7 Spezifikation objekt-orientierter Rechte

Zugriffsrechte erlauben oder verbieten Handlungen.

Handlungen beschreiben, wer was bei wem tut.

Zur Beschreibung der Komponenten der Handlung werden **objektorientierte Strukturkonzepte** benutzt, die Klassenbildung und die Klassenhierarchie.
Durch die Klassenhierarchie werden implizit Rechte an Unterklassen vergeben;
durch die Klassen implizit Rechte an Klassenmitglieder.

Dieses Vorgehen kann auch als Erweiterung des klassischen Zugriffskontrollkonzepts der Rechtematrix um objektorientierte Strukturkonzepte (für jede Dimension) angesehen werden.

Andererseits werden explizite Erlaubnis- und **Verbotskennzeichnungen** eingeführt,
insbesondere um bei Rechteänderungen ggf. Rechtekonflikte feststellen zu können.

Durch die expliziten Erlaubnis- und Verbotskennzeichnungen kann überprüft werden, ob die Rechtespezifikation unvollständig oder gar widersprüchlich ist.

Zur Einordnung **widersprüchlicher Rechtespezifikationen** werden zwei Konfliktbegriffe benutzt, den des unmittelbar wirksamen aktuellen Konflikts und den des -evtl. versteckten- Basiskonflikts.

Für Erlaubnisse und Verbote kann es unterschiedliche Klassenhierarchien geben, die allerdings voneinander ableitbar sind.

Um die Rechte kompakter darstellen zu können, wird (ggf. mehrstufig) zwischen allgemeinen Regeln und Ausnahmen dazu unterschieden; syntaktisch werden hierfür **explizite Prioritäten** benutzt.

Wir unterscheiden zwischen spezifizierten Rechten, die Klassennamen enthalten dürfen, und expliziten Rechten, in denen nur noch Objekte vorkommen dürfen und in denen die Priorität entfernt wurde, da dann nur noch das Recht mit der für eine Handlung höchsten Priorität erwähnt wird.

Da die Anzahl der expliziten Rechte i.a. drastisch größer ist als die Anzahl der entsprechenden spezifizierten Rechte, brauchen und liefern wir effiziente Strategien für Anfragen an das Rechtesystem.

Es werden zwei Semantiken für Rechteanfragen vorgestellt, die unterschiedliche Interpretationsmöglichkeiten für Klassennamen deutlich machen.

Einerseits eine Zustandssemantik, die Klassennamen im wesentlichen als Abkürzung verwendet.

Betrachtet man Klassen jedoch als strukturelle Einheiten einer Organisation, so lässt die Zustandssemantik einige Wünsche offen, die die Struktursemantik erfüllen kann.

Zur Begrenzung des Wirkungsbereichs der Prioritäten werden **partiell geordnete Prioritäten** eingeführt und typische Anwendungsbereiche wie Strukturierung von Rechtestrategien, verteilt arbeitende Rechteadministratoren oder Strukturierung in Rechtepakete vorgeführt.

Insbesondere werden effiziente Algorithmen zur Erkennung von Rechtekonflikten und zur Berechnung der Struktursemantik vorgestellt.

7.1 Objektorientierte Spezifikation von Handlungen

Bevor wir Rechte bezüglich eines Weltausschnittes modellieren können, müssen wir zunächst festlegen, was in unserem Weltausschnitt überhaupt vorhanden ist, also als Bestandteil eines Rechtes auftreten kann.

7.1.1 Subjekt, Operation, Granul; Elementare Handlungen

Eine **Handlung**, die erlaubt oder verboten werden kann, wird durch ein Tripel festgelegt, das aus je einer Beschreibung für Subjekt(e), Operation(en) und Granul(e) besteht[2].

Wir müssen also zunächst die möglichen Subjekte, Operationen und Granule festlegen.

Dazu behandeln wir die Menge der Subjekte, die Menge der Operationen und die Menge der Granule jeweils unabhängig voneinander.

