

# 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。

- イントロダクション及びガイダンス
- 整拡大・整閉整域
- ネーター環・デデキント環・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

テキストは特に指定しない。参考書として以下を挙げておく。

- P. サミュエル著，織田進訳『数の代数的理論』（丸善出版，2012）
- F. Jarvis, Algebraic Number Theory, 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4時限 (14:40–16:10)

## ウェブページ

<http://www.comp.tmu.ac.jp/y-uchida/lectures/2017ko4/>

講義に関する情報をここに掲載する。