

|      |                                                                       |     |                                |      |        |             |      |      |
|------|-----------------------------------------------------------------------|-----|--------------------------------|------|--------|-------------|------|------|
| 科目名  | 応用数学特論                                                                |     |                                | 担当教員 | 谷口 浩朗  |             |      |      |
| 学年   | 専攻科                                                                   | 1年  | 学期                             | 前期   | 履修条件   | 選択          | 単位数  | 2    |
| 分野   | 一般                                                                    |     | 授業形式                           | 講義   | 科目番号   | 09AG1_20060 | 単位区別 | 学修単位 |
| 学習目標 | 素因数分解、群の概念、射影平面上の曲線について学習する。その応用として平面3次曲線・楕円曲線法を学習する。                 |     |                                |      |        |             |      |      |
| 進め方  | 準備した教材プリントに基づき、出来るだけ多くの時間を演習に振り向けて、問題を解く手続きの中で、理解を深めながら進む。また適宜課題も与える。 |     |                                |      |        |             |      |      |
| 履修要件 |                                                                       |     |                                |      |        |             |      |      |
|      | 学習項目 (時間数)                                                            |     |                                |      | 学習到達目標 |             |      |      |
| 学習内容 | 1 有限体                                                                 | (2) | 有限体に慣れる。D1:1                   |      |        |             |      |      |
|      | 2 素因数分解 $\rho$ 法                                                      | (2) |                                |      |        |             |      |      |
|      | 3 素因数分解 $p-1$ 法                                                       | (2) |                                |      |        |             |      |      |
|      | 4 群・置換群                                                               | (2) | 群の概念に慣れる。D1:1                  |      |        |             |      |      |
|      | 5 群・置換群 演習                                                            | (2) |                                |      |        |             |      |      |
|      | 6 部分群・正規部分群                                                           | (2) |                                |      |        |             |      |      |
|      | 7 部分群・正規部分群 演習                                                        | (2) |                                |      |        |             |      |      |
|      | 8 射影平面と直線                                                             | (2) | 射影平面の概念に慣れる。D1:1               |      |        |             |      |      |
|      | 9 射影平面上の3次曲線                                                          | (2) | 射影平面上の3次曲線の計算が出来るようになる。D1:1, 2 |      |        |             |      |      |
|      | 10 平面3次曲線の群構造                                                         | (2) |                                |      |        |             |      |      |
|      | 11 平面3次曲線の群構造(演習)                                                     | (2) | 3次曲線の群の計算が出来るようになる。D1:1, 2     |      |        |             |      |      |
|      | 12 有限体上の3次曲線                                                          | (2) |                                |      |        |             |      |      |
|      | 13 楕円曲線法による素因数分解                                                      | (2) | 楕円曲線法を理解する。D1:1                |      |        |             |      |      |
|      | 14 楕円曲線法による素因数分解(演習)                                                  | (3) |                                |      |        |             |      |      |
|      | 15 前期期末試験                                                             | (1) |                                |      |        |             |      |      |
|      | 16 試験問題の解答と授業評価アンケート                                                  | (1) |                                |      |        |             |      |      |
| 評価方法 | 定期試験(70%)，レポート(30%)で総合評価する。                                           |     |                                |      |        |             |      |      |
| 関連科目 | 基礎数学Ⅱ，応用解析学                                                           |     |                                |      |        |             |      |      |
| 教材   | 教材プリントを使用 参考書：佐武一郎 著「線型代数学」 数学選書1 裳華房                                 |     |                                |      |        |             |      |      |
| 備考   | 特になし                                                                  |     |                                |      |        |             |      |      |