MAT4200 Fall 2016
Mandatory Assignment

Ivar Haugaløkken Stangeby

Due: Thursday, November 3, 2:00 PM

Problem 1

Recall that an element e in a ring A is called *idempotent* if it satisfies $e^2 = e$.

(i) We wish to characterize the idempotents in the ring $\mathbb{Z}/(p^k)$ given a prime p and a positive integer k. Note that any prime ideal in the ring $\mathbb{Z}/(p^k)$ is in one to one correspondence with prime ideals in $\mathbb{Z}$ containing (p^k). There is only one maximal ideal in $\mathbb{Z}$ containing (p^k), and that is (p). Hence, $\mathbb{Z}/(p^k)$ is a local ring. Consequently, the only idempotent elements in $\mathbb{Z}/(p^k)$ is 0 and 1. This amounts to all elements $n \in \mathbb{Z}$ such that $n \equiv 0 \pmod{p^k}$ or $n \equiv 1 \pmod{p^k}$.

(ii) We can find the idempotents in $\mathbb{Z}/(12)$ by inspection. Since $\mathbb{Z}/(12) \simeq \mathbb{Z}_{12}$ the idempotent elements are $0, 1, 4$, and 9. The recurring pattern seems to be, since $12 = 2^2 \cdot 3$, the idempotent elements are precisely those elements in $n \in \mathbb{Z}$ satisfying $n \equiv 0, 1 \pmod{2^2}$ *and* $n \equiv 0, 1 \pmod{3}$.

(iii) We wish to find the number of idempotent elements in $\mathbb{Z}/(n)$ where $n = \prod_{i=1}^{N} p_i^{n_i}$, $n_i \geq 1$ and the p_i are distinct prime numbers. Based on the observation from (ii) we conjecture that the idempotent elements in the ring $\mathbb{Z}/(n)$ are precisely those elements $m \in \mathbb{Z}$ satisfying $m \equiv 0, 1 \pmod{p_i^{n_i}}$ for $i = 1, \ldots, N$.

The *Chinese Remainder Theorem* tells us that if we have a set of pairwise coprime ideals, then

$$\mathbb{Z}/(\cap_{i=1}^{N}(p_i^{n_i})) \simeq \prod_{i=1}^{N} \mathbb{Z}/(p_i^{n_i}).$$

Note however that the expression on the left involves an intersection of ideals, and not the product of ideals we have given. This can remedied by the fact that since the ideals are pairwise coprime, we have $\bigcap_{i=1}^{N}(p_i^{n_i}) = \prod_{i=1}^{N}(p_i^{n_i})$. For an element $(x_1, x_2, \ldots, x_N)$ to be idempotent in the expression on the right we need each x_i idempotent in the

corresponding ring. There are two choices of idempotent element for each x_i, and there are N choices to be made, so we have 2^N idempotent elements in total. Hence, following the isomorphisms, we can conclude that $\mathbb{Z}/(n)$ contains 2^N idempotent elements.

Problem 2

We let A be a ring, $\mathfrak{a}$, $\mathfrak{b}$ ideals in A, and $\mathfrak{p}$ a prime ideal. We wish to show that the following statements are equivalent:

(1) $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$;

(2) $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{b}$;

(3) $\mathfrak{ab} \subseteq \mathfrak{p}$.

Proof.

(1) $\implies$ (2):
Let $x \in \mathfrak{a} \cap \mathfrak{b}$. Then x is an element of both $\mathfrak{a}$ and $\mathfrak{b}$. If $\mathfrak{a} \subseteq \mathfrak{p}$, then $x \in \mathfrak{p}$. Similarly, if $\mathfrak{b} \subseteq \mathfrak{p}$, then $x \in \mathfrak{p}$. In an case, $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$.

(2) $\implies$ (3):
Assume that $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$. Let $x \in \mathfrak{ab}$. We wish to show that $x \in \mathfrak{p}$. By definition of $\mathfrak{ab}$ we know that $x = \sum a_i b_i$ where each $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. Note that each term $a_i b_i$ is in both $\mathfrak{a}$ and $\mathfrak{b}$ as these are ideals. So by assumption, $a_i b_i \in \mathfrak{p}$. Since we have a sum of elements in $\mathfrak{p}$, it must also lie in $\mathfrak{p}$. Hence $x \in \mathfrak{p}$.

