GALOIS THEORY
Worksheet 4

Q 1. The Eisenstein criterion is not a brilliant way to decide if a polynomial $f(X) \in \mathbb{Z}[X]$ is irreducible. A much better strategy is to choose a prime p and show that the reduction of f modulo p is irreducible in $\mathbb{F}_p[X]$.

Make a list of all monic irreducible polynomials of degree 2 and 3 in $\mathbb{F}_2[X]$. Make a list of all monic irreducible degree 2 polynomials in $\mathbb{F}_3[X]$, and $\mathbb{F}_5[X]$. (This is most definitely NOT a stupid thing to do.)

Q 2. The purpose of this question is to make the proof of the Gauss Lemma more digestible.

(a) Prove that if R is a commutative ring with 1, and $x \in R$ then $0x = 0$.

(b) Prove that if K is a field and $a, b \in K$ are both non-zero, then $ab \neq 0$.

(c) If K is a field and $f = \sum_{i=0}^{d} a_i X^i \in K[X]$ is a non-zero polynomial, then (by choosing d sensibly) we may assume $a_d \neq 0$; we call $a_d X^d$ the *leading term* of f, and d the *degree* of f, and we write $d = \deg(f)$. Prove that if $f, g \in K[X]$ are non-zero, then fg is also non-zero, and $\deg(fg) = \deg(f) + \deg(g)$.

(d) Prove that if $f, g, h \in K[X]$ and $h \neq 0$ and $fh = gh$, then $f = g$ (the cancellation property for polynomial rings).

[Some of you will know that $f, g \neq 0 \implies fg \neq 0$ is the assertion that $K[X]$ is an *integral domain*. **Note** that we used the fact that $\mathbb{F}_p[X]$ is an integral domain in the proof of the Gauss Lemma.]

Q 3. Let A denote the set of complex numbers that are algebraic (over $\mathbb{Q}$).

(i) Prove that A is a field.

(ii) Prove that $[A : \mathbb{Q}] = \infty$. [*Hint*: you can use Eisenstein to construct irreducible polynomials of large degree.]

(iii) Prove that $[\mathbb{C} : A] = \infty$.

Q 4. In this question, let K be a field of characteristic **zero**.

(a) Prove that every irreducible polynomial $f \in K[X]$ is separable. [*Hint*: Jacobian criterion.]

(b) If suppose that $f, g \in K[X]$ are monic, irreducible, and distinct. Prove that fg is a separable polynomial.

(c) Suppose that $K \subset L$ is the splitting field of some polynomial. Show that $K \subset L$ is the splitting field of a separable polynomial.