Math 581 Problem Set 1 Solutions

1. Find the splitting field of $f(x) = x^4 - 4x^2 - 5$ over $\mathbb{Q}$.

Observe that $f(x)$ factors as

$$f(x) = (x^2 - 5)(x^2 + 1).$$

It is then easy to see that the roots of $f(x)$ are given by $\pm\sqrt{5}$ and $\pm i$. Let K be the splitting field of $f(x)$.
Claim: $K = \mathbb{Q}(\sqrt{5}, i)$.
Proof: Observe that since K is by definition the smallest field that contains all the roots of $f(x)$ and $\mathbb{Q}(\sqrt{5}, i)$ contains all the roots of $f(x)$, we must have $K \subseteq \mathbb{Q}(\sqrt{5}, i)$. On the other hand, since K must contain all the roots of $f(x)$, it contains $\sqrt{5}$ and i and so must contain $\mathbb{Q}(\sqrt{5}, i)$. Thus we have equality as claimed.

2. Let X be a finite set and $f : X \to X$ a function. Prove that f is injective if and only if f is surjective.

Proof: Suppose f is injective. Then we assume that f is not surjective and find a contradiction. Let $x \in X$ be such that $f(y) \neq x$ for any $y \in X$. However, since each $x \in X$ must go to an element of X, we must have two elements in X mapping to the same element. (Note that it is important X be finite for this to work!) This contradicts the injectivity. Thus if f is injective, it must be surjective.
Now suppose that f is surjective but not injective. Let $x, y \in X$ so that $f(x) = f(y)$ but $x \neq y$. This means that there are not enough elements left to map to each element of X since we have essentially used two of them to map to one element. Thus f cannot be surjective. Both of these are examples of the pigeonhole principle. It states if you have N "pigeonholes" and $M > N$ pigeons, some pigeons must go into the same box. ■

3. Let B be a set of n elements. Prove that the number of different injective functions from B to B is $n!$. (Hint: induction may be helpful here!)

Proof: We proceed by induction on the number of elements of B. If $n = 1$ then there is only one possible function, sending the element to itself and so the claim is true. Now suppose that for some positive integer k we know that any set of k elements has precisely $k!$ injective functions to itself. Let B be a

set of $k+1$ elements, say $B = \{b_1, \ldots, b_k, b_{k+1}\}$. We split the injective functions into $k+1$ sets $\mathcal{A}_i$ where the functions in $\mathcal{A}_i$ are the injective functions that send b_1 to b_i. The functions in the set $\mathcal{A}_1$ send b_1 to b_1, so are determined by what the function does on the set of k elements $\{b_2, \ldots, b_{k+1}\}$. Thus, by our induction hypothesis there are $k!$ such functions. Similarly, each set $\mathcal{A}_i$ has $k!$ elements. Thus, when we count all the functions we have $k+1$ sets of $k!$ elements, so $(k+1)k! = (k+1)!$ different functions. Thus the result is true by induction. ■

4. Let $a, b, c \in \mathbb{Z}$. If $a|(b+c)$ and $\gcd(b,c) = 1$, prove that $\gcd(a,b) = 1 = \gcd(a,c)$.

Proof: Suppose that $\gcd(a,b) = d > 1$. Since $a|(b+c)$ we have that there exists an integer k so that $ak = b + c$. Since $d|a$ and $d|b$ this equation gives that $d|c$. But then $\gcd(b,c) > 1$, a contradiction. One proves that $\gcd(a,c) = 1$ in the same way. ■

5. If $5|(a^2 + b^2 + c^2)$, prove $5|a$ or $5|b$ or $5|c$.

Proof: Since we are talking about divisibility by 5, we work modulo 5. The fact that $5|(a^2 + b^2 + c^2)$ means that $a^2 + b^2 + c^2 \equiv 0 (\mathrm{mod}\, 5)$. Observe that the only possible squares modulo 5 are $0, 1$, and 4. If one of a^2, b^2, or c^2 is congruent to 0 modulo 5 then we have that 5 divides the square. Then one uses that if a prime divides the square of a number it must divide the number itself. Therefore we just need to show one of them is congruent to 0 modulo 5. To prove this, just consider all the possibilities of a^2, b^2, and c^2 being 1 or 4 and show that you can never add these up to get 0 modulo 5. ■

6. Let $a, n \in \mathbb{Z}$ with $n > 1$. Prove that $\gcd(a,n) = 1$ in $\mathbb{Z}$ if and only if the equation $\overline{a}x = \overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$ has a solution.

