GALOIS THEORY
Solutions to Worksheet 4

A 1. I will make a few comments (and I will not finish the question).

A polynomial of degree ≤ 3 in $\mathbb{F}_p[X]$ is irreducible if and only if it has no roots in $\mathbb{F}_p$, and this can be checked by evaluating at all elements $0, \dots, p-1 \in \mathbb{F}_p$.

For example with $p = 2$ the only irreducible quadratic polynomial is:

$$X^2 + X + 1$$

and the irreducible cubic polynomials are:

$$X^3 + X + 1, \quad X^3 + X^2 + 1$$

For $p = 3$ there are 3 irreducible monic quadratic polynomials; they are:

$$X^2 + 1, \quad X^2 + X - 1, \quad X^2 - X - 1$$

(when you will learn about finite fields, you will know that there are $(27-3)/3 = 8$ irreducible monic cubic polynomial, and it should not be too time-consuming to write them all down...)

For $p = 5$, there are $(25 - 5)/2 = 10$ irreducible monic quadratic polynomial and it should not be too bad to list them all. There are $(125 - 5)/3 = 40$ irreducible monic cubic polynomials in $\mathbb{F}_5[X]$.

A 2. (a) We know 0 is the additive identity in R so $0+0 = 0$. Hence $0x = (0+0)x = 0x+0x$ and subtracting $0x$ (which we can do, because $(R, +)$ is a group so $0x$ has an additive inverse) we deduce $0 = 0x$.

(b) If $a \neq 0$ and $b \neq 0$ then there exist multiplicative inverses a^{-1} and b^{-1}, and now $abb^{-1}a^{-1} = 1 \times 1 = 1$. However if $ab = 0$ then we deduce $0(b^{-1}a^{-1}) = 1$ which contradicts part (a) (as $0 \neq 1$ in a field).

(c) Look at top degree terms.

(d) $fh = gh$ implies $(f - g)h = 0$, and if $h \neq 0$ we must have $f - g = 0$ by (c).

A 3. (i) To check that a subset of a field is a subfield all we need to do is to check 0 and 1 are in, and that the subset is closed under addition, subtraction, multiplication, and division-by-things-that-aren't-zero. These things follow from the tower law: if α, β are algebraic then $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] < \infty$, but then

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\beta) : \mathbb{Q}][\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$$

But then for all $\lambda \in \mathbb{Q}(\alpha, \beta)$ $[\mathbb{Q}(\lambda) : \mathbb{Q}] < \infty$, i.e., λ is algebraic.

(ii) Say for a contradiction that $[A : \mathbb{Q}] = n < \infty$. Let $p(X) = X^{n+1} - 2$ and let $\alpha \in \mathbb{C}$ be a root. Then α is algebraic and its min poly must be $p(X)$ as $p(X)$ is monic and irreducible. So $n = [A : \mathbb{Q}] = [A : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = (n+1)[A : \mathbb{Q}(\alpha)] \geq n + 1 > n$, a contradiction.

(iii) We first argue that A is countable. For each n there are only countably many elements of $\mathbb{Q}[X]$ with degree at most n, and a countable union of countable sets is countable, so there are only countably many polynomials. Each algebraic number is a root of a non-zero polynomial in $\mathbb{Q}[X]$ and such a polynomial has only finitely many roots, and a countable union of finite sets is countable, so A is countable.

If $[\mathbb{C} : A]$ were finite then $\mathbb{C}$ would be isomorphic to A^n for some $n \in \mathbb{Z}_{>0}$ and hence $\mathbb{C}$ would be countable, a contradiction.

A 4. (a) If f has degree n then Df has degree $n-1$; in particular Df is a non-zero polynomial. Because f is irreducible, $\mathrm{hcf}(f, Df)$ is either f or 1. In the first case $f \mid Df$, but then either Df has degree $\geq n$ or $Df = 0$, impossible. So f and Df are coprime so by the Jacobian criterion f is separable.

(b) If $K \subset L$ is a splitting field of fg then I claim that f, g have no common root in L. Indeed f and g are coprime in K, and hence they are coprime in L. (There exist $a(X)$, $b(X)$ in $K[X]$ such that $fa + gb = 1$; this identity is valid in $L[X]$ and it shows that f, g are coprime in $L[X]$.)

(c) Suppose that $K \subset L$ is the splitting field of $f \in K[X]$. Let

$$f = \prod f_i^{r_i}$$

be the prime decomposition of f. It is clear that $K \subset L$ is the splitting field of the polynomial

$$f_{\text{red}} = \prod f_i$$

By a and b, f_{red} is separable.