-divisors in A/J are nilpotent. Equivalently, if $ab \in J$ and $a \notin J$ then there exists an $n \in \mathbb{N}$ such that $b^n \in J$.

Lemma 3.48. *If $J \lhd A$ is primary then $\sqrt{J}$ is a prime ideal.*

Proof. If $ab \in \sqrt{J}$ then $(ab)^n = a^n b^n \in J$ so if $a^n \in J$ then we are done, else $(b^n)^k \in J$ by J being primary so $b \in \sqrt{J}$. □

Definition 3.49. Let M be an A-module and $N \leq M$ is *primary* if the set of zero-divisors on M/N is $\sqrt{\operatorname{ann}(M/N)}$.

Remark 3.50. If $N \leq M$ is a submodule then $\operatorname{ann}(M/N)$ (so its radical as well) is always contained in the zero-divisors of M/N. So it is a primary ideal if and only if this containment is an equality.

Remark 3.51. The above definition is a generalization of primary ideals, i.e. an ideal $I \lhd A$ is primary if and only I is a primary submodule in the regular A-module A.

Lemma 3.52. *If A is a Noetherian ring and M is a finitely generated A-module then $N \leq M$ is primary if and only is $\operatorname{Ass}(M/N) = \{P\}$ for some $P \in \operatorname{Spec}(A)$.*

Definition 3.53. In the mentioned case N is called $\underline{P}$*-primary*, if we want to emphasize that the prime ideal is P.

Proof. For any $N \leq M$ submodule we have

$$\bigcup_{P \in \operatorname{Ass}(M/N)} P \overset{3.41}{=} \{\text{zero-divisors on } M/N\} \overset{3.50}{\supseteq} \sqrt{\operatorname{ann}(M/N)} \overset{3.27}{=} \bigcap_{P \in \operatorname{Supp}(M/N)} P \overset{3.46}{=} \bigcap_{P \in \operatorname{Ass}(M/N)} P$$

With equality if and only if N is a primary. However equality can happen if and only if $|\operatorname{Ass}(M/N)| = 1$. □

Remark 3.54. Necessarily, this P is nothing else than $\sqrt{\operatorname{ann}(M/N)}$.

NINTH LECTURE, 25TH OF NOVEMBER

Lemma 3.55. *Let N_1 and N_2 be P-primary submodules in a finite A-module M, where A is Noetherian. Then $N_1 \cap N_2$ is P-primary too.*

Proof. By the natural isomorphism $M/(N_1 \cap N_2) \cong M/N_1 \oplus M/N_2$ one gets

$$\operatorname{Ass}(M/(N_1 \cap N_2)) = \operatorname{Ass}(M/N_1 \oplus M/N_2) = \{\operatorname{ann}((x,y)) \in \operatorname{Spec}(A) \mid (x,y) \in M/N_1 \oplus M/N_2\} =$$

$$= \{\operatorname{ann}(x) \cap \operatorname{ann}(y) \in \operatorname{Spec}(A) \mid x \in M/N_1,\ y \in M/N_2\} = \{P\}$$

using the Lemma above, which means exactly that $M/(N_1 \cap N_2)$ is P-primary again. □

Theorem 3.56. (Noether-Lasker Theorem) *Let A be a Noetherian commutative ring and M a nonzero finite A-module. Then*

1. (Existence) *Any proper submodule N of M can be written as*

$$N = N_1 \cap \cdots \cap N_r$$

where the module N_i is primary for all $i = 1, \ldots, r$ such that the decomposition is irredundant (i.e. no N_i can be omitted) and the prime ideals $P_i := \sqrt{\operatorname{ann}(M/N_i)}$ are distinct. This is called the primary decomposition of N.

2. (Uniqueness) *If $N = N_1 \cap \cdots \cap N_r$ is a primary decomposition as in the first point then $\{P_1, \ldots, P_r\} = \operatorname{Ass}(M/N)$ in particular they are independent of the actual decomposition. Moreover, if P_i is a minimal element of $\operatorname{Ass}(M/N)$ then $N_i = M \cap N_{P_i} := \kappa^{-1}(N_{P_i})$ so these parts of the decomposition are unique as well.*

Proof. The first step of the proof is to write a module as an intersection of finitely many "intersection-irreducible" modules.

Definition 3.57. A submodule N of M is intersection-irreducible if it is not the intersection of finitely many submodules.

Let $\mathcal{F} := \{$submodules in M which can not be written as the intersection of finitely many intersection-irreducible submodules$\}$. If this family of submodules is nonempty then – by Noetherianity of M – $\mathcal{F}$ has a maximal element. Then N is not intersection-irreducible so $N = N' \cap N''$ for some submodules N' and N'' of M. Then, by the definition of N the two new modules are already not in $\mathcal{F}$ so they have a decomposition into finitely many intersection-irreducible submodules of M. So we got a decomposition for N as well what contradicts the existence of N.

The second step of the proof is that an intersection-irreducible submodule is primary. Suppose $N \leq M$ is intersection-irreducible. We can pass to the factor module M/N or in other words we can assume that $N = \{0\}$. Suppose $\{0\}$ is not primary on M so by Lemma 3.52 there exists $P_1 \neq P_2$ that are associated primes of M. Then these are annihilators, so $P_i = \operatorname{ann}(m_i)$ for some $m_i \in M$ $(i = 1, 2)$. Therefore there exists $K_i \leq M$ such that $K_i \cong A/P_i$. In particular, every $k_i \in K_i$ we have $\operatorname{ann}_A(k_i) = P_i$ by Remark 3.42. This means that $K_1 \cap K_2 = \{0\}$ since $P_1 \neq P_2$.

These two steps imply that every submodule of M is an intersection of finitely many primary submodules. Omitting superfluous terms, one can easily reach irredundancy. Besides, if there are two terms that are P-primary with the same prime ideal then we can replace them with their intersection which is again a P-primary submodule by Lemma 3.55. This proves the existence.