Dies heißt jedoch nicht, dass ein Objekt nur einer dieser Mengen angehören kann.

Insbesondere gibt es dabei keine Beschränkung, dass die Menge der Subjekte mit der Menge der Granule disjunkt ist, so dass ein Bestandteil durchaus in einem Recht als Subjekt und in einem anderen Recht als Granul vorkommen kann.

---

2 Wir verwenden zur Beschreibung von Handlungen die klassische SPO-Reihenfolge des englischen Satzbaus: Subjekt, Prädikat, Objekt.

Definition: S sei die Menge der **Subjekte**, O die Menge der **Operationen** und G die Menge der **Granule**[3].
Die Menge aller elementaren Handlungen ist $EA:=S\times O\times G$.
Eine **elementare Handlung** ist also ein Tripel $ea=(es,eo,eg) \quad S\times O\times G$.

Da die drei verschiedenen Komponenten einer Handlung (der Aspekt des Subjekts, der Operation und des Granuls) nach im wesentlichen einheitlichen Verfahren behandelt werden, möchten wir manchmal einen Oberbegriff für diese Komponenten benutzen. Dann bezeichnen wir sie als **Kategorien**.

7.1.2 Klassen, Klassenhierarchien; Handlungen

Subjekte können jeweils geeignet zu Klassen zusammengefasst werden, ebenso Operationen und Granule.

Allerdings müssen wir syntaktisch zwischen Klassen- und Objektnamen, also den Namen der Klassenmitglieder, unterscheiden können; daher schreiben wir in unseren Beispielen Klassennamen mit großen Anfangsbuchstaben und Objektnamen mit kleinen.

Wir verlangen i.a. nicht, dass ein Objekt höchstens zu einer Klasse gehört oder dass jedes Objekt zu mindestens einer Klasse gehört.

Ebenso brauchen die Mengen der Subjektklassen, Operationsklassen und Granulklassen nicht disjunkt zu sein.

---

3 Genaugenommen müssten wir zwischen potentiellen (abzählbar unendlich vielen) und tatsächlich vorkommenden (endlich vielen) Subjekt-, Operations- und Granulmengen unterscheiden.
Wir bezeichnen hier nur die Menge der tatsächlich vorkommenden Subjekte, Operationen und Granule und setzen voraus, dass für Änderungen stets genügend neue Namen zur Verfügung stehen.

Definition: Sei SC die Menge der **Subjektklassen**, OC die Menge der **Operationsklassen** und GC die Menge der **Granulklassen**[4].
Wir setzen voraus, dass $S \cap SC = \emptyset$, $O \cap OC = \emptyset$ und $G \cap GC = \emptyset$ gilt.
Allgemein ist dann die Menge aller Handlungen $A := (S \quad SC) \times (O \quad OC) \times (G \quad GC)$.
Eine **Handlung** ist also ein Tripel $a=(s,o,g) \quad (S \quad SC) \times (O \quad OC) \times (G \quad GC)$.

Klassenmitgliedschaften werden durch Funktionen beschrieben, die einen Klassennamen in die Menge ihrer Klassenmitglieder abbilden:

$mc_S : SC \rightarrow \quad (S)$,
$mc_O : OC \rightarrow \quad (O)$,
$mc_G : GC \rightarrow \quad (G)$.

Insbesondere um die Abweichungen der Klassenmitgliedschaften in der Zukunft und Vergangenheit von der Gegenwart technisch grob zu simulieren (vgl. Kapitel 7.5.3), nehmen wir manchmal an, dass jede Klasse automatisch ein formales **charakteristisches Objekt** enthält, das wir mit _Klassenname bezeichnen. Diesen charakteristischen Objekten kann individuell kein Recht gegeben werden. Trivialerweise schließen wir so auch leere Klassen aus.

