Math 210B: Homework 2 Solutions

All rings are commutative with 1. Recall that if $A \subseteq B$ are rings and $\mathfrak{p}, \mathfrak{P}$ are prime ideals of A, B respectively we say $\mathfrak{P}$ *lies above* $\mathfrak{p}$ if $\mathfrak{P} \cap A = \mathfrak{p}$.

Problem 1. Let p be a prime, so $(p) = p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Determine the primes $\mathfrak{P}$ of the Gaussian integers $\mathbb{Z}[i]$ above (p). Thus determine the number of different $\mathfrak{P}$ and describe $\mathbb{Z}[i]/\mathfrak{P}$ for each $\mathfrak{P}$. Your answer should depend on p modulo 4.

Solution. If $\mathfrak{P}$ is a prime of $\mathbb{Z}[i]$ above (p) then $\mathfrak{P}$ is maximal by Lang Proposition VII.1.11, so $\mathbb{Z}[i]/\mathfrak{P}$ is a field containing $\mathbb{F}_p = \mathbb{Z}/(p)$. So may identify $\mathbb{Z}[i]/\mathfrak{P}$ with a subfield of $\overline{\mathbb{F}}_p$. Now the image of i in $\mathbb{Z}[i]/\mathfrak{P}$ is a root α of the polynomial $X^2 + 1$. This is a quadratic polynomial so either it factors in $\mathbb{F}_p$, in which case $\mathbb{Z}[i]/\mathfrak{P} \cong \mathbb{F}_p$, or it is irreducible, in which case $\mathbb{Z}[i]/\mathfrak{P} \cong \mathbb{F}_{p^2}$. Given α we may recover the prime ideal $\mathfrak{P}$ as the kernel of the ring homomorphism $\mathbb{Z}[i] \longrightarrow \overline{\mathbb{F}}_p$ such that $i \mapsto \alpha$.

Suppose $p \equiv 1 \bmod 4$. Then $\mathbb{F}_p^\times$ is a cyclic group of order a multiple of 4, so -1 is a square in $\mathbb{F}_p$. Let $\pm a$ be the two square roots of -1. Then there are homomorphisms $\mathbb{Z}[i] \longrightarrow \mathbb{F}_p$ such that $i \mapsto \pm a$, and the kernels of these homomorphisms are prime ideals above (p). Thus in this case there are two such prime ideals $\mathfrak{P}_1$ and $\mathfrak{P}_2$ and both satisfy $\mathbb{Z}[i]/\mathfrak{P}_i \cong \mathbb{F}_p$.

Next suppose $p \equiv 3 \bmod 4$. In this case $|\mathbb{F}_p^\times|$ is not a multiple of 4 and so -1 is not a square in $\mathbb{F}_p^\times$. But $|\mathbb{F}_{p^2}^\times| = p^2 - 1 \equiv 1 \bmod 4$, so there are two roots α and β of $x^2 + 1 = 0$ in $\mathbb{F}_{p^2}$. Thus there are homomorphisms $\phi, \phi' : \mathbb{Z}[i] \longrightarrow \mathbb{F}_{p^2}$ such that $\phi(i) = \alpha$ and $\phi'(i) = \beta$. However $\beta = \alpha^p$ and $\phi' = \sigma \circ \phi$ where $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ is the Frobenius automorphism, so ϕ and ϕ' have the same kernel $\mathfrak{P}$. In this case there is one prime ideal $\mathfrak{P}$ and $\mathbb{Z}[i]/\mathfrak{P} \cong \mathbb{F}_{p^2}$.

Finally if $p = 2$ there is one root (with multiplicity 2) of $x^2 + 1$ in $\mathbb{F}_2$; that root is 1. So there is a unique homomorphism $\mathbb{Z}[i] \longrightarrow \mathbb{F}_2$ such that $i \mapsto 1$. The kernel in this case is the principal ideal generated by $1 + i$, which is the unique principal ideal above (2).

Problem 2. Let $A = \mathbb{Q}[x, y]$ be the polynomial ring $\mathbb{Q}[X, Y]$ modulo the ideal generated by the polynomial $Y^2 - X^2(X + 1)$. This polynomial is irreducible since $X^2(X + 1)$ is not a square in $\mathbb{Q}[X]$, so A is an integral domain. If x, y are the images of X and Y then $y^2 = x^3 + x^2$. Let $\mathfrak{p}$ be the ideal generated by x and y. Let $t = y/x$ in the field of fractions of A.

(a) Show that $\mathfrak{p}$ is maximal and that it is the unique prime ideal of A above the ideal (x) of $\mathbb{Q}[x]$.

(b) Consider the rings $\mathbb{Q}[x] \subseteq \mathbb{Q}[x, y] \subseteq \mathbb{Q}[x, t]$, which are all subrings of the field of fractions of A. How many prime ideals of $\mathbb{Q}[x, t]$ lie above $\mathfrak{p}$?