To prove uniqueness, assume that $N = N_1 \cap \cdots \cap N_r$ with prime ideals $P_1, \ldots, P_r$ as in the statement. Again, passing to M/N we can assume that $N = \{0\}$. Then we can consider the map:

$$M \hookrightarrow \oplus_{i=1}^{r} M/N_i$$

which is injective because $N = \{0\}$. By this, we get

$$\mathrm{Ass}(M) \overset{3.43}{\subseteq} \cup_{i=1}^{r} \mathrm{Ass}(M/N_i) = \cup_{i=1}^{r} \{P_i\} = \{P_i \mid i \leq r\}$$

so $\mathrm{Ass}(M)$ is a subset of P_i's. It is enough to show that $P_1 \in \mathrm{Ass}(M)$. So take a nonzero $x \in N_2 \cap \cdots \cap N_r$ (which is possible because the decomposition is irredundant). Then $\mathrm{ann}(x) \subseteq \{\text{zero-divisors for } M/N_1\}$ because $x \notin N_1$ so for an $a \in \mathrm{ann}(x)$ we have $a\overline{x} = 0 \in M/N_1$. However,

$$\{\text{zero-divisors on } M/N_1\} \overset{P_1-\text{primarity}}{=} P_1 \overset{def}{=} \sqrt{\mathrm{ann}(M/N_1)}$$

On the other hand, $\mathrm{ann}(M/N_1) \subseteq \mathrm{ann}(x)$ by the definitions. We would like to state $\mathrm{ann}(x) = \sqrt{\mathrm{ann}(M/N_1)}$ here to verify the statement but that is not necessarily the case. So we "repair" that x a bit:

By Noetherianity, we know that some power of P_1 is contained in $\mathrm{ann}(M/N_1)$, so we can take the $k \in \mathbb{N}$ such that $P_1^k x \not\subseteq N_1$ but $P_1^{k+1} x \subseteq N_1$. For an arbitrary $y \in P_1^k x \backslash N_1$ we have

$$y \in (N_2 \cap \cdots \cap N_r) \backslash N_1$$

in particular $y \neq 0$. So – by the same argument as for x – we get that $\mathrm{ann}(y) \subseteq P_1$, but in this case $P_1 \subseteq \mathrm{ann}(y)$ also holds because $P_1 y = P_1^{k+1} x \subseteq N_1$. Therefore, $\mathrm{ann}(y) = P_1$ so $P_1 \in \mathrm{Ass}(M)$ as we stated.

For the last part of the uniqueness, assume that $P := P_1$ is minimal among $\{P_1, \ldots, P_r\} = \mathrm{Ass}(M/N)$. For $i > 1$ we have

$$\mathrm{Ass}\big((M/N_i)_P\big) \overset{3.45}{=} \mathrm{Ass}(M/N_i) \cap \mathrm{Spec}(A_P) = \{P_1, \ldots, P_r\} \cap \{\text{prime ideals contained in } P\} = \emptyset$$

because P was minimal in $\mathrm{Ass}(M/N)$ so P_i cannot be inside P. This also means that $(M/N_i)_P = \{0\}$ because by Proposition 3.44 a nonzero module always has associated primes. Therefore, $(N_i)_P = M_P$ by the exactness of localization so we got that

$$N_P = \Big(\bigcap_{i=1}^{r} N_i\Big)_P = \Big(\bigcap_{i=1}^{r} (N_i)_P\Big) = (N_1)_P \cap \bigcap_{i=1}^{r} M_p = (N_1)_P$$

So the only thing what is left is to show that $N_1 = M \cap (N_1)_P \overset{def}{=} \kappa^{-1}((N_1)_{P_i})$. But this is true by the definition of localization: if $\frac{n}{s} = \frac{x}{1} \in (N_1)_P \cap M$ where $n \in N_1$, $x \in M$ and $s \in A\backslash P$ then by definition it means that there exists a $u \in S$ such that $u(sx - n) = 0 \in M$. Fortunately, $S = A\backslash P = A\backslash\{\text{zero-divisors on } M/N_1\}$ so if the element $usx = un$ is in N_1 then x is in N_1 as well. The statement follows. □

Corollary 3.58. *Let A be a Noetherian ring and $I \lhd A$. Then there exist primary ideals $Q_1, \ldots, Q_r$ in A such that*

$$I = Q_1 \cap \cdots \cap Q_r$$

where we can assume that the prime ideals $P_i := \sqrt{Q_i}$ are distinct and no Q_i can be omitted. Besides, P_i's are uniquely determined by I. Moreover, the those Q_j's for which the corresponding P_i's is minimal in $\mathrm{Ass}(A/I)$ are also unique.

Corollary 3.59. *Any radical ideal $\sqrt{I}$ can be written in the form $\sqrt{I} = P_1 \cap \cdots \cap P_r$ with finitely many prime ideals. (Here the new information is finitely many, see Proposition 3.27)*

Example 3.60. The decomposition itself is not necessarily unique: let $A = \mathbf{k}[x, y]$ where $\mathbf{k}$ is a field and let $I = (x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x^2, xy, y^2)$. Here, the associated prime ideals are (x) and (x, y) so we can see that (x) – as a minimal associated ideal – is always there.

3.8 Krull dimension

Definition 3.61. Let A be a commutative ring. The *Krull dimension* of A is

$$\dim(A) := \sup\{r \in \mathbb{N} \mid \exists P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_r \text{ prime ideals}\}$$

Theorem 3.62. (Krull) *Let A be a domain which is a finitely generated $\mathbf{k}$-algebra. Then*

$$\dim(A) = \mathrm{tr.deg}_{\mathbf{k}}(A)$$

Proof. First let us prove the inequality $\dim(A) \leq \mathrm{tr.deg}_{\mathbf{k}}(A)$. It is sufficient to show that for a nonzero prime ideal $P \lhd A$ we have

$$\mathrm{tr.deg}_{\mathbf{k}}(A/P) < \mathrm{tr.deg}_{\mathbf{k}}(A)$$

Let $y_1, \ldots, y_r$ be a transcendence basis for A/P and pull them back to A as $z_1, \ldots, z_r$. Now, take a nonzero $u \in P$. Assume that for a nonzero polynomial $0 \neq F \in \mathbf{k}[x_0, \ldots, x_r]$ we have

$$F(u, z_1, \ldots, z_r) = 0$$

Then $F = x_0 F_1(x_0, \ldots, x_r) + F_2(x_1, \ldots, x_r)$ where we may assume that $0 \neq F_2 \in \mathbf{k}[x_1, \ldots, x_n]$ or otherwise

$$F(u, z_1, \ldots, z_r) = uF_1(u, z_1, \ldots, z_r) = 0$$

so we can replace F with F_1 until we reach the stated situation. However, this F_2 gives a nontrivial relation in A/P among $y_1, \ldots, y_r$ which contradicts their algebraic independence. So there is no such F and $u, z_1, \ldots, z_r$ is an algebraically independent system.