---

4 Fussnote 3 gilt analog auch für Klassen.

Wir benutzen die folgende Abkürzung, um (mehrfache) Klassenmitgliedschaften zu beschreiben (und analog für Granule und Operationen):

Bezeichnung:

$classes_S$: S → (SC) mit

$classes_S(s) := \{sc \quad SC \mid s \quad mc_S(sc)\}$

Für einelementige Mengen identifizieren wir die Menge mit dem Element.

Für die Subjektklassen, Operationsklassen und Granulklassen gibt es jeweils eine **Klassenhierarchie**.

Eine Klasse darf mehrere Oberklassen haben.
Die intuitive Vorstellung, dass eine Oberklasse (neben den eigenen Elementen) implizit alle Elemente seiner Unterklassen[5] enthält, wird sich als praktisch herausstellen.

---

5 Im folgenden Beispiel ist (für Erlaubnisse) insbesondere die Klasse Arzt Unterklasse der Klasse Zivildienstleistender, was bedeutet, dass alle Elemente der Klasse Arzt auch Elemente der Klasse Zivildienstleistender sind.
Die soll nicht ausdrücken, dass alle Ärzte stets Zivildienstleistende sind, sondern dass alle Ärzte insbesondere alle Erlaubnisse von Zivildienstleistenden haben.

Wir modellieren diese drei Klassenhierarchien durch azyklische, reflexive, transitive Relationen, indem wir (Klassen, Oberklassen)-Paare angeben:

$\leq_S$ $SC \times SC$,
$\leq_O$ $OC \times OC$,
$\leq_G$ $GC \times GC$.

Der reflexive Teil der Relation modelliert die Existenz einer Klasse, der irreflexive Teil die Klassenhierarchie.

Wir bezeichnen die Menge der Unterklassen bzw. der Oberklassen einer Klasse c folgendermaßen:

Bezeichnung:

$subclasses_S(c) := \{c' \mid c' \leq_S c\}$, und (3.4a)
$superclasses_S(c) := \{c' \mid c' \geq_S c\}$ (3.4b)

(und analog für Granule und Operationen).

Gibt es keine Mehrdeutigkeiten, so lassen wir den Index weg.

Wir haben also alle Kategorien unabhängig voneinander modelliert und werden diese auch später unabhängig voneinander auswerten.

Das Rechtesystem kann z.B. auf den vorhandenen Klassen und Klassenhierarchien eines objektorientierten Systems aufbauen; die Klassen oder Klassenhierarchien können aber auch speziell für das Rechtesystem (z.B. eines nicht objektorientierten Systems) entworfen werden.

Es ist jedoch klar, dass in typischen objektorientierten Systemen die Klassen sowohl Methoden (als Operationen) als auch Attribute (als Granule) enthalten, man es also mit kombinierten Operation-Granul-Klassen zu tun hat.

Dann betrachtet man nur zwei Kategorien, nämlich Subjekte und Operation-Granul-Kombinationen.

Wir verfolgen im Folgenden jedoch unseren allgemeinen Ansatz weiter, da er systematischer ist und die Reduktion von drei auf zwei Kategorien (von denen eine dann wieder zusammengesetzt ist) kein Problem wesentlich vereinfacht.

