Fundamentals of Algebra for Computer Science (Home work 3)

November 10, 2006

- Due on Wednesday, November 20, before 4 p.m.
- Late submissions will not be accepted.
- Please give precise arguments for all statements that you write.
- To disprove a fact it is enough to give a counter example.
- Please do not hesitate to contact me if you do not understand the problems.
- Each problem in this homework bear 5 points.

1. **Ideals**

   (a) A and B are ideals in a ring R such that $A \cap B = (0)$, prove that for every $a \in A$ and $b \in B$, $ab = 0$.

   (b) Let R be a commutative ring and A be an ideal of R. Let $N(A) = \{x \in R : x^n \in A, \text{ for some } n\}$. Prove that $N(A)$ is an ideal of R which contains A.

   (c) The ideal $A = (a_0)$ is a maximal ideal of the Euclidean ring if and only if a_o is a prime element of R.

2. **The Euclidean Rings**

   (a) Let F be a field, and $F[x]$ the set of polynomials over F. Prove that $F[x]$ is an Eucledian ring

   (b) In an Euclidean ring (a, b) can be found using the following algorithm:

$$
\begin{aligned}
b &= q_0 a + r_1, \text{ where } d(r_1) < d(a) \\
a &= q_1 r_1 + r_2 \text{ where } d(r_2) < d(r_1) \\
r_1 &= q_2 r_2 + r_3 \text{ where } d(r_3) < d(r_2) \\
&\vdots \\
r_{n-1} &= q_n r_n
\end{aligned}
$$

And $(a, b) = r_n$. Prove the correctness of this algorithm.

(c) Find the gcd of the following polynomials over F, the field of rational numbers:

i. $x^3 - 6x^2 + x + 4$ and $x^5 - 6x + 1$

ii. $x^2 + 1$ and $x^6 + x^3 + x + 1$

3. **Vector Spaces**

(a) Let $T : U \to V$ be a vector space homomorphism with kernel K. Prove that K is a subspace of U.

(b) If S and T are subseta of a vector space V then prove that

i. $S \subset T$ implies $L(S) \subset L(T)$.

ii. $L(L(S)) = L(S)$

Where $L(S)$ denote the linear span of S.

(c) If V has a basis of n elements show that V is isomorphic to $F^{(n)}$

(d) Let F be a field, and $F[x]$ be polynomials over x. Prove that $F[x]$ is not finite dimensional over F.

4. **Fields**

(a) Show that $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$

(b) Give an explicit construction of a finite field $\mathbb{F}_{16}$ containing 16 elements.

(c) Let $\mathbb{F}_{16}^*$ be the set of units in $\mathbb{F}_{16}$. $\mathbb{F}_{16}^*$ is a cyclic group, find all generators of this group.