The other inequality can be proved by induction on $\mathrm{tr.deg}_{\mathbf{k}}(A)$: If it is zero then there is nothing to do since the Krull dimension is non-negative by definition. Now, suppose that $r := \mathrm{tr.deg}_{\mathbf{k}}(A) > 0$. Then $A = \mathbf{k}[\alpha_1, \ldots, \alpha_n]$ where α_1 is transcendental over $\mathbf{k}$. Let $S := \mathbf{k}[\alpha_1] \backslash \{0\} \subseteq A$ and define $B := A[S^{-1}]$. Then $\mathbf{k}(\alpha_1) \subseteq B$ because $\mathbf{k}[\alpha_1] \cong \mathbf{k}[x_1]$. So one can view B as an algebra over $\mathbf{k}(\alpha_1)$. Then

$$\mathrm{tr.deg}_{\mathbf{k}(\alpha_1)}(B) = \mathrm{tr.deg}_{\mathbf{k}}(A) - 1$$

By the induction hypothesis, there exists a chain of prime ideals $Q_{r-1} \supsetneq Q_{r-2} \supsetneq \cdots \supsetneq Q_0$ in B. So one can define $P_i = Q_i \cap A$ as the pullback of Q_i's along κ. These form a strictly decreasing chain of prime ideals (disjoint from S) in A by Proposition 3.33. So $P_{r-1} \cap S = \emptyset$ means that $\overline{\alpha_1}$ is transcendental over A/P_{r-1} since if it would be algebraic then $p(\alpha_1) \in P_{r-1}$ could be satisfies with some polynomial p which contradicts $P_{r-1} \cap S = \emptyset$.

Consequently P_{r-1} is not a maximal ideal in A because in that case A/P_{r-1} would be a field which is finitely generated as a $\mathbf{k}$-algebra but not $\dim_{\mathbf{k}}(A/P_{r-1}) \not< \infty$ since $\overline{\alpha_1}$ is not algebraic. This is impossible because of Zariski's lemma 3.15. So we can take a maximal ideal which is necessarily prime and extend the chain of P_i's into a chain of length r. □

Example 3.63. $\dim \mathbf{k}[x_1, \ldots, x_n] = n$ since we know that $\mathrm{tr.deg}_{\mathbf{k}}\mathbf{k}[x_1, \ldots, x_n] = n$. A chain of prime ideals can be explicitly constructed by taking $P_i = (x_1, \ldots, x_i)$ but without the theorem it is not clear why there cannot be a longer chain.

3.9 Basic Notions of Algebraic Geometry

Convention: In the following, $\mathbf{k}$ is an algebraically closed field.

Definition 3.64. On $\mathbb{A}^n(\mathbf{k}) := \mathbf{k}^n$ we can introduce a topology called the *Zariski-topology*. Here, a subset $X \subseteq \mathbf{k}^n$ is closed (or *Zariski-closed*) if there exists an $S \subseteq \mathbf{k}[x_1, \ldots, x_n]$ such that $X = \mathcal{V}(S)$. These subsets $\mathcal{V}(S)$ are also called *(affine) algebraic sets* or *(affine) algebraic varieties*.

Remark 3.65. In the use of the word "variety" there is some confusion: in some books, it stands for any algebraic set and in some other books, it means irreducible algebraic set.

Proposition 3.66. *Basic properties of Zariski-closed sets:*

1. $\mathcal{V}(S) = \mathcal{V}((S))$ *by definition*
2. $\mathcal{V}(S) = \mathcal{V}(f_1, \ldots, f_n)$ *where* $f_1, \ldots, f_n$ *is a generating set of* S *which always exists by Hilbert's Basissatz*
3. $\mathcal{V}(1) = \emptyset$, $\mathcal{V}(0) = \mathbf{k}^n$
4. $\cap_{\alpha \in A} \mathcal{V}(S_\alpha) = \mathcal{V}(\cup_{\alpha \in A} S_\alpha)$
5. $\mathcal{V}(f_1, \ldots, f_s) \cup \mathcal{V}(h_1, \ldots, h_t) = \mathcal{V}(\{f_i h_j \mid i \leq s,\ j \leq t\})$

Remark 3.67. In the above proposition, 3., 4. and 5. means that it is indeed a topology. However, it is usually a really weird topology compared to the usual Euclidean topology. For example, these spaces are never Hausdorff.

Example 3.68. For $n = 1$ it gives the co-finite topology.

Remark 3.69. The closure of $X \subseteq \mathbf{k}^n$ in the Zariski-topology is $\overline{X} = \mathcal{V}(I(X))$ by the definitions.

Definition 3.70. A closed subset $X \subseteq \mathbf{k}^n$ is *irreducible* if it is not the union of two proper closed subsets.

By this definition, we get a correspondence between the Zariski-closed subsets of $\mathbf{k}^n$ and some ideals in $\mathbf{k}[x_1, \ldots, x_n]$. In fact, Hilbert's Nullstellensatz means that

$$\{\text{Zariski-closed subsets of } \mathbf{k}^n\} \longleftrightarrow \{\text{radical ideals of } \mathbf{k}[x_1, \ldots, x_n]\}$$

where the bijection is realized by $\mathcal{V}$ and $\mathcal{I}$ (for definitions see 3.11 and 3.24). We have just seen that $\mathcal{V}(\mathcal{I}(X)) = X$ by definitions and the Nullstellensatz proves that $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I} = I$ for a radical ideal I.

