MATH 402/502 Weekly Update

Answers to the exercises in **bold font** and to all the additional exercises (not from the book) should be submitted for grading.

• **Week 1** Definitions of ring, integral domain and field. Simple examples (for instance $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Z}[x], \mathbb{Z}[i], \mathbb{Z}[\sqrt{2}], \mathbb{R}[x], M_n(\mathbb{Z})$) and properties (e.g. $a0 = 0$). Subrings, direct sums. A finite integral domain is a field. The fields $\mathbb{Z}_p$.

HW **12.1, 12.2, 12.3, 12.4, 12.11.** Also: let S be a finite set, and let $\mathcal{P}(S)$ be the power set of S. Show that $\mathcal{P}(S)$ can be made into a ring with addition $A \triangle B$ and multiplication $A \cap B$. Does this make $\mathcal{P}$ into a field? Could I have defined the addition to be $A \cup B$? Due 9 April

• **Week 2** The characteristic of a ring. Ideals, principal ideals and factor rings, with examples. Prime and maximal ideals. Ring homomorphisms.

HW 14.4, 14.5, 14.6, **14.8, 14.12, 14.16, 14.38, 14.41, 14.53, 14.58 and question 38 on page 278**. Due 16 April

• **Week 3** Properties of ring homomorphisms. The isomorphism theorem for rings. Prime subfields. The field of quotients of an integral domain.

HW 15.5, 15.8, 15.10, 15.13, **15.21, 15.22, 15.30, 15.42, 15.44, 15.56**. Due 26 April

• **Week 4** Polynomial rings. Division algorithm, remainder and factor theorems. Lagrange's theorem for polynomials over a field.

HW No homework this week.

• **Week 5** $F[x]$ is a principal ideal domain if F is a field. Tests for irreducibility over $\mathbb{Z}$ and $\mathbb{Q}$: Gauss's theorem, Eisensteins's criterion, and reduction mod n. If F is a field, $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over F. Euclid's lemma for polynomials over a field.

HW No homework this week. Exam on Friday.

• **Week 6** Associates, irreducibles and primes. Euclidean domains (EDs), principal ideal domains (PIDs), and unique factorization domains (UFDs), with examples. The ascending chain condition. ED $\implies$ PID $\implies$ UFD.

HW 18.33, 18.35, **18.38, 18.40 and question 6 on page 341**. Also: for $p = 3, 7, 11$, define the sets R_p by

$$R_p = \{a + b(\tfrac{1+\sqrt{-p}}{2}) | a, b \in \mathbb{Z}\}$$

Show that the R_p are all Euclidean domains. Due 14 May

• **Week 7** Review of vector spaces: definition, subspaces, linear span, linear independence, bases, Steinitz exchange lemma, dimension. Extension fields. Kronecker's theorem. Existence and uniqueness of splitting fields.

HW No homework this week.

• **Week 8** Zeros of irreducible polynomials. Formal differentiation. The Frobenius map. Finite extensions; tower law.

HW **20.2, 20.4, 20.8, 20.14, 20.26.** Also: draw a Venn diagram illustrating the relationship between algebraic, finite, simple and transcendental extensions. Is every finite extension simple? If so, prove it. If not, give a counterexample. Due 28 May

• **Week 9** Algebraic and transcendental extensions; simple extensions. Primitive element theorem. Classification of finite fields. Fermat's theorem on sums of two squares.

HW None this week.

• **Week 10** Ruler and compass constructions. Review.

HW None this week. Exam next week.

Extra Credit Homework

Here is Euler's proof that $x^3+y^3 = z^3$ has no nontrivial solutions in integers. Fill in the details.

1. Suppose that (x, y, z) is a nontrivial solution. Show that, without loss of generality, we may assume that no two of x, y and z have a common factor, and that, also without loss of generality, x and y are odd and z is even.

2. Show that, consequently, there must exist coprime positive integers p and q, one even and the other odd, such that $2p(p^2 + 3q^2)$ is a perfect cube. [Hint: $x + y$ and $x - y$ are both even.]

3. Assume now that $3 \nmid p$. Use the identity $p^2+3q^2 = (p-q\sqrt{-3})(p+q\sqrt{-3})$, together with the unique factorization property of the ring R_3 defined on the previous page, to show that there must exist coprime integers a and b, one even and the other odd, such that

$$p = a(a - 3b)(a + 3b) \quad \text{and} \quad q = 3b(a - b)(a + b)$$

Complete the proof for this case ($3 \nmid p$), using Fermat's method of infinite descent.

4. Now assume that $3 \mid p$. Write $p = 3s$, and hence dispatch this case also.

Historical note. Euler's proof for Steps 3 and 4 was incomplete.