Homework I Solutions

2) Show that if a prime ideal $\mathfrak{p} = I \cap J$ for ideals I and J, then $\mathfrak{p} = I$ or $\mathfrak{p} = J$.

▷ Assume that there exist an $x \in I \setminus (I \cap J)$ and a $y \in J \setminus (I \cap J)$. Then, we have

$$xy \in IJ \subset I \cap J = \mathfrak{p}$$

which is a contradiction as this implies x or y is in $\mathfrak{p} = I \cap J$ since $\mathfrak{p}$ is a prime ideal.

7) Let k be an infinite field, and $f \in k[X_1, \ldots, X_n]$. Show that $f = 0$ if and only if $f(x_1, \ldots, x_n) = 0$ for all $(x_1, \ldots, x_n) \in k^n$. Give a counter-example to the statement when $k = \mathbb{F}_2$ (finite field with 2 elements).

▷ Clearly, $f(X) = X^2 - X$ vanishes for all $X \in \mathbb{F}_2$ but $f \neq 0$. So, let's assume k is an infinite field.

If $f = 0$, it follows trivially that $f(x_1, \ldots, x_n) = 0$ for all $(x_1, \ldots, x_n) \in k^n$. Conversely, suppose $f(x_1, \ldots, x_n) = 0$ for all $(x_1, \ldots, x_n) \in k^n$. We want to show that $f = 0$. We argue by induction. The case $n = 1$ is elementary: a degree d polynomial in $k[X]$ can have at most d roots, since for every root a, we must have that $(X - a) \mid f(X)$. Since the filed k is infinite, it follows that if $f(x) = 0$ for all $x \in k$, then $f = 0$. Suppose now that the statement is true for $n - 1$. Given a polynomial $f \in k[X_1, \ldots, X_n]$, write it as $f(X_1, \ldots, X_n) = \sum_{i=1}^{s} f_i(X_1, \ldots, X_{n-1}) X_n^i$ for polynomials $f_i(X_1, \ldots, X_{n-1}) \in k[X_1, \ldots, X_{n-1}]$. Suppose that $f \neq 0$, then there exists an i such that $f_i \neq 0$. By induction hypothesis, there exists $(a_1, \ldots, a_{n-1}) \in k^{n-1}$ such that $f_i(a_1, \ldots, a_{n-1}) \neq 0$. Then, the polynomial $g(X) \in k[X]$ defined by $g(X) = f(a_1, \ldots, a_{n-1}, X)$ is a nonzero polynomial. So, it can only have finitely many zeros (by the $n = 1$ case). This contradicts the assumption that $f(x_1, \ldots, x_n) = 0$ for all $(x_1, \ldots, x_n)$.

8) Let $\mathfrak{p} \subset \mathbb{Z}[X]$ be a prime ideal. Suppose $\mathfrak{p} \neq \mathbb{Z}[X]$ or (0). Show that $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Thus, $\mathfrak{p} \cap \mathbb{Z} = (p)$ where $p = 0$ or p is a prime number.

(i) Suppose $\mathfrak{p} \cap \mathbb{Z} = (0)$, then $\mathfrak{p} = (f)$ where $f \in \mathbb{Z}[X]$ is an irreducible polynomial.

(ii) Suppose $\mathfrak{p} \cap \mathbb{Z} = (p)$ with p a prime number. Then, $\mathfrak{p} = (p, f)$ where $f = 0$ or $f \in \mathbb{Z}[X]$ is a monic polynomial (leading coefficient is one) and its mod p reduction $\overline{f} \in \mathbb{F}_p[X]$ is irreducible.

▷ We note that $\mathfrak{p} \cap \mathbb{Z}$ is the preimage of the prime ideal $\mathfrak{p}$ under the ring homomorphism $\mathbb{Z} \to \mathbb{Z}[X]$, hence is a prime ideal.

