Dartmouth College

Mathematics 81/111 — Homework 1

1. In class (cf. [S] Corollary 7.3.13), we showed that if A is an integral domain, then any polynomial $f \in A[x]$ of degree n has at most n distinct roots in A. The crux of the argument is if a is a root of f, then $f = (x-a)g(x)$ for some $g \in A[x]$ having degree $n-1$. So if $b \neq a$ is another root of f, then $0 = f(b) = (b-a)g(b)$, and since A is has no zero divisors, $g(b) = 0$ and the result follows by induction.

   So now let $A = \mathbb{H}$ be Hamilton's quaternions. $\mathbb{H}$ is a four-dimensional vector space over $\mathbb{R}$ with basis $\{1, i, j, k\}$. It is made into a non-commutative division ring via the relations $i^2 = j^2 = k^2 = -1$ and $ij = k = -ji$. More information is in the exercises to §7.1 of [S].

   So let $f(x) = x^2 + 1$. Clearly $f(\pm i) = f(\pm j) = f(\pm k) = 0$. Mimicking the argument above, we see that i is a root of f, so we write $f = x^2 + 1 = (x-i)g(x) = (x-i)(x+i)$. Now j is another root of f and $j \neq i$ (why?) and if we write $0 = f(j) = (j-i)g(j) = (j-i)(j+i)$, we are supposed to conclude that $g(j) = j + i = 0$, but that is clearly not true (again, why?). So the main question is where has the argument failed and why?

2. Let $\varphi : A \to B$ be a ring homomorphism.
   (a) Suppose that $J \subseteq B$ is an ideal. Show
   - $\varphi^{-1}(J)$ is an ideal of A.
   - $\varphi(\varphi^{-1}(J)) \subseteq J$, and give an example to show equality need not hold.
   - Show that equality does hold if φ is surjective.

   (b) Next let $I \subset A$ be an ideal.
   - Show by example that $\varphi(I)$ need not be an ideal of B, but is an ideal if φ is surjective.
   - Assuming that φ is surjective, determine $\varphi^{-1}(\varphi(I))$.

   (c) Use the above to show that there is a one-to-one correspondence between the ideals of A/I and the ideals of A which contain I.

3. Let A be a ring and I a proper ideal in A. Let $\pi : A \to A/I$ be the canonical map. For $f \in A[x]$, let f^π (Lang's notation) denote the image of f in $(A/I)[x]$.
   (a) Show that $A[x]/(I, f(x)) \cong (A/I)[x]/(f^\pi)$.
   (b) Use the previous part to that if $p \in \mathbb{Z}$ is a prime, then (x, p) is a maximal ideal in $\mathbb{Z}[x]$.
   (c) Characterize all ideals I with $(x) \subseteq I \subseteq \mathbb{Z}[x]$. There is certainly more than one way to proceed.

4. Let D be an integral domain, and $a, b \in D$ not both zero. Recall that we say that $d \in D$ is **a gcd** of a and b if $d \mid a$, $d \mid b$ and if c is any other common divisor of a and b then $c \mid d$. We know (or will show) that $\mathbb{Q}[x]$ is a UFD, so in particular gcds exist. Let $A = \mathbb{Q}[x^2, x^3]$, the subring of $\mathbb{Q}[x]$ generated by x^2 and x^3.

(a) Show that A is not a UFD by showing the $\gcd(x^5, x^6)$ does not exist in A.

(b) Determine the structure of $\mathbb{Q}[x^2, x^3]/(x^3)$ as a $\mathbb{Q}$-algebra. You might start by determining its structure as a vector space over $\mathbb{Q}$.

5. Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ be a primitive nth root of unity, that it a generator for the cyclic group, μ_n, of nth roots of unity (all the complex roots of $x^n - 1$).

   (a) Suppose that k, m are integers relatively prime to n. Show that $\dfrac{\zeta_n^m - 1}{\zeta_n^k - 1}$ is a unit in the ring $\mathbb{Z}[\zeta_n]$.

   (b) Show that if $n > 3$ is odd, then $(\zeta_n^2 - 1)/(\zeta_n - 1)$ has infinite order in $\mathbb{Z}[\zeta_n]^\times$.