Proof: Suppose that $\gcd(a,n) = 1$. There exists $s, t \in \mathbb{Z}$ so that $1 = as + nt$. Considering this equation in $\mathbb{Z}/n\mathbb{Z}$ we see that $\overline{s}$ is a solution to the equation $\overline{a}x = \overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$.
Now suppose there is a solution $\overline{b}$ of the equation $\overline{a}x = \overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$. This is equivalent to the statement that $n|ab - 1$. Thus there exists a $t \in \mathbb{Z}$ so that $nt = ab - 1$, i.e., $1 = ab + n(-t)$. If $\gcd(a,n) = d > 1$, then $d|a$ and $d|n$ so $d|1$, a contradiction. Thus $\gcd(a,n) = 1$. ■

7. Define a new addition and multiplication on $\mathbb{Q}$ by

$$r \oplus s = r + s + 1$$

and

$$r \odot s = rs + r + s.$$

Prove that with these new operations $\mathbb{Q}$ is a commutative ring. Is it an integral domain? (Note, this has new operations so is NOT a subring of anything you know of, so you have to check ALL the properties of being a ring.)

Proof: We begin by noting that the set $\mathbb{Q}$ is clearly closed under each of these operations. Now one must check each property of being a ring.
Observe that -1 is the zero element for this ring: $r \oplus -1 = r + -1 + 1 = r$. It is easy to see that the addition is commutative. The associativity of addition is also clear. The additive inverse of an element r is given by $-2 - r$: $r \oplus (-2 - r) = r + -2 - r + 1 = -1$, which is the zero element of the ring.
The multiplicative identity is given by 0: $r \odot 0 = r \cdot 0 + r + 0 = r$. The fact that the multiplication is commutative is clear, as is the associativity. (You should be able to write down proofs though if asked!!!)
One needs to check the distributive properties as well. We check one here and omit the other as they are analogous. We need to show that $r \odot (s \oplus t) = r \odot s \oplus r \odot t$.

$$\begin{aligned} r \odot (s \oplus t) &= r \odot (s + t + 1) \\ &= r(s + t + 1) + r + (s + t + 1) \\ &= rs + rt + r + r + s + t + 1 \\ &= (rs + r + s) + (rt + r + t) + 1 \\ &= (r \odot s) \oplus (r \odot t). \end{aligned}$$

Thus we have shown this is a commutative ring. Now we need to determine if there are any zero divisors. Suppose r and s are zero divisors, i.e., they multiply together to give 0. In this ring that means that $r \odot s = -1$, i.e., $rs + r + s = -1$. Then manipulating this equation we must have:

$$\begin{aligned} r(s + 1) + s &= -1 \\ r(s + 1) &= -1 - s \\ r &= -1 \end{aligned}$$

i.e., r must already be zero. Thus there are no zero divisors. ■

8. Let $f(x), g(x), h(x) \in F[x]$, with $f(x)$ and $g(x)$ relatively prime. If $f(x)|h(x)$ and $g(x)|h(x)$, prove that $f(x)g(x)|h(x)$.

Proof: The fact that $f(x)|h(x)$ implies that there exists an $s(x)$ so that $h(x) = f(x)s(x)$ and similarly one has $t(x)$ so that $h(x) = g(x)t(x)$. Since $f(x)$ and $g(x)$ are assumed to be relatively prime, there exists $a(x)$ and $b(x)$ so that $1 = f(x)a(x) + g(x)b(x)$. Multiply both sides of this equation by $h(x)$. Then we have

$$\begin{aligned} h(x) &= f(x)a(x)h(x) + g(x)b(x)h(x) \\ &= f(x)a(x)g(x)t(x) + g(x)b(x)f(x)s(x) \\ &= f(x)g(x)[a(x)t(x) + b(x)s(x)]. \end{aligned}$$

Thus we have that $f(x)g(x)|h(x)$. ■

9. Show that $x - 1_F$ divides $a_n x^n + \cdots + a_1 x + a_0$ in $F[x]$ if and only if $a_0 + a_1 + \cdots + a_n = 0_F$.

Proof: Suppose that $x - 1_F$ divides $a_n x^n + \cdots + a_1 x + a_0$. Then we know that 1_F is a root of $a_n x^n + \cdots + a_1 x + a_0$, which means that $a_0 + a_1 + \cdots + a_n = 0_F$. Now suppose that $a_0 + a_1 + \cdots + a_n = 0_F$. Then we have that 1_F is a root of $a_n x^n + \cdots + a_1 x + a_0$ and so $x - 1_F$ divides $a_n x^n + \cdots + a_1 x + a_0$. ■