M3P11 Galois Theory, Problem Sheet 1

[new version: typos in Q2(c) and Q5(b) fixed, and Q6 now only has one part (v)]

1. Let K be a field and let $R = K[x]$ be the set of all polynomials in one variable over K. So an element of R is a finite formal sum $\sum_{i=0}^{d} a_i x^i$ with $a_i \in K$.

If $f = \sum_i a_i x^i$ and $g = \sum_j b_j x^j$ then define $f + g$ and fg in the obvious way: $f + g = \sum_i (a_i + b_i) x^i$ and $fg = \sum_i c_i x^i$ with $c_k = \sum_{i+j=k} a_i b_j$.

Prove that R becomes a commutative ring with a 1 with these definitions of $+$ and $*$.

2.

(a) Prove that if R is a commutative ring with a 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 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).

[Those doing Algebra III will know that $f, g \neq 0 \implies fg \neq 0$ is the assertion that $K[x]$ is an *integral domain.*]

3. Let's goof around in $\mathbb{Q}[x]$.

(a) Find the quotient and remainder when $x^5 + x + 1$ is divided by $x^2 + 1$.

(b) Find the remainder when $x^{1000} + 32x^{53} + 8$ is divided by $x - 1$ (hint: use your head instead of just calculating).

(c) Find polynomials $s(x)$ and $t(x)$ such that

$$(2x^3 + 2x^2 + 3x + 2)s(x) + (x^2 + 1)t(x) = 1.$$

[extra q: I just made those two polynomials above up. How did I know for sure that they were coprime?]

(d) Find an hcf for $x^4 + 4$ and $x^3 - 2x + 4$. Express it as $a(x)(x^4 + 4) + b(x)(x^3 - 2x + 4)$.

4. Prove that if $f, g \in K[x]$ and at least one is non-zero, and if s, t are both hcfs of f and g, then $s = \lambda t$ for some $\lambda \in K^\times$.

5. (a) We know that whether or not a polynomial is irreducible depends on which field it's considered as being over – for example $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{R}[x]$. But show that the notion of divisibility does not depend on such issues. More precisely show that if $K \subseteq L$ are fields, if $f, g \in K[x]$, and if $f \mid g$ in $L[x]$ then $f \mid g$ in $K[x]$.

(b) Is it true that if $f, g \in \mathbb{Z}[x]$ and $f|g$ in $\mathbb{Q}[x]$ then $f|g$ in $\mathbb{Z}[x]$? [hint: no]. Is it true under the extra assumption that f is monic? [hint:yes]

6. Factor the following polynomials in $\mathbb{Q}[x]$ into irreducible ones, giving proofs that your factors really are irreducible.

(i) $x^3 - 8$

(ii) $x^{1000} - 6$

(iii) $x^4 + 4$ (hint: Q3)

(iv) $2x^3 + 5x^2 + 5x + 3$

(v) $x^5 + 6x^2 - 9x + 12$

(vi) $x^{73} - 1$

(vii) $x^{73} + 1$

(viii) $x^{12} - 1$.