(3) $\implies$ (1):
We prove this contrapositively. Assume that $\mathfrak{a} \not\subseteq \mathfrak{p}$, $\mathfrak{b} \not\subseteq \mathfrak{p}$ and choose $x \in \mathfrak{a} \setminus \mathfrak{p}$, $y \in \mathfrak{b} \setminus \mathfrak{p}$. Since $\mathfrak{p}$ is prime we can use the fact that $x, y \notin \mathfrak{p} \implies xy \notin \mathfrak{p}$. Now, xy is an element in $\mathfrak{ab}$, but $xy \notin \mathfrak{p}$, hence $\mathfrak{ab} \not\subseteq \mathfrak{p}$. We have now shown contrapositively that (3) $\implies$ (1).

□

Problem 3

For this problem we assume that A is a ring, B an algebra with the structure map $f\colon A \to B$[1]. Furthermore, we assume B to be flat as an A-module. We recall that B is *faithfully flat* if for every A-module M, the map $M \to M \otimes_A B$ given by $x \mapsto x \otimes 1$ is injective. We wish to show that the following statements are equivalent:

(1) B is faithfully flat;

[1] I made a slight change in names, calling A' for B instead. Due to simplicity.

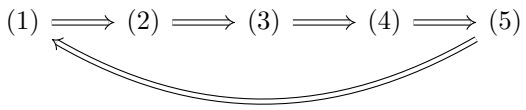
(2) every ideal of A is the contraction of its extension, i.e., $f^{-1}(\mathfrak{a}B) = \mathfrak{a}$ for every ideal $\mathfrak{a} \subseteq A$;

(3) every prime ideal of A is the contraction of a prime ideal of B;

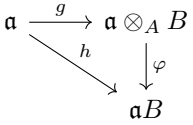
(4) for every maximal ideal $\mathfrak{m} \subset A$, the ideal $\mathfrak{m}B$ is different from B;

(5) for any nonzero A-module M, the module $M \otimes_A B$ is nonzero.

Proof. The plan for the proof is as follows:



(1) $\implies$ (2):
We assume B to be faithfully flat. Let $g\colon \mathfrak{a} \to \mathfrak{a} \otimes_A B$ be the map defined by $x \mapsto x \otimes 1$. By assumption, since B is faithfully flat, g is injective. We also have an isomorphism $\varphi\colon \mathfrak{a} \otimes B \to \mathfrak{a}B$ given by $a \otimes b \mapsto ab$. Note that the multiplication takes place in B, so by definition, we have $ab \coloneqq f(a)b$ as the only sensible thing to do. We are interested in the function $h \coloneqq \varphi \circ g$ taking elements in $\mathfrak{a}$ to elements in $\mathfrak{a}B$ as the following diagram illustrates:



Taking $a \in \mathfrak{a}$ we see that $h(a) = \varphi(g(a)) = \varphi(a \otimes 1) = f(a)$. So f factors through φ and g. We can therefore consider the contraction of $\mathfrak{a}B$ as passing through g and φ. Consider now $f^{-1}(\mathfrak{a}B) = g^{-1} \circ \varphi^{-1}(\mathfrak{a}B)$. Now, φ is an isomorphism so this equals $g^{-1}(\mathfrak{a} \otimes_A B)$ and g is injective, so we get $f^{-1}(\mathfrak{a}B) = \mathfrak{a}$.

(2) $\implies$ (3):
Assume that $f^{-1}(\mathfrak{a}B) = \mathfrak{a}$ for every ideal $\mathfrak{a}$ in A. Let $\mathfrak{p}$ be a prime ideal in A. By assumption, we know that $\mathfrak{p} = f^{-1}(\mathfrak{p}B)$. By Proposition 3.16, $\mathfrak{p}$ is the contraction of a prime ideal of B if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$.

(3) $\implies$ (4):
Assume that every prime ideal of A is the contraction of a prime ideal of B. Let $\mathfrak{m}$ be a maximal ideal of A. So, we have $\mathfrak{m} = \mathfrak{q}^c$ for some prime ideal $\mathfrak{q}$ in B. We need to show that $\mathfrak{m}^e \neq B$. Extending, we see that $\mathfrak{m}^e = \mathfrak{q}^{ce}$ but $\mathfrak{q}^{ce} \subseteq \mathfrak{q}$. Since $\mathfrak{q}$ is prime, it is properly contained in B, hence $\mathfrak{m}^e$ is properly contained in B. This proves the claim.

