広域数理科学概論 (4)

担当：内田　幸寛

講義の内容

代数的整数論の基礎的内容を数論アルゴリズムの観点から講義する．その応用として，素因数分解のアルゴリズムである 2 次篩法，数体篩法について講義する．具体的な内容は以下の通りである．ただし，状況に応じて変更することがある．

- 導入・体論の復習
- 代数的整数の定義と基本的な性質
- 素イデアル分解
- イデアル類群の有限性・ディリクレの単数定理
- 素因数分解アルゴリズム（2 次篩法・数体篩法）
- まとめ・レポート

テキスト・参考書等

教科書は特に指定しない．参考書として以下を挙げておく．

- 木田雅成『数理・情報系のための整数論講義』SGC ライブラリ 58，サイエンス社，2007.
- 雪江明彦『整数論 1：初等整数論から p 進数へ』日本評論社，2013.
- F. Jarvis, *Algebraic Number Theory*, Springer Undergraduate Mathematics Series, Springer, 2014.
- R. Crandall, C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, 2nd ed., 2005（邦訳：和田秀夫監訳『素数全書―計算からのアプローチ』朝倉書店，2010）.

成績評価方法

授業参加度 (30%)，レポート (70%) により評価する．

オフィスアワー

8 号館 6 階 667 室，水曜日 5 時限 (16:20–17:50)

ウェブページ

`http://www.comp.tmu.ac.jp/y-uchida/lectures/2015ko4/`

講義に関する情報をここに掲載する．