Mathematik und Logik (2011W)

3. Übungsaufgaben

bis 2011-11-17

1. Formulieren Sie zu den bisherigen Übungen oder zum Stoff der Vorlesung mindestens eine konkrete inhaltliche Frage, entweder betreffend ein Problem, das Sie tatsächlich nicht verstehen, oder in Form eines Problems, das Ihnen als Prüfungsfrage geeignet erscheint. Posten Sie diese im KUSSS-Diskussionsforum zu dieser Vorlesung (`https://www.kusss.jku.at/kusss/forumview.action?forum=1883`). Beantworten Sie weiters mindestens 4 Antworten auf die Fragen der anderen, oder auch Kommentare zu bereits vorhandenen Antworten. Um die Übersichtlichkeit zu wahren, sollten Sie besondere Sorgfalt bei der Formulierung eines möglichst aussagekräftigen und doch kurzen Betreffs walten lassen; auch bei den Antworten sollte der Betreff angepaßt werden.

2. Informieren Sie sich über das RSA-Verfahren (z.B.: `http://de.wikipedia.org/wiki/RSA-Kryptosystem`), insbesondere jene Aspekte, bei denen die in der Vorlesung besprochene Zahlentheorie Anwendung findet. Sollte dabei etwas unklar bleiben, ist auch dies als Frage für das Diskussionsforum geeignet.

3. Suchen Sie im gesamten bisher besprochenen Stoff Aussagen, in denen eine Disjunktion vorkommt. Arbeiten Sie genau heraus, wie dann in den Beweisen die Introduktions- und Eliminationsregeln für die Disjunktion verwendet werden.

4. Beweisen Sie ein paar triviale Sätze über die Disjunktion:

   (a) $A \implies A \lor B$;

   (b) $A \land B \implies A \lor B$;

   (c) $A \lor B \iff B \lor A$;

   (d) $A \iff A \lor A$;

   (e) $A \lor (B \lor C) \iff (A \lor B) \lor C$.

   Formulieren und beweisen Sie analoge Sätze für die Konjunktion.

5. Beweisen Sie:

   (a) $A \implies A \land A$;

   (b) $A \land A \implies A$.

   (c) $A \land (B \land C) \implies (A \land B) \land C$;

   (d) $(A \land B \implies C) \implies (A \implies B \implies C)$;

   (e) $(C \implies A) \land (C \implies B) \implies (C \implies A \land B)$;

   (f) $(C \implies A \land B) \implies (C \implies A) \land (C \implies B)$;

   (g) $(A \land B \implies A) \land (A \land B) \implies B)$.

6. Beweisen Sie

$$(A \implies B) \lor (C \implies D) \implies (A \lor C \implies B \lor D).$$

Gilt auch die Umkehrung?

7. Mit $\perp$ bezeichnen wir die Aussage "Jede Aussage ist wahr"; und P sei irgendeine Aussage. Was halten Sie dann von den Aussagen $\perp \implies P$ und $P \implies \perp$?

8. Versuchen Sie die folgenden Sätze der Minimallogik (in dieser kommt nur Implikation vor) zu beweisen:

   (a) $(A \implies B) \implies (B \implies C) \implies A \implies C$;

   (b) $(A \implies B \implies C) \implies (B \implies A \implies C)$;

   (c) $A \implies A$;

   (d) $(A \implies A) \implies (A \implies A)$;

   (e) $(A \implies B) \implies (A \implies B)$;

   (f) $(A \implies C) \implies A \implies B \implies C$;

   (g) $(A \implies A \implies B) \implies (A \implies B)$;

   (h) $(A \implies B) \implies (A \implies A \implies B)$;

   (i) $(A \implies B) \implies (B \implies A)$;

   (j) A;

   Anmerkung: Fehlen bei der Implikation die Klammern, so ist sie immer rechtsassoziativ zu verstehen (vgl. `http://de.wikipedia.org/wiki/Operatorrangfolge`). Insbesondere ist eine Formel der Form $X \implies Y \implies Z$ stets wie $X \implies (Y \implies Z)$ zu lesen, und niemals wie $(X \implies Y) \implies Z$.

9. Versuchen Sie

$$((((A \implies B) \implies A) \implies A) \implies B) \implies B.$$

   zu beweisen.

   Anmerkung: Dieser Beweis ist leichter zu finden, als er aussieht. Es kommen nur 2 logische Schlußregeln in Frage, und in jedem Beweisschritt ist stets nur eine davon wirklich anwendbar. Sie müssen aber genau aufpassen, welche Aussagen jeweils Annahmen sind, und welche zu zeigen sind, und dann immer nachsehen, welche Annahme gerade helfen könnte, um das aktuelle Beweisziel zu erreichen.

10. Ersetzen Sie im (normalen) Distributionsgesetz (für Zahlen) die Multiplikationen durch Konjunktionen und die Additionen durch Disjunktionen (und auch umgekehrt) sowie die normale Gleichheit durch die logische Äquivalenz. Beweisen Sie all diese (auf diese Art gewonnenen) logischen Distributivgesetze.

    Was passiert, wenn im arithmetischen Distributivgesetz die Additionen und Multiplikationen vertauscht werden?

    Gibt es auch logische Distributivgesetze, bei denen die Implikation beteiligt ist?