Algebra Homework 1

Due Monday, January 14

1 Let D be a domain.

a Show that every (nonzero) subring of D contains 1, the unity element of D.

Solution

Let $R \subseteq D$ be a (nonzero) subring with multiplicative identity u (which is necessarily nonzero). Then $uu = u1 = u$. Hence $u(u-1) = 0$, and since $u \neq 0$, we see that $u - 1 = 0$, i.e., $u = 1$.

b If D is finite, show that D is actually a field.

Solution

Let $d \in D$; we need to show that $d^{-1} \in D$. Define $f : D \longrightarrow D$ by $f(x) = dx$. Then f is an F-linear transformation. Since D is a domain, f is injective. Since $|D| < \infty$, f is also surjective. Thus, there is $x \in D$ such that $f(x) = 1$. In other words, there is $x \in D$ such that $dx = 1$. Thus, $x = d^{-1} \in D$.

c If F is a field with $F \subseteq D$ and $|D : F| < \infty$, show that D is a field.

Solution

Nearly the same! Let $d \in D$; we need to show that $d^{-1} \in D$. Define $f : D \longrightarrow D$ by $f(x) = dx$. Then f is an F-linear transformation. Since D is a domain, f is injective. Since $|D : F| < \infty$, f is also surjective. Thus, there is $x \in D$ such that $f(x) = 1$. In other words, there is $x \in D$ such that $dx = 1$. Thus, $x = d^{-1} \in D$.

2 Let D be a domain. Show that all the nonzero elements of D have equal additive orders, and that this common order is either ∞ or a prime number. This common order is called the **characteristic** of the domain D.

Solution

Let n be the additive order of 1. We will show that n is also the additive order of every nonzero element x of D. First notice that $nx = (n1)x = 0$, so the order of x is at most n. On the other hand, if $mx = 0$ then $(m1)x = 0$, and since $x \neq 0$ and D is a domain, it must be that $m1 = 0$, i.e., the order of 1 is at most the order of x. This proves that the additive order of x is n.

Now we have to show that n is either prime or infinite. If n is infinite, then we are done, so assume that $n < \infty$. If $n = pq$ with neither p nor q equal to 1 then p and q must be strictly less than n. Now $n1 = (p1)(q1)$ and so either $p1 = 0$ or $q1 = 0$. This means that either p or q is at least n, which is a contradiction.

3 A field of prime characteristic p is **perfect** if the map $F \to F$ given by $\alpha \mapsto \alpha^p$ is surjective.

a Show every finite field is perfect.

Solution

Recall that $(\alpha + \beta)^p = \alpha^p + \beta^p$ in a field of characteristic p, so the map $\phi(x) = x^p$ is a group homomorphism. Since F is a field, $\phi(x) = 0$ if and only if $x = 0$; in other words ϕ is injective. Since a map of finite sets is injective if and only if it is surjective, this means that F is perfect.

b Let F be an arbitrary field of finite characteristic $p \neq 0$. Show that the field of rational functions $F(X)$ is not perfect.

Solution

It is enough to find one element of $F(X)$ which is not a p^{th} power.
Claim X is not a p^{th} power.
Proof Say $X = (a(X)/b(X))^p$. Then $X \cdot b(X)^p = a(X)^p$. Since F is a field, the degree of the left hand side is $p \cdot \deg(b) + 1$ and the degree of the right side is $p \cdot \deg(a)$. Since one side is divisible by p and the other isn't, they can't be equal.