Moreover, the irreducible Zariski-closed sets correspond to the prime ideals since every ideal have a primary decomposition and radical ideals even have a prime decomposition so

$$X = \mathcal{V}(\mathcal{I}(X)) = \mathcal{V}(P_1 \cap \cdots \cap P_r) = \mathcal{V}(P_1) \cup \cdots \cup \mathcal{V}(P_r)$$

Definition 3.71. A map $\mathbf{k}^n \supseteq X \xrightarrow{f} Y \in \mathbf{k}^m$ is a *morphism* of affine algebraic varieties if f is the restriction to X of a polynomial mapping $\mathbf{k}^n \to \mathbf{k}^n$. The coordinate ring $\mathcal{O}(X)$ of X is the ring of morphisms $X \to \mathbf{k}$.

Goal: (for next lecture) $\mathcal{O}$ is a contravariant functor. In fact the category of affine varieties is equivalent (by $\mathcal{O}$) to the category of reduced $\mathbf{k}$-algebras. (Where reduced means that it contains no nilpotent elements.)

Tenth Lecture, 2nd of December

Example 3.72. For (commutative) Noetherian rings:

1. Every finitely generated $\mathbf{k}$-algebra is Noetherian (where $\mathbf{k}$ is a field) since the definition means that the algebra is a factor of the polynomial ring $\mathbf{k}[x_1, \ldots, x_n]$ for some n which is Noetherian by Hilbert's Basissatz.
2. The localization of a Noetherian ring is Noetherian too because a strictly ascending chain of ideals in the localization could be pulled back to the ring. However, "typically" a localization of a finitely generated $\mathbf{k}$-algebra is no longer finitely generated but still Noetherian.
3. For a commutative Noetherian ring, the formal power series ring $A[[x]]$ is also Noetherian. However, say $\mathbf{k}[[x]]$ is not a finitely generated $\mathbf{k}$-algebra.

3.10 Hilbert's Syzygy Theorem

Historically, this is the origin of homological algebra.

Definition 3.73. Let R be a ring and take a sequence of R-module homomorphisms:

$$\ldots \longleftarrow M_{i-1} \xleftarrow{\varphi_i} M_i \xleftarrow{\varphi_{i+1}} M_{i+1} \longleftarrow \ldots$$

We say that this sequence is *exact* at M_i if $\operatorname{Ker}\varphi_i = \operatorname{Im}\varphi_{i+1}$. Similarly, the sequence is exact, if it is exact at all M_i.

Definition 3.74. Suppose that M is a finitely generated R-module where R is Noetherian. The *free R-module of rank d* is $R^d = R \oplus \cdots \oplus R$ the d-fold direct sum of the base ring.

Suppose that M is generated by $w_1, \ldots, w_d \in M$. Then we can define a surjective homomorphism $\varphi_0 : R^d = F_0 \twoheadrightarrow M$ by

$$(r_1, \ldots, r_d) \to \sum_{i=1}^{n} r_i w_i$$

Let us denote the kernel of φ_0 by S_0, i.e. $S_0 := \operatorname{Ker}\varphi_0 < F_0$. R is Noetherian so F_0 is Noetherian as well hence S_0 is a finitely generated R-module. Say it is generated by d_1 elements. So we can apply the previous procedure using S_0 and d_1 getting $F_1 = R^{d_1}$ and a homomorphism $\varphi_1 : F_1 \twoheadrightarrow S_0$ with a kernel S_1.

Now, we can iterate this process for every resulting (finitely generated) module S_i hence we get an infinite sequence of R-modules and homomorphisms

$$\begin{array}{ccccccccccc} 0 & \longleftarrow & M & \xleftarrow{\varphi_0} & F_0 & \xleftarrow{\varphi_1} & F_1 & \xleftarrow{\varphi_2} & F_2 & \longleftarrow & \ldots \\ & & & & \uparrow & \swarrow & \uparrow & \swarrow & & & \\ & & & & S_0 & & S_1 & & & & \end{array}$$

This is called the *free resolution* of M.

Remark 3.75. Since every free module is projective, it is also a projective resolution. However, under some conditions, finitely generated projective modules are all free so the two notions then coincide.

Now, let's turn to the context we will use:

Definition 3.76. A ring R is *graded* if it decomposes

$$R \cong \bigoplus_{i=0}^{\infty} R_i$$

as an abelian group and $R_i \cdot R_j \subseteq R_{i+j}$ for all $i, j \in \mathbb{N}$. Here, R_i is called the *degree i homogeneous component* of R.

Remark 3.77. Instead of $\mathbb{N}$ one can generally use $\mathbb{Z}$ or other abelian groups.

Example 3.78. $R = \mathbf{k}[x_1, \ldots, x_n]$ with the usual grading is a graded ring.

Remark 3.79. When we deal with $\mathbf{k}$-algebras then the R_i are assumed to be $\mathbf{k}$-subspaces as well (not only abelian subgroups). Besides, frequently $R_0 = \mathbf{k} = \mathbf{k}1_{\mathbf{k}}$ is the case.

Definition 3.80. Let $R = \oplus_{i=0}^{\infty} R_i$be a graded ring. Then a *graded R-module M* is an R-module that has a decomposition as an abelian group:

$$M = \bigoplus_{j=0}^{\infty} M_j \qquad \text{such that} \qquad R_i M_j \subseteq M_{i+j} \quad (\forall i, j)$$

The summand M_i is called a *homogeneous submodule* or the submodule generated by degree i elements.

Example 3.81. Let $R = \mathbf{k}[x_1, \ldots, x_n]$ with the standard grading. Then a homogeneous submodule I of R is called a homogeneous ideal. Equivalently, I is homogeneous if it is generated be homogeneous elements.

In this case R/I is a graded R-module.

Remark 3.82. The motivation of these definitions is projective algebraic geometry where in the projective n-space $\mathbb{P}^n(\mathbf{k}) := (\mathbf{k}^{n+1}\backslash\{0\})/\mathbf{k}^\times$ we consider projective algebraic varieties that are defined as the common zero locus X of a set of homogeneous polynomial from $\mathbf{k}[x_1, \ldots, x_n]$. (Without the homogeneity assumption we could not decide whether a point is a zero of a polynomial.)

For this projective algebraic variety X we can analogously define the so called homogeneous coordinate ring of $X \subseteq \mathbb{P}^n(\mathbf{k})$ as

$$\mathbf{k}[x_1, \ldots, x_n]/\mathcal{I}(X)$$

which is again a graded ring where the grading is inherited from $\mathbf{k}[x_1, \ldots, x_n]$.

