Final Examples

Exercise 1: Let R be an integral domain with field of fractions F. Suppose that $\varphi : R \to K$ is an injective homomorphism from R to a field K. Show that φ extends to an injective homomorphism $\Phi : F \to K$. When is φ not injective?

Proof. Suppose that φ is injective. Then define the homomorphism $\theta : F \to K$ as defined as

$$\theta(a, b) \mapsto \frac{\varphi(a)}{\varphi(b)}$$

We get that θ is injective because φ is injective. It follows that for $\frac{\varphi(a)}{\varphi(b)}$ to equal 0, we have that $\varphi(a) = 0$ and therefore, $a = 0$. Since $(0, b)$ is the zero element in F, we get that the $\ker\theta = \{0\}$. □

Exercise 2: Let R be a ring. Show that $R[x]$ is a PID iff R is a field.

Proof. $(\to)$ Supose that $R[x]$ is a PID. Then consider the ideal generated by x. We will show that this is a maximal ideal and therefore, $R[x]/(x) \cong R$ is a field. Suppose that (x, f) is an ideal. Since $R[x]$ is a PID, it must be generated by a single element. Furthermore, constants live in our ideal (x, f) so that element must divide constants and therefore be a constant. So

$$\begin{aligned}
(c) &= (x, f) \\
x &= cf\prime \\
\deg x &= \deg c + \deg f\prime \\
\deg f\prime &= 1 \\
x &= c(ax + b) \\
x &= cax + cb \\
x &= cax
\end{aligned}$$

so c is a unit and therefore, (x) is maximal. □

Exercise 3: If S is a set of primes, let $\mathbb{Z}_S$ be the set of all rational numbers m/n (in lowest terms) such that all prime factors of n are in S. If R is a subring of $\mathbb{Q}$ show that there is a set of primes S such that R is of the form $\mathbb{Z}_S$. What are the maximal subrings of $\mathbb{Q}$?

Proof. □

Exercise 4:

1. Consider $f(x, y) = x^3y + x^2y^2 + y^3 - y^2 - x - y + 1$ in $\mathbb{C}[x, y]$. Show that f is prime.

   Proof. We can rewrite the polynomial as an element in $\mathbb{C}[x][y]$:

   $$f(x, y) = y^3 + (x^2 - 1)y^2 + (x^3 - 1)y - (x - 1)$$

   by eisenstein, this polynomial is irreducible because $x - 1$ divides all coefficients besides the first one, the polynomial is primitve, and $(x - 1)^2$ does not divide the last coefficient.

We just need to check that $x-1$ is irreducible:

$$\begin{aligned} x-1 &= fg \\ \deg(x-1) &= \deg(f)+\deg(g) \\ 1 &= 0+1 \\ x-1 &= c(ax+b) \\ x-1 &= cax+cb \\ ca &= 1 \end{aligned}$$

therefore, $f=c$ is a unit and $x-1$ is irreducible. ☐

2. Let F be any field. Show that $f(x,y)=x^2+y^2-1$ is irreducible in $\mathbb{F}[x,y]$ unless $\mathbb{F}$ has characteristic 2. What happens in that case?

Proof. We can rewrite this equation as an element in $\mathbb{F}[x][y]$:

$$f(y)=y^2+x^2-1$$

and by eisenstein again, the polynomial $x-1$ is irreducible such that the polynomial $f(x,y)$ is irreducible. Now if $\mathbb{F}$ has characteristic 2, then we have

$$x^2+y^2-1=x^2+y^2+1$$

but

$$(x+y+1)^2=x^2+y^2+1+2(x+y+xy)=x^2+y^2+1$$

so this polynomial is not irreducible when $\mathbb{F}$ has characteristic 2. ☐

Exercise 5:

1. Show that if R is a PID, the gcd of $a,b\in R$ can be written as $ra+sb$ for some $r,s\in R$. Give an example of a UFD where this fails.

Proof. If R is a PID, then we have that if $a,b\in R$, then considering the ideal generated by a,b:

$$(a,b)=(s)$$

since the gcd of a,b divides both elements, we can let s be the gcd. This tells us that

$$s=r_1a+r_2b$$

which completes the proof. Now for an example of a UFD which does not satisfy the property, we can take $\mathbb{Z}[x]$ which is a UFD but not a PID since $(x,2)$ is not a principal ideal. We can find the gcd of two elements in $\mathbb{Z}[x]$ such as x^2+x+1 and x^2+1. Such elements are irreducible because these polynomials have all their roots in $\mathbb{C}$ so if we could factor any of them to get polynomials of lower degree, that would imply that the complex numbers are in $\mathbb{Z}$ which is impossible. Notice that the gcd of the polynomials is 1 but there is no way to write them as such:

$$\begin{aligned} r(x^2+x+1)+s(x^2+1) &= 1 \\ (r+s)x^2+rx+r+s &= 1 \end{aligned}$$

which does not work because the coefficient for x in the LHS is non-zero. ☐

2. Find the gcd of $11+7i$ and $18-i$ in $\mathbb{Z}[i]$.

Proof. We first take the norm of both numbers to find the prime factorization:

$$N(11+7i) = 121+49 = 170 = 17*5*2$$
$$N(18-i) = 324+1 = 325 = 5^2*13$$

Now we use the fact that integers $p \equiv 3 \pmod 4$ are prime and that the ones $p \equiv 1 \pmod 4$ and equal to 2 can be written as a sum of squares and therefore factorizable in $\mathbb{Z}[i]$:

$$N(11+7i) = (1 \pm 4i)(1 \pm 2i)(1 \pm i)N(13-i) = (1 \pm 2i)^2(2 \pm 3i)$$

so our only choice is that either $1+2i$, $1-2i$, $2+i$, or $2-i$ divides both elements or otherwise, their gcd is 1. We can check:

$$\frac{11+7i}{1+2i} = \frac{11+14-22i+7i}{5} = \frac{25-15i}{5} = 5-3i$$
$$\frac{13-i}{1+2i} = \frac{13-2+26i-i}{5} = \frac{11+25i}{5}$$

But this shows that $1+2i$ divides $11+7i$ but not $18-i$, so that one does not work. This tells us that $2-i$ does not work also because $1+2i$ divides this. So we are done, the gcd is 1. $\square$