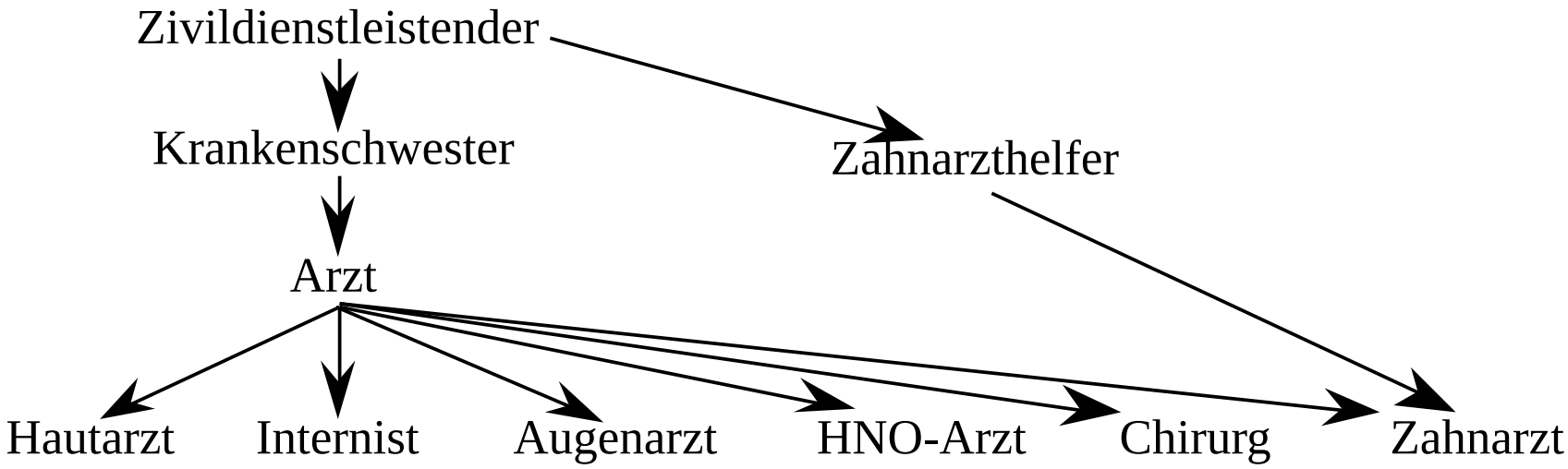
7.1.3 Beispiel

Wir spezifizieren einen Ausschnitt des medizinischen Bereichs.

Wir veranschaulichen die Klassenhierarchien und Objekt-Klassenbeziehungen graphisch.

Bei den Klassenhierarchien veranschaulichen wir z.B. Hautarzt $\leq_S$ Arzt durch Arzt ➜ Hautarzt.

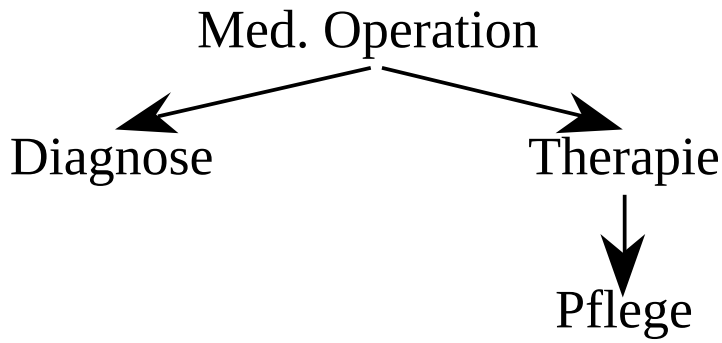
Wir benutzen hier als Bedeutung der
- Subjektklassenhierarchie "**darf weniger**" (also z.B. "Ein Arzt darf weniger als ein Hautarzt"),
- Operationsklassenhierarchie "**ist nicht so sensibel**" und
- Granulklassenhierarchie "**ist Teil von**".