Definition 3.83. Suppose M and N are grade R-module. A homomorphism between these is an R-module homomorphism $f : M \to N$ which is graded in a sense that $f(M_\bullet) \subseteq N_\bullet$ for all i.

A graded R-module M has a *free resolution*

$$0 \longleftarrow M \xleftarrow{\varphi_0} F_0 \xleftarrow{\varphi_1} F_1 \longleftarrow \ldots$$

where the φ_i are homomorphisms of graded modules where the grading on F_i's is defined as follows:

By the assumptions M is generated by finitely many homogeneous elements $w_1, \ldots, w_d$. The map φ_0 was defined so that $R^d \ni e_i \mapsto w_i$. Therefore, we can set $\deg(e_i) := \deg(w_i)$ to make φ_0 a graded morphism. Then, by the free property of F_0, this uniquely determines a grading of F_0, namely: an element

$$\sum_{i=1}^{d} r_i e_i \in F_0$$

is homogeneous of degree t if and only if all r_i are homogeneous and $\deg r_i + \deg e_i = t$ for all i. With this grading φ_0 is indeed a graded homomorphism.

Theorem 3.84. (Hilbert Syzygy Theorem) *Take $R = \mathbf{k}[x_1, \ldots, x_n]$ with the standard grading. Then any finitely generated graded R-module M has a free resolution*

$$0 \longleftarrow M \xleftarrow{\varphi_0} F_0 \xleftarrow{\varphi_1} F_1 \longleftarrow \ldots \longleftarrow F_n \longleftarrow 0$$

More precisely, for any exact sequence of

$$0 \longleftarrow M \xleftarrow{\varphi_0} F_0 \xleftarrow{\varphi_1} F_1 \longleftarrow \ldots \xleftarrow{\varphi_{n-1}} F_{n-1}$$

of graded R-modules where the F_i's are finitely generated free modules, we have that kernel of φ_{n-1} is free. (Here, the zero module is considered as a free module of rank zero.)

Remark 3.85. The module $S_i := \operatorname{Ker}\varphi_i = \operatorname{Im}\varphi_{i+1}$ in the theorem is called the i-th syzygy module of the resolution.

Proof. Let us introduce the notation $\mathfrak{m}_j := (x_1, x_2, \ldots, x_j) \lhd \mathbf{k}[x_1, \ldots, x_n] = R$.

Claim 3.86. For $i \geq j$ we have $\mathfrak{m}_j F_i \cap S_i = \mathfrak{m}_j S_i$

Proof. Apply induction on j: In the case of $j = 1$, take an element $x_1 a_i \in \mathfrak{m}_1 F_i \cap S_i$ where $a_i \in F_i$ and

$$0 = \varphi_i(x_1 a_i) = x_1 \varphi_i(a_i)$$

but since a free module is torsion-free we get $\varphi_i(a_i) = 0$ implying that $x_1 a_i \in \mathfrak{m}_1 S_i$. The reverse inclusion is trivial.

Assume that $j > 1$ and the claim holds for all k smaller than j. Now, take

$$\sum_{k=1}^{j} x_k a_k \in \mathfrak{m}_j F_i \cap S_i \qquad \text{so} \qquad \varphi_i\Big(\sum_{k=1}^{j} x_k a_k\Big) = 0$$

where $a_1, \dots, a_j \in F_i$. Then we get

$$0 = \varphi_i\Big(\sum_{k=1}^{j} x_k a_k\Big) = \sum_{k=1}^{j} x_k \varphi_i(a_k)$$

where the terms are in $\mathfrak{m}_k F_{i-1}$ so $x_j \varphi_i(a_j) \in \mathfrak{m}_{j-1} F_{i-1}$ since

$$x_j \varphi_i(a_j) = -\sum_{k=1}^{j-1} x_k \varphi_i(a_k)$$

but this means that $\varphi_i(a_j) \in \mathfrak{m}_{j-1} F_{i-1}$ because multiplying by x_j cannot help us to get into $\mathfrak{m}_{j-1} F_{i-1}$. Besides, $\varphi_i(a_j)$ is obviously in $\operatorname{Im}(\varphi_i) = S_{i-1}$ too so we can apply the induction hypothesis. Therefore $\varphi_i(a_j) \in \mathfrak{m}_{j-1} S_{i-1}$ so there exist $b_1, \dots, b_{j-1} \in F_i$ such that

$$\varphi_i(a_j) = \sum_{k=1}^{j-1} x_k \varphi_i(b_k) \qquad \Rightarrow \qquad a_j - \sum_{k=1}^{j-1} x_k b_k \in \operatorname{Ker} \varphi_i = S_i$$

Hence, we can observe that in the following (arithmetically trivial) identity which terms belong to which submodule:

$$S_i \ni \sum_{k=1}^{j} x_k a_k = x_j(a_j - \sum_{k=1}^{j-1} x_k b_k) + \sum_{k=1}^{j-1} x_k (x_j b_k + a_k) \in \mathfrak{m}_j S_i + \big(S_i \cap \mathfrak{m}_{j-1} F_i\big)$$

where we used that $a_j - \sum_{k=1}^{j-1} x_k b_k$ and $\sum_{k=1}^{j} x_k a_k$ are in S_i therefore $\sum_{k=1}^{j-1} x_k (x_j b_k + a_k)$ is also in S_i. However, the latter is in $\mathfrak{m}_{j-1} F_i$ as well by definition, so – by the induction hypothesis –

$$\sum_{k=1}^{j-1} x_k (x_j b_k + a_k) \in \mathfrak{m}_{j-1} S_i \subseteq \mathfrak{m}_j S_i$$

as we claimed. □

In particular, the claim says that $\mathfrak{m}_n F_n \cap S_n = \mathfrak{m}_n S_n$ no matter how we choose F_n. Now, we want to modify F_n to make $S_{n-1} = \operatorname{Ker} \varphi_i$ free. So take a minimal generating system of homogeneous generators of S_{n-1}. These generator elements will be the images of the generator elements of our "new" F_n by the obviously defined φ_n.