(i) Suppose $\mathfrak{p} \cap \mathbb{Z} = (0)$. Thus, $\mathfrak{p}$ consists of zero and polynomials with no constant terms. Let f be a non-zero polynomial in $\mathfrak{p}$ of minimal degree. We may assume f is primitive: Otherwise

$f = cf' \in \mathfrak{p}$ for some $c \in \mathbb{Z}$, but $c \notin \mathfrak{p}$, hence $f' \in \mathfrak{p}$. So, let us pick f to be primitive. It is also irreducible since otherwise, there would be a polynomial of smaller degree in $\mathfrak{p}$. We want to show that $\mathfrak{p} = (f)$. Consider another element $g \in \mathfrak{p}$, by viewing f and g as in $\mathbb{Q}[X]$, we can consider division with remainder

$$g = qf + r$$

for $q, r \in \mathbb{Q}[X]$ with $deg(r) < deg(f)$. Clearing the denominators by multiplying with an appropriate $c \in \mathbb{Q}$, we can write

$$cr = cqf - cg \in \mathbb{Z}[X]$$

But, since $f, g \in \mathfrak{p}$, this implies $cr \in \mathfrak{p}$ which contradicts to minimality of $deg(f)$ unless $r = 0$. Hence, we have

$$g = qf$$

since $f, g \in \mathbb{Z}[X]$, and f is primitive, it follows from Gauss lemma that $q \in \mathbb{Z}[X]$, hence $g \in (f) \subset \mathbb{Z}[X]$. Thus, we proved that $\mathfrak{p} = (f)$.

(ii) Let $\mathfrak{p} \cap \mathbb{Z} = (p)$. If $(p) = \mathfrak{p}$, then there is nothing to prove. Otherwise, we have $(p) \subsetneq \mathfrak{p} \subsetneq \mathbb{Z}[X]$. Now, let us observe that the reduction modulo p of coefficients induces a ring isomorphism

$$\mathbb{Z}[X]/(p) \cong \mathbb{F}_p[X]$$

Under this ring isomorphism the image of $\mathfrak{p}$ goes to a non-zero proper prime ideal $\overline{\mathfrak{p}}$. As $\mathbb{F}_p[X]$ is a PID, we have $\overline{\mathfrak{p}} = (\overline{f})$ for some irreducible polynomial $\overline{f} \in \mathbb{F}_p[X]$ which we can take to be monic (since $\mathbb{F}_p$ is a field). Let $f \in \mathfrak{p} \subset \mathbb{Z}[X]$ be an arbitrary lift of $\overline{f}$ which is monic. We claim that $\mathfrak{p} = (p, f)$. We have $(p, f) \subset \mathfrak{p}$. Next, we see that there is a ring isomorphism

$$\mathbb{Z}[X]/(p, f) \cong \mathbb{F}_p[X]/(\overline{f})$$

Indeed, as before the mod p reduction of coefficients $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ induces the ring map and if an element $g \in \mathbb{Z}[X]$ maps to $(\overline{f})$, we have $\overline{g} = \overline{fk}$ for some $k \in \mathbb{Z}$ but this means $g - fk \in (p)$. Now, $\mathbb{F}_p[X]/(\overline{f})$ is a field, hence so is $\mathbb{Z}[X]/(p, f)$. Therefore (p, f) is a maximal ideal, hence it must be that $(p, f) = \mathfrak{p}$.

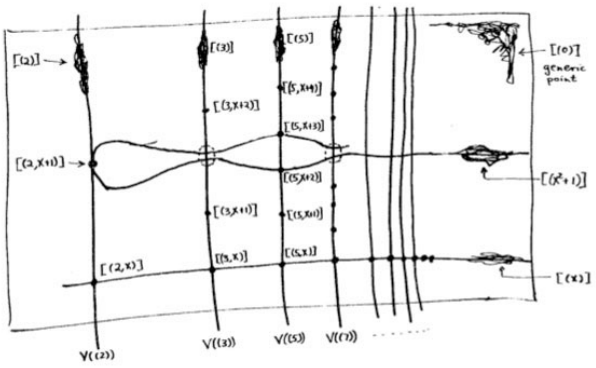

Figure 1: Mumford's picture of prime ideals in $\mathbb{Z}[X]$