(c) Show that the ring A is not integrally closed.

Solution. (a) The polynomial $Y^2 - X^2(X+1)$ is irreducible over $\mathbb{Q}[X]$ since it is Eisenstein with respect to the ideal $(X + 1)$. Hence it is irreducible as an element of $\mathbb{Q}[X, Y]$. It follows that $\mathbb{Q}[x, y] = \mathbb{Q}[X, Y]/(Y^2 - X^2(X + 1))$ is an integral domain.

The ideal $\mathfrak{p} = (x, y)$ of A is the kernel of the homomoorphism $\mathbb{Q}[x, y] \longrightarrow \mathbb{Q}$ such that $x \mapsto 0$ and $y \mapsto 0$. Thus $\mathbb{Q}[x, y]/\mathfrak{p}$ is a field and so $\mathfrak{p}$ is maximal.

We show that $\mathfrak{p}$ is the unique prime ideal of A above the prime ideal (x) of $\mathbb{Q}[x]$. If $\mathfrak{p}'$ is another such ideal, consider the ring $A/\mathfrak{p}'$. The images x' and y' in this ring satisfy $(y')^2 = (x')^2(x' + 1)$. But $x' = 0$ so $y' = 0$. Hence $\mathfrak{p}'$ contains y as well as x and so $\mathfrak{p} \subseteq \mathfrak{p}'$. But $\mathfrak{p}'$ is maximal, so $\mathfrak{p}' = \mathfrak{p}$.

(b) The subring $B = \mathbb{Q}[x, t]$ of the field K of fractions of $\mathbb{Q}[x, y]$ contains A because $y = tx$. Now t is the solution of the equation $t^2 = x + 1$ which is also Eisenstein over $\mathbb{Q}[x]$ with respect to the ideal $x+1$. The homomorphism $\mathbb{Q}[x] \longrightarrow \mathbb{Q}$ such that $x \mapsto 0$ has two extensions to B in which $t \mapsto 1$ and $t \mapsto -1$. The kernels of these homomorphisms are two distinct prime ideals of B above the ideal (x) of $\mathbb{Q}(x)$.

(c) It follows from (b) that $B \neq A$ and so $t \notin A$. But as a root of $t^2 = x + 1$ it is integral over $\mathbb{Q}[x]$, *a fortiori* over $\mathbb{Q}[x, y]$. Thus A is not integrally closed.

Let K be a field. Define $\mathbb{A}^n(K) = K^n$ to be the affine space. You may assume that K is infinite, so that $f(x) = f(x_1, \cdots, x_n)$ in the polynomial ring $K[X] = K[X_1, \cdots, X_n]$ is zero as a polynomial if and only if it is zero as a function on $\mathbb{A}^n(K)$. When we discuss the Nullstellensatz we will assume K is algebraically closed.

If $S \subseteq K[X]$ define

$$V(S) = \{x \in \mathbb{A}^n(K) | f(x) = 0 \text{ for } f \in S\}.$$

We call $V(S)$ an *algebraic set*. Clearly $V(S) = V(\mathfrak{a})$ where $\mathfrak{a}$ is the ideal generated by S, and indeed $V(S) = V(r(\mathfrak{a}))$ where

$$r(\mathfrak{a}) = \{f \in K[X] | f^n \in A \text{ for some } n > 0\}$$

is the radical of A.

Problem 3. Prove that $\mathbb{A}^n(K)$ has a topology in which the algebraic sets are the closed sets. (This is the *Zariski topology.*)

Solution. To show that the algebraic sets are the closed sets in a topology, we must show they are closed under arbitrary intersections and finite unions.

Let $X_i = V(\mathfrak{a}_i)$ be a family of algebraic sets indexed $i \in I$ where $\mathfrak{a}_i$ are ideals of $K[X]$. Then $x \in \mathbb{A}^n(K)$ lies in all X_i if and only if $f(x) = 0$ for all f in any $\mathfrak{a}_i$; that is, $f(x) = 0$ for all $f \in \sum \mathfrak{a}_i$. Thus

$$\bigcap_{i \in I} V(X_i) = V\left(\sum_i \mathfrak{a}_i\right).$$

Now to show that if $X = V(\mathfrak{a})$ and $Y = V(\mathfrak{b})$ are algebraic then so is $X \cup Y$, we will show that

$$X \cup Y = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}).$$

Note that if $\mathfrak{a} \subseteq \mathfrak{b}$ then $V(\mathfrak{a}) \supseteq V(\mathfrak{b})$. Thus $X \subseteq V(\mathfrak{a} \cap \mathfrak{b})$ and $Y \subseteq V(\mathfrak{a} \cap \mathfrak{b})$ and so $V(X \cup Y) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$. Now $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ and so $V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{a}\mathfrak{b})$. We claim that $V(\mathfrak{a}\mathfrak{b}) \subseteq X \cup Y$. If $x \notin X \cup Y$ then there is $f \in \mathfrak{a}$ such that $f(x) \neq 0$ and $g \in \mathfrak{b}$ such that $g(x) \neq 0$. Thus $fg \in \mathfrak{a}\mathfrak{b}$ and $(fg)(x) \neq 0$. We have proved that

$$X \cup Y \subseteq V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{a}\mathfrak{b}) \subseteq X \cup Y$$

so these sets are all equal, proving that $X \cup Y$ is an algebraic set.