Claim 3.87. $S_n \subseteq \mathfrak{m}_n F_n$

Proof. Indeed, otherwise there exists an $r_1, \dots, r_d \in S_n$ such that all r_i are homogeneous but not all of them is contained in $\mathfrak{m}_n$. Say, $r_1 \notin \mathfrak{m}_n$ then it means that $r_1 \in \mathbf{k}^\times$. Denoting $w_1, \dots, w_d$ the chosen generators of S_N we have a relation

$$r_1 w_1 + \dots + r_d w_d = 0$$

so by $r_1 \in \mathbf{k}^\times$we get

$$w_1 = -\sum_{k=1}^{d} \frac{r_k}{r_1} w_k$$

so w_1 is a superfluous generator which is a contradiction. □

Therefore,

$$\mathfrak{m}_n S_n \overset{3.86}{=} \mathfrak{m}_n F_n \cap S_n \overset{3.87}{=} S_n$$

but it would contradict $S_n \neq 0$: take a nonzero homogeneous element s of S_n of minimal degree. Then $s \in S_n = \mathfrak{m}_n S_n$ so

$$s = x_1 t_1 + \cdots + x_n t_n$$

for some $t_i \in S_n$ but then $\sum t_i$ has lower degree than s which is possible only if $S_n = 0$. (This is, in fact, the graded Nakayama lemma.) □

Remark 3.88. The bound is strict since the module $M := \mathbf{k}[x_1, \ldots, x_n]/(x_1, \ldots, x_n) \cong \mathbf{k}$ has exactly n-long free resolution: (with no shorter resolution)

Indeed, we recursively define the so called Koszul resolution (or Koszul complex?) of M: the first step is to take the natural surjection $\varphi_0 : R \to \mathbf{k}$:

$$0 \longleftarrow \mathbf{k} \xleftarrow{\varphi_0} R \xleftarrow{\varphi_1} R^n$$

where φ_1 is defined as $e_i \mapsto x_i$. The higher terms in the resolution are $F_i \cong R^{\binom{n}{i}}$. It is left for the reader to find to corresponding maps.

Definition 3.89. Let $R = \mathbf{k}[x_1, \ldots, x_n]$ with the natural grading and $M = \bigoplus_{i=0}^{\infty} M_i$ a finitely generated graded R-module. Then $\dim_{\mathbf{k}}(M_i) < \infty$ for all i. So we can define the generating function of these dimensions, usually called the *Hilbert-* or *Poincaré-series*:

$$H(M; t) := \sum_{i=0}^{\infty} \dim_{\mathbf{k}}(M_i) t^i$$

Now, to compute this function, take a free resolution of M:

$$0 \longleftarrow M \xleftarrow{\varphi_0} F_0 \xleftarrow{\varphi_1} F_1 \longleftarrow \ldots \longleftarrow F_n \longleftarrow 0$$

The alternating sums of the dimensions is zero by exactness so

$$H(M; t) = \sum_{j=0}^{n} (-1)^j H(F_j; t)$$

so it is enough to compute the Hilbert-series of free modules. Let us denote the degree of $e_i \in F_i \cong R^d$ by $q_j = \deg(e_j) \in \mathbb{N}$. Therefore

Proposition 3.90. *the Hilbert-series of such a free module is*

$$H(F_i; t) = \frac{\sum_{j=1}^{d} t^{q_j}}{(1-t)^d}$$

Proof. If we put the standard grading on a free module then we get

$$H(\mathbf{k}[x_1, \ldots, x_d], t) = \Big(\sum_{j=0}^{\infty} t^j \Big)^d =: \frac{1}{(1-t)^d}$$

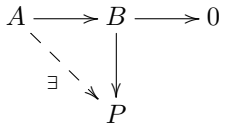
because we can easily count the dimension of the homogeneous polynomials in a fixed degree. However, if the grading is modified, i.e. $q_j = \deg(e_j)$ then the power-series are shifted and that proves the formula for $H(F_i; t)$. □

Corollary 3.91. *$H(M; t) = \frac{P(t)}{(1-t)^n}$ for some polynomial $P \in \mathbb{Z}[t]$ and some positive integer n.*

Remark 3.92. When M is the homogeneous coordinate ring of a projective algebraic variety $X \subseteq \mathbb{P}^n(\mathbf{k})$. Then one can read off from the Hilbert series of the coordinate ring the dimension of X or the degree of X.

Usually, in homological algebra projective resolutions are used instead of free resolutions:

Definition 3.93. An R-module P is *projective* if O is a direct summand of a free module. Equivalently, for any diagram (with exact first row)



can be completed in a commutative way.

Proposition 3.94. *If R is a local commutative ring then any finitely generated projective R-module is free.*

Eleventh Lecture, 9th of December

4 Lie algebras

Definition 4.1. Let $\mathbb{F}$ be a field. A Lie algebra L is a vector space over $\mathbb{F}$ with a bilinear map $[.,.] : L \times L \to L$ usually called *Lie multiplication* or *Lie bracket* such that

1. for all $x \in L$: $[x, x] = 0$
2. for all $x, y, z \in L$: $\big[[x, y], z\big] + \big[[y, z], x\big] + \big[[z, x], y\big] = 0$ (called *Jacobi-identity*)

Remark 4.2. The first axiom implies that the bracket antisymmetric, i.e. $[y, x] = -[x, y]$

Example 4.3.

1. If A is an associative $\mathbb{F}$-algebra then define $[a, b] := ab - ba$. With this definition $(A, [.,.])$ becomes a Lie algebra. In particular, if one considers $\mathrm{End}_{\mathbb{F}}(V)$ for an $\mathbb{F}$-vector space with the Lie bracket as above one gets $\mathfrak{gl}(V)$.

2. Let A be an associative $\mathbb{F}$-algebra. The derivations

$$\mathrm{Der}_{\mathbb{F}}(A) := \big\{D : A \to A \mid D \text{ is } \mathbb{F}\text{-linear}, D(ab) = D(a)b + aD(b)\big\} \subseteq \mathrm{End}_{\mathbb{F}}(A)$$

   is a Lie algebra with the restriction of $\mathrm{End}_{\mathbb{F}}(A)$'s Lie bracket.

   Remark 4.4. The rule $D(ab) = D(a)b + aD(b)$ is called the *Leibniz-rule*.

   Remark 4.5. The composition of two derivations is typically not a derivation but their commutator is.