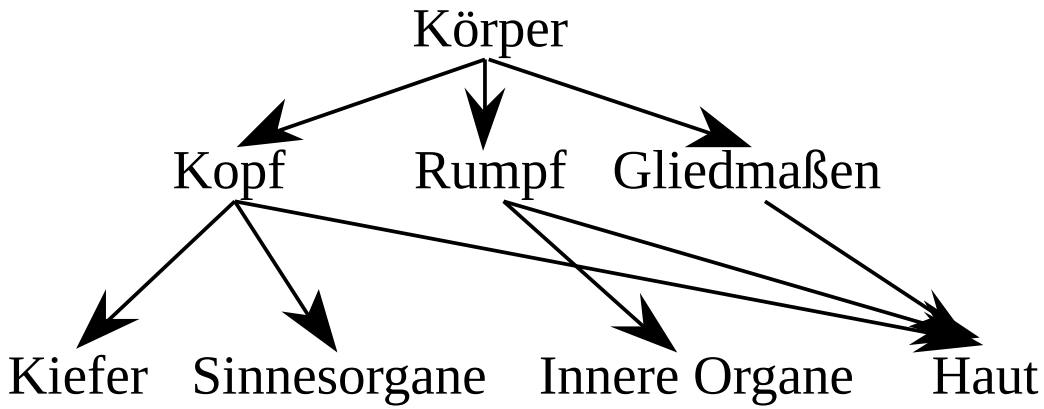
Hierarchie der Subjektklassen für Erlaubnisse[6]

Die (Subjekt-)Klasse Hautarzt ist direkte Unterklasse von Arzt.

6 In Kapitel 7.3.2 wird sich herausstellen, dass wir für Erlaubnisse und Verbote unterschiedliche Klassenhierarchien betrachten müssen.



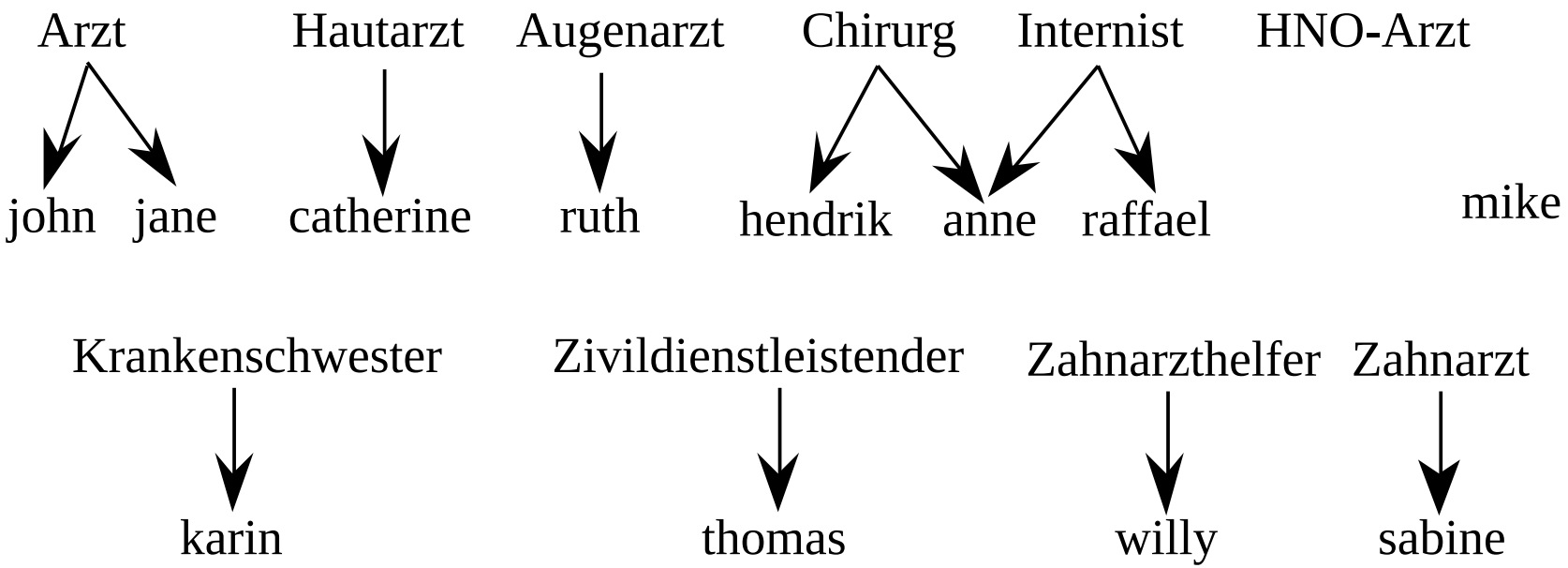
Hierarchie der Operationsklassen für Erlaubnisse



Hierarchie der Granulklassen (für Erlaubnisse)

Die (Granul-)Klasse Haut hat drei direkte Oberklassen: Kopf, Rumpf, Gliedmaßen.