The *Jacobson radical* $J(A)$ is the intersection of all maximal ideals of A. We encountered it in Nakayama's Lemma.

Problem 4. Prove that the Jacobson radical equals

$$\left\{a \in A | 1 + ab \in A^\times \text{ for all } b \in A\right\}.$$

Solution. If $a \in J(A)$ and $1+ab$ is not a unit, then $1+ab \in \mathfrak{P}$ for some maximal ideal. But $a \in \mathfrak{P}$ so $1 \in \mathfrak{P}$, contradiction. This proves that $J(A) \subseteq \{a \in A | 1+ab \in A^\times \text{ for all } b \in A\}$.

On the other hand, suppose that $1+ab$ is a unit for all b. To show that $a \in J(A)$ we must show that a lies in every maximal ideal $\mathfrak{P}$. If not, $\mathfrak{P} + aA = A$ so we may write $1 = \pi - ab$ for some $\pi \in \mathfrak{P}$ and $b \in B$, contradicting the assumption that $1+ab$ is a unit.

Problem 5. Let A be an integral domain, and Ω a field containing A. If Ω is integral over A prove that A is a field.

Solution. Let $0 \neq x \in A$. Our hypothesis implies that $1/x \in \Omega$ is integral over A so we may write

$$\left(\frac{1}{x}\right)^n + a_{n-1}\left(\frac{1}{x}\right)^{n-1} + \ldots + a_0 = 0, \qquad a_i \in A.$$

Then

$$\frac{1}{x} = -(a_{n-1} + a_{n-2}x + \cdots a_0 x^{n-1}) \in A$$

proving that A is a field.

Let $A \subseteq B$ be rings, B integral over A, and let S be a multiplicative subset of A. Then by Proposition VII.1.8, $S^{-1}B$ is integral over $S^{-1}A$. Now let $\mathfrak{P}$ be a prime ideal of B and $\mathfrak{p} = A \cap \mathfrak{P}$. Then there is a homomorphism $A_\mathfrak{p} \longrightarrow B_\mathfrak{P}$ and we might hope that $B_\mathfrak{P}$ is integral over $A_\mathfrak{p}$. The following problem shows that this may not be true.

Problem 6. Let k be a field of characteristic $\neq 2$. Let $A = k[x^2-1]$ and $B = k[x]$. Show that B is integral over A. Let $\mathfrak{P} = (x-1)B$ and $\mathfrak{p} = A \cap \mathfrak{P}$. Prove that $1/(x+1) \in B_\mathfrak{P}$ is not integral over $A_\mathfrak{p}$.

Solution. Let $\mathfrak{P}' = (x+1)B$. We will show that $\mathfrak{P}' \cap A = \mathfrak{P} \cap A = \mathfrak{p}$. Indeed, an element of A is a polynomial $f(x^2-1)$ where $f \in k[X]$. Write

$$f(X) = a_k X^k + \cdots + a_0.$$

Clearly $f(x^2-1)$ is divisible by $x-1$ in $B = k[x]$ if and only if $a_0 = 0$, in which case it is divisible by $x+1$ also, so indeed $\mathfrak{P}$ and $\mathfrak{P}'$ have the same intersection with A.

Since $B = k[x]$ is an integral domain, we may identify $B_\mathfrak{P}$ and $B_{\mathfrak{P}'}$ with subrings of its field of fractions $k(x)$, and with this identification $A_\mathfrak{p}$ is a subring of both.

Note that $x+1 \notin \mathfrak{P}$. Indeed $\mathfrak{P}$ is the kernel of the homomorphism $B \longrightarrow k$ that sends x to 1, and $x+1$ is not in this kernel. Thus $1/(x+1) \in B_{\mathfrak{P}}$.

Now suppose that $1/1+x$ is integral over $A_{\mathfrak{p}}$. This means that we have a relation

$$\left(\frac{1}{x+1}\right)^n + a_{n-1}\left(\frac{1}{x+1}\right)^{n-1} + \ldots + a_0 = 0, \qquad a_i \in A_{\mathfrak{p}}.$$

Thus

$$1 = -a_{n-1}(x+1) - \ldots - a_0(x+1)^n.$$

Since $a_i \notin \mathfrak{p}$, we have $a_i \notin \mathfrak{P}'$, so the right hand side is an element of $\mathfrak{P}'B_{\mathfrak{P}'}$ which is a proper ideal of $B_{\mathfrak{P}'}$. This is a contradiction.