   In particular, if M is a $\mathcal{C}^\infty$-manifold then $\mathcal{C}^\infty(M)$ is an associative (also commutative) algebra. Then

$$\mathrm{Der}_{\mathbb{R}}\big(\mathcal{C}^\infty(M)\big) \longleftrightarrow \{\text{smooth vector fields on } M\}$$

   is a Lie algebra. By this identification we can speak about X_p for a derivation $X \in \mathrm{Der}\big(\mathcal{C}^\infty(M)\big)$.

3. Historically, one of the main motivations of the study of Lie algebras was the notion of Lie algebra of a Lie group.

   Definition 4.6. A *Lie group* is a group G which is also a $\mathcal{C}^\infty$-manifold (on $\mathbb{R}$) such that the group operations are smooth, i.e. $\cdot : G \times G \to G$ is a $\mathcal{C}^\infty$-map where we consider the product manifold-structure and similarly, $^{-1} : G \to G$ is required to be $\mathcal{C}^\infty$.

Definition 4.7. A *left invariant vector field* on a Lie group G is defined as a vector field such that $L_g \circ X = X \circ L_g \in \mathrm{End}_{\mathbb{F}}\big(\mathcal{C}^\infty(M)\big)$ where $L_g : \mathcal{C}^\infty(G) \to \mathcal{C}^\infty(G)$, $f \mapsto \big(x \mapsto f(g^{-1}x\big)$ is the left translation. In this case $X_g = (\mathrm{d}_{1_G}L_g)(X_{1_G})$ where $\mathrm{d}_{1_G}L_g : T_{1_G}G \to T_gG$ is the associated tangent map of the left multiplication $L_g : G \to G$. (We use the same notation for both left multiplications but we doubt that it will confuse any of the readers.) The left-invariant smooth vector fields constitute a Lie subalgebra of the Lie algebra $\mathrm{Der}_{\mathbb{R}}\big(\mathcal{C}^\infty(M)\big)$. This is called the Lie algebra of G as a vector space thus can be identified with $T_{1_G}G$.

Example 4.8.

(a) Take $GL(V)$ for a finite dimensional $\mathbb{R}$-vector space V. Then $Lie(GL(V)) = \mathfrak{gl}(V)$.

(b) The Lie algebra of the Lie group $O(V)$ is the "skew-symmetric matrices" if we identify V by $\mathbb{R}^n$.

Remark 4.9. If $\rho : G \to H$ is a homomorphism of Lie groups then $\mathrm{d}_{1_G}\rho$ is a homomorphism of Lie algebras. In particular, from a finite dimensional representation of a Lie algebra $\rho : G \to GL(V)$ we get a homomorphism $\mathrm{d}_{1_G}\rho : Lie(G) \to Lie(GL(V)) \cong \mathfrak{gl}(V)$. So a general strategy appears: sometimes it is easier to understand a representations of a group by investigating its differential.

Theorem 4.10. (Lie's Third Theorem) *For any finite dimensional real Lie algebra L there exists a unique simply connected Lie group G with $Lie(G) = L$. Moreover, if G is a simply connected Lie group and H is any connected Lie group then for any Lie algebra homomorphism $\overline{\rho} : Lie(G) \to Lie(H)$ there exists a unique homomorphism $\rho : G \to H$ such that $\mathrm{d}_{1_G}\rho = \overline{\rho}$.*

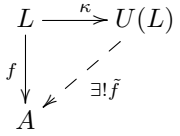
4.1 Universal enveloping algebra of a Lie algebra L

Definition 4.11. (Construction) The *universal enveloping algebra* is defined as $U(L) := T(L)/I_L$ where $T(L)$ is the tensor algebra of L:

$$T(L) = \bigoplus_{d=0}^{\infty} L^{\otimes d}$$

with the associative multiplication the tensor product. Equivalently, it is the free associative algebra on a basis of L. The ideal I_L is generated by the elements $a \otimes b - b \otimes a - [a, b] \in T(L)$ for all $a, b \in L$.

Proposition 4.12. *For any Lie algebra homomorphism $f : L \to A$ into some associative algebra A (viewed as a Lie algebra with the standard bracket) there exists a unique homomorphism of associative algebras $\tilde{f} : U(L) \to A$ such that $f = \tilde{f} \circ \kappa$ where $\kappa : L \to U(L)$ is the canonical Lie homomorphism obtained by restricting to L the natural surjection $T(L) \to U(L)$. In diagram:*



one should not forget that $\tilde{f}$ is a homomorphism of associative algebras while f is a Lie homomorphism.

Corollary 4.13. *There exists a bijection between $U(L)$-modules and representations of the Lie algebra L.*

Fact: κ is injective but it is nontrivial. This follows from the next (much stronger) theorem:

Theorem 4.14. (Poincaré-Birkhoff-Witt theorem) *Denote $y := \kappa(x_i) \in U(L)$ where $x_1, \ldots, x_n$ is an $\mathbb{F}$-vector space basis of L. Then*

$$\{y_1^{\alpha_1} \cdot y_2^{\alpha_2} \cdot \cdots \cdot y_n^{\alpha_n} \mid \alpha_1, \ldots, \alpha_n \in \mathbb{N}\}$$

is an $\mathbb{F}$-vector space basis in $U(L)$.

Corollary 4.15. *κ is injective.*

Definition 4.16. A Lie algebra L is *abelian*, if $[x,y]=0$ for all $x,y\in L$. $\dim_{\mathbb{F}} L = n$. In this case $U(L)=\mathbb{F}[x_1,\dots,x_n]$ by definition.