Bei den Objekt-Klassenbeziehungen veranschaulichen wir z.B. john Arzt graphisch durch Arzt ➜ john.



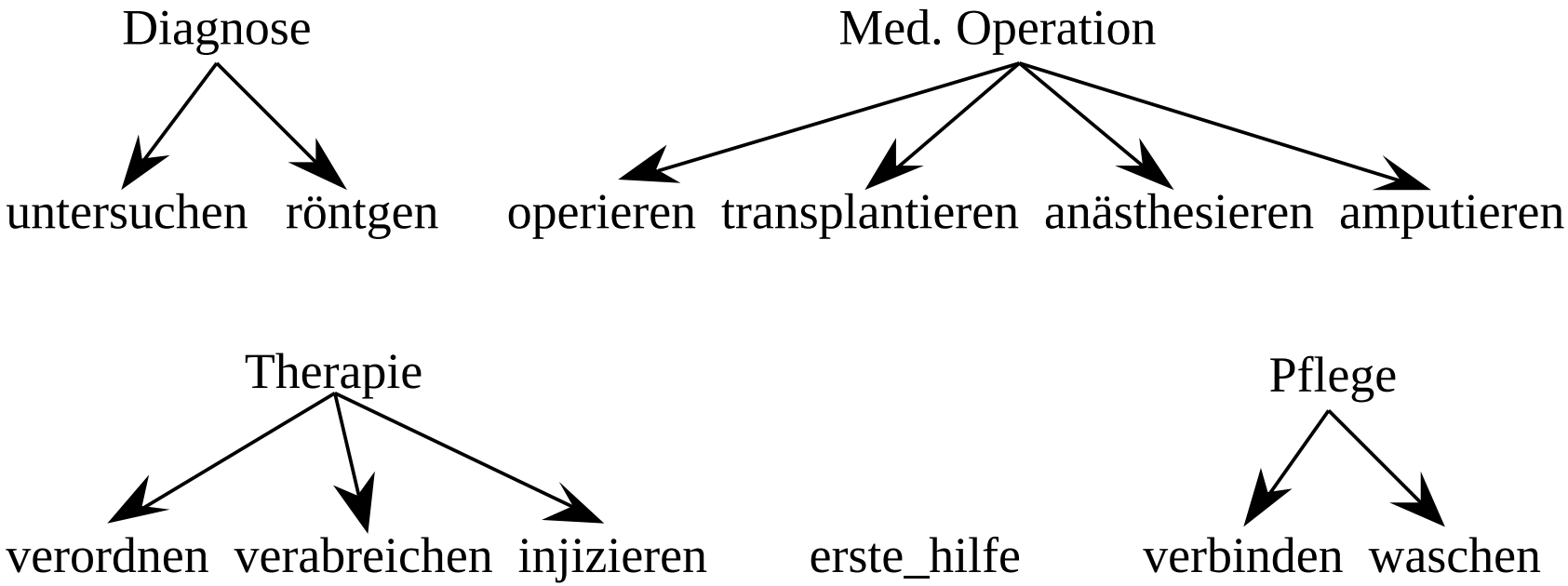
Objekt-Klassenbeziehungen für Subjekte

john und jane sind Subjekte der Klasse Arzt.

