UNIVERSITY OF ST ANDREWS
MT5826 Finite Fields
Tutorial Sheet: Chapter 1

1. For the equivalence relation *congruence modulo* n on $\mathbb{Z}$, show that

(a) the binary operation

$$[a] + [b] = [a + b]$$

is well-defined, i.e. does not depend on our choice of representatives;

(b) the set $\{[0], [1], \ldots, [n-1]\}$ forms a group under this operation;

(c) this group is cyclic with $[1]$ as a generator.

2. Let ϕ denote Euler's phi function: for $n \in \mathbb{N}$, $\phi(n)$ is the number of integers k with $1 \leq k \leq n$ and $\gcd(k, n) = 1$. Prove that

(a) For $n > 1$, $\phi(n) = n - 1 \Leftrightarrow n$ is prime.

(b) If p is prime and $k > 0$, then

$$\phi(p^k) = p^k - p^{k-1}.$$

(c) $\phi(mn) = \phi(m)\phi(n)$ if $\gcd(m, n) = 1$.

(d) If n has prime factorization $p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, then

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r}).$$

3. Let $G = \langle a \rangle$ be a group of finite order m. Prove that

(a) for any positive divisor d of m, G contains one and only one subgroup of index d;

(b) for any positive divisor f of m, G contains one and only one subgroup of order f.

(Hint: this is part (iii) of Theorem 1.13 of the notes; you may wish to use parts (i) and (ii) in your proof.)

4. (a) Show that $(\mathbb{Z}, +, *)$ is an integral domain but not a field.

(b) Show that the set of 2×2 matrices with entries from $\mathbb{R}$, with matrix addition and multiplication, form a non-commutative ring with an identity.

(c) Show that $\mathbb{Z}_n$, with operations $[a] + [b] = [a + b]$ and $[a][b] = [ab]$, is a commutative ring with an identity.

5. For the following statements, decide whether each is True/False and give a proof or counterexample as appropriate: (a) $\mathbb{Z}$ is a subring of $\mathbb{Q}$; (b) $\mathbb{Z}$ is an ideal of $\mathbb{Q}$.

6. Prove the assertion in Example 2.7 of the notes that $\mathbb{Z}$ is a principal ideal domain. You may wish to use the following proof outline:

- Either $I = \{0\}$, or
- $I \neq \{0\}$. In this case, I contains both positive and negative elements. Let m be the least positive element of I.
  Show that $I = (m)$. (Hint: Consider $a \in I$ and use the Division Algorithm to write $a = mq + r$.)

7. Show that $\mathbb{Z}/(n)$ is not a field when n is composite.

8. Write out the addition and multiplication tables for $\mathbb{F}_7$.

9. Prove the fact (needed in the proof of Freshmen's Exponentiation) that p is a divisor of $\binom{p}{i}$, for any $i \in \mathbb{Z}$ with $0 < i < p$.

10. Find all irreducible polynomials over $\mathbb{F}_2$ of degree 4.

11. Each residue class $g + (f)$ of $F[x]/(f)$ contains at least one representative $r \in F[x]$ with $\deg r < \deg f$, namely the remainder when g is divided by f. Prove that this representative is unique.

12. (a) State (without considering elements) whether the following are fields: (i) $\mathbb{F}_3[x]/(x^3 - x - 1)$; (ii) $\mathbb{F}_5/(x^3 - x^2 + x - 1)$.

(b) Is $\mathbb{F}_3[x]/(x^3 - x - 1) \cong \mathbb{F}_3[x]/(x^3 - x + 1)$?

(c) What is the multiplicative order of $x + (x^3 - x - 1)$ in $\mathbb{F}_3[x]/(x^3 - x - 1)$? (Hint: it must divide $3^3 - 1$.)

13. Write out addition and multiplication tables for

(a) $\mathbb{F}_3[x]/(f)$ where $f(x) = x^2 + 1$;

(b) $\mathbb{F}_2[x]/(f)$ where $f(x) = x^3 + 1$.

In each case decide whether or not it is a field, giving justification.

14. Let $a \in F$, where F is a field. Prove that

(a) If a is a multiple root of $f \in F[x]$, then it is a root of both f and its derivative f'.

(b) If a is a root of both f and its derivative f', then it must be a multiple root of f.