Proof. (of Theorem 4.14)

Remark 4.17. The universal enveloping algebra is usually not graded since we got it by factoring out by non-homogeneous elements. However, we still have a filtration on $U(L)$:

Definition 4.18. $U(L)_d := \mathrm{Span}_{\mathbb{F}}\{y_{i_1}\cdot\dots\cdot y_{i_k} \mid k\le d,\ i_1,\dots,i_k\in\{1,\dots,n\}\}$

Lemma 4.19. *For all $\pi\in S_d$, $Y_1,\dots,Y_d\in\kappa(L)$ we have $Y_1\cdot\dots\cdot Y_d - Y_{\pi(1)}\cdot\dots\cdot Y_{\pi(d)}\in U(L)_{d-1}$*

Proof. It is enough to show the statement for transposition of neighboring elements since they generate S_n. So let $\pi=(i,i+1)$. Then

$$Y_1,\dots,Y_{i-1}Y_iY_{i+1}Y_{i+2}\dots Y_d - Y_1,\dots,Y_{i-1}Y_{i+1}Y_iY_{i+2}\dots Y_d =$$

$$= Y_1,\dots,Y_{i-1}(Y_iY_{i+1}-Y_{i+1}Y_i)Y_{i+2}\dots Y_d = Y_1,\dots,Y_{i-1}[Y_i,Y_{i+1}]Y_{i+2}\dots Y_d\in U(L)_{d-1}$$

□

Corollary 4.20. *$\{y_1^{\alpha_1}\dots y_n^{\alpha_n} \mid \alpha_i\in\mathbb{N}\}$ span $U(L)$ as an $\mathbb{F}$-vector space.*

Proof. Using the lemma, one shows by induction on d that

$$U(L)_d = \mathrm{Span}_{\mathbb{F}}\{y_1^{\alpha_1}\dots y_n^{\alpha_n} \mid \alpha_1+\dots+\alpha_n\le d\}$$

so the stated system indeed spans $U(L)$. □

The harder part of the proof is the linear independence:

Notation: Let $P=\mathbb{F}[z_1,\dots,z_n]$ be the polynomial algebra. If $(i_1,\dots,i_k)=I$ then we write z_I for $z_{i_1}\cdot\dots\cdot z_{i_k}$.
Let us denote the span of homogeneous components of P of degree at most d by P_d. In other words:

$$P_d = \mathrm{Span}_{\mathbb{F}}\{z_I \mid I=(i_1,\dots,i_k) \text{ increasing sequence}, k\le d\}$$

For $i\in\{1,2,\dots,n\}$ and $I=(i_1,\dots,i_k)$ we write $i\le I$ if $i\le i_j$ for all $j\le k$.

Lemma 4.21. *For $d\in\mathbb{N}$ there exists a unique $\mathbb{F}$-bilinear map $f_d: L\times P_d\to P_{d+1}$, $(x,z)\mapsto xz$ such that*

1. *For $i\le I$ we have $x_iz_I = z_iz_I$*
2. *For all $i\in\{1,2,\dots,n\}$ and $I=(i_1,\dots,i_k)$, $k\le d$ we have $x_iz_I - z_iz_I\in P_d$*
3. *For all i,j and all $z_J\in P_{d-1}$ we have $x_i(x_jz_J) = x_j(x_iz_J)+[x_i,x_j]z_J$ (i.e. it is a Lie-algebra representation)*

Moreover, $f_d|_{L\times P_{d-1}} = f_{d-1}$ (so it is a well defined representation on P)

Corollary 4.22. *The elements $y^{\alpha_1}y^{\alpha_2}\dots y^{\alpha_n}$ for increasing sequences are in fact linearly independent since they act linearly independently on P.*

Proof. (of Lemma 4.21) We prove by induction on d: If $d = 0$ then one can define $x_i 1 = z_1$ by the first property. The other properties trivially hold in this case. Now, suppose that $d > 0$ so we have a map $f_{d-1} : L \times P_{d-1} \to P_d$ with the stated properties. To define f_d we does not have any freedom: the properties determine the definition we just have to check that it is indeed a good definition.

Indeed, we need to define $x_i z_I$ for an increasing sequence I and $i \in \{1, 2, \ldots, n\}$. The first property says that $x_i z_I = z_i z_I$. If we are not in this case but – by the notation $I = (j, J)$ – $i > j$ and $j \leq I$ then if f_d exists, it must satisfy the following

$$x_i z_I = x_i(x_j z_J) = x_j(x_i z_J) + [x_i, x_j] z_J = x_j(z_i z_J + w) + [x_i, x_j] z_J$$

where the right hand side is already defined by f_{d-1}. So this is the only possible choice to define f_d on z_I:

$$x_i z_I = \begin{cases} z_i z_I & \text{if } i \leq I \\ z_i z_I + x_j w + [x_i, x_j] z_J & \text{if } i \not\leq I \end{cases}$$

where $w = x_i z_J - z_i z_J \in P_{d-1}$. For this f_d the first two properties hold by constitution. The third property obviously holds for $i > j$ and $j \leq J$. However, it also holds when $i < j$ and $i \leq J$ since $[x_i, x_j] = -[x_j, x_i]$. In the case $i = j$ it is trivially true. Similarly, if $i \leq J$ or $j \leq J$ then it is true. Therefore, we only have to check the case when $J = (k, K)$ and both $i, j > k$.

In that case,

$$x_j z_J = x_j(x_k z_K) = x_j(x_k z_K) \overset{\text{induction}}{=} x_k(x_j z_K) + [x_j, x_k] z_K = x_k(z_j z_K + w) + [x_j, x_k] z_K$$

for some $w \in P_{d-1}$. Since $k \leq (j, K)$ we can use the induction hypothesis so

$$x_k z_j z_K = z_k z_j z_K$$

Similarly, the third property holds for $x_i(x_k w)$ so finally we get

$$x_i(x_j z_J) = x_i(x_k(x_j z_K)) + x_i([x_j, x_k] z_K) = x_k(x_i(x_j z_K)) + [x_i, x_k](x_j z_K) + [x_j, x_k](x_i, z_K) + [x_i, [x_j, x_k]] z_K$$

in which interchanging the variables and taking the difference one gets

$$x_i(x_j z_J) - x_j(x_i z_J) = x_k([x_i, x_j] z_K) + [x_i, [x_j, x_k]] z_K - [x_j, [x_i, x_k]] z_K \overset{\text{Jacobi}}{=} [x_i, x_j](x_k z_K) + 0$$

as we stated. □

The theorem follows. □

Corollary 4.23. *Let $X = \{x_1, \ldots, x_n\}$ and take $\mathbb{F}\langle X \rangle$ the free associative algebra on X. The Lie subalgebra $\mathcal{L}_X$ of $\mathbb{F}\langle X \rangle$ generated by X is free as a Lie algebra.*

Proof. If we map X into any Lie algebra L then take $U(L)$. By the universality we get a map $F\langle X \rangle \to U(L)$ that proves the free property. □