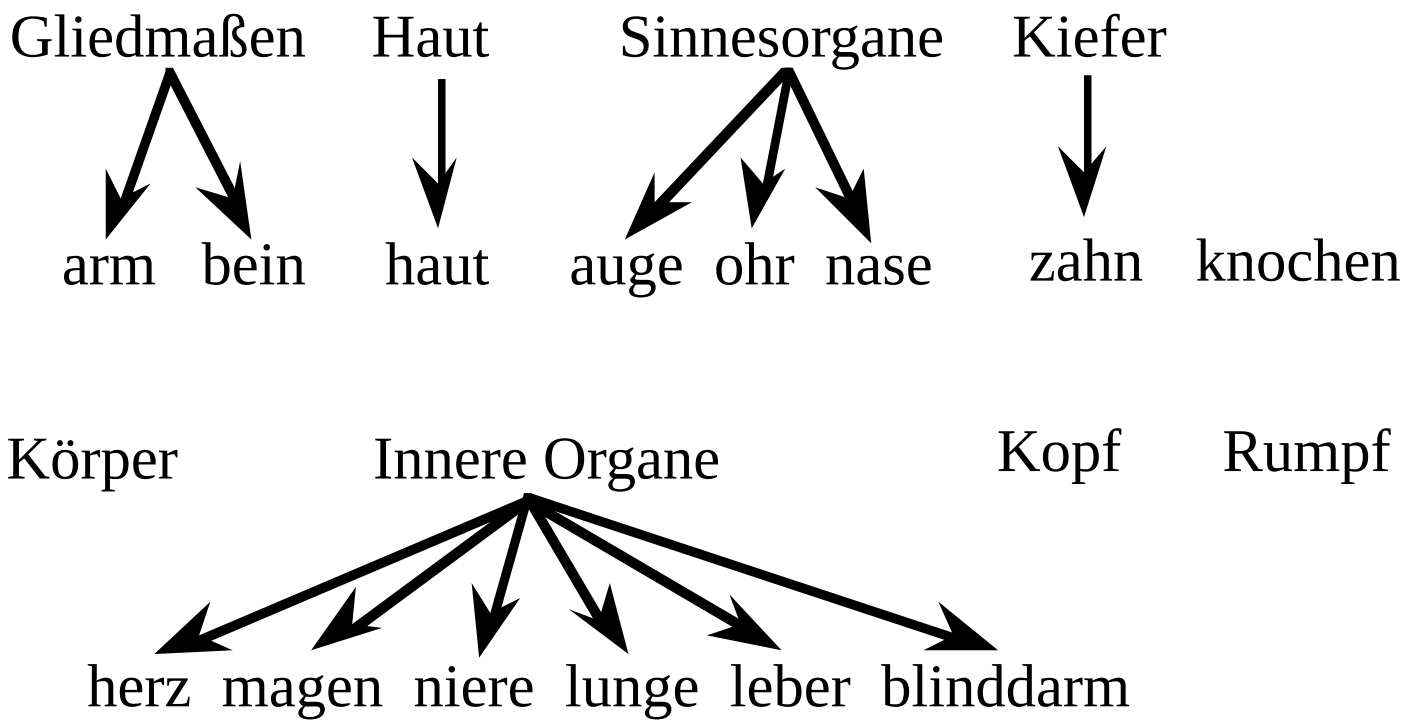
anne ist Mitglied der zwei Klassen Chirurg und Internist.

Das Subjekt mike gehört keiner Klasse an.

Die Klasse HNO-Arzt ist leer.



Objekt-Klassenbeziehungen für Operationen



Objekt-Klassenbeziehungen für Granule

Eine elementare Handlung wäre z.B. ea=(raffael, röntgen, lunge),
eine Handlung wäre a=(thomas, waschen, Kopf).

Die charakteristischen Objekte sind der Übersichtlichkeit halber dabei nicht mit aufgeführt, es gilt aber z.B. _Arzt mc_S(Arzt), _Diagnose mc_O(Diagnose), _Körper mc_G(Körper).