(4) $\implies$ (5):
Assume that for every maximal ideal $\mathfrak{m}$ we have $\mathfrak{m}B \neq B$. Assume that $M \neq 0$. We wish to show that $M \otimes_A B \neq 0$. We do this by constructing a non-zero submodule of $M \otimes_A B$. Since $M \neq 0$ we chose $x \neq 0$ as an element in M. We know that the annihilator $\mathfrak{a} \coloneqq \mathrm{Ann}(x)$ has to be a proper ideal of A, as $1 \notin \mathfrak{a}$. The map $\varphi\colon A \to M$ given by $a \mapsto ax$ have precisely $\mathfrak{a}$ as its kernel. This induces an injection from $(A/\mathfrak{a})$ to M. By flatness of B, we can tensor and preserve injectiveness as the following diagram illustrates:

$$\begin{array}{ccc} (A/\mathfrak{a}) \otimes_A B & \hookrightarrow & M \otimes_A B \\ \downarrow \simeq & \nearrow & \\ B/\mathfrak{a}B & & \end{array}$$

Since $\mathfrak{a}$ is an ideal of A and contained in a maximal ideal $\mathfrak{m}$, we have that $\mathfrak{a}B \subseteq \mathfrak{m}B \subset B$, hence $B/\mathfrak{a}B \neq 0$, which tells us that $M \otimes_A B \neq 0$.

(5) $\implies$ (1):
Assume the contrapositive of the hypothesis, namely that $M \otimes_A B = 0 \implies M = 0$. Fix the A-module M and let $g : M \to M \otimes B$ given by $x \mapsto x \otimes 1$ be the canonical map. We need to show that $\mathrm{Ker}(g) = 0$. Since g is an A-module homomorphism, $\mathrm{Ker}(g)$ is an A module. We tensor it with B to to obtain $\mathrm{Ker}(g) \otimes_A B$. Let $x \otimes b$ be an element. Since $M \otimes_A B$ is naturally a B-module we can write this as $b(x \otimes 1)$, but our x lies in $\mathrm{Ker}(g)$ so, $x \otimes 1 = 0$. Consequently, $\mathrm{Ker}(g) \otimes_A B = 0$. By our assumption, we must have $\mathrm{Ker}(g) = 0$, so g is injective. Since M was arbitrary, B must be faithfully flat.

□

Problem 4

Let k be a field, and let $A \coloneqq k[x, y, z]$ be the polynomial ring in three variables. Set $\mathfrak{a} \coloneqq (xy, x - yz)$, $\mathfrak{q}_1 \coloneqq (x, z)$, and $\mathfrak{q}_2 \coloneqq (y^2, x - yz)$. We wish to show that $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ and that this is a minimal primary decomposition of $\mathfrak{a}$.

Proof. We start by showing the inclusion $\mathfrak{q}_1 \cap \mathfrak{q}_2 \subseteq \mathfrak{a}$. Let $f \in \mathfrak{q}_1 \cap \mathfrak{q}_2$. We can then write $f = ax + az = cy^2 + d(x - yz)$ for $a, b, c, d \in A$. Rearranging we see that $x(a - d) = cy^2 - bz - dyz$. From this equality we can conclude that $x | cy^2 - bz - dyz$. In particular, x divides c, so $c = c'x$ for some $c' \in A$. Substituting, we can write $f = c'xy^2 + d(x - yz)$ which is a linear combination of the generators of $\mathfrak{a}$. We can therefore conclude that $f \in \mathfrak{a}$.

Conversely, to show $\mathfrak{a} \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2$ we can consider the generators of $\mathfrak{a}$. If we can show that they lie in the intersection, then so must any linear combination of the two. Consider first the generator xy of $\mathfrak{a}$. We see immediately that $xy \in \mathfrak{q}_1$.

Similarly, the generator $x - yz$ is a linear combination of x and z, hence lies in $\mathfrak{q}_1$. Since it also lies in $\mathfrak{q}_2$ as a generator, it remains to show that xy lies in $\mathfrak{q}_2$. In other words, we need to write $xy = ay^2 + b(x - yz)$ for some $a, b \in A$. Taking $a = z$ and $b = y$ we get $zy^2 + yx - y^2z$ which equals xy. Hence $xy \in \mathfrak{q}_2$. Since both generators of $\mathfrak{a}$ lie in $\mathfrak{q}_1 \cap \mathfrak{q}_2$ we can conclude that $\mathfrak{a} \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2$.

We now show that both $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are primary ideals. Consider the quotient $A/\mathfrak{q}_1$. This is isomorphic to $k[y]$, and since k is a field, this is an integral domain. Hence $k[y]$ contains no zero divisors, so vacuously, all zero divisors are nilpotent. Hence $\mathfrak{q}_1$ is primary. Equivalently, note that modding out by $\mathfrak{q}_1$ yields an integral domain, hence $\mathfrak{q}_1$ is prime and any prime ideal is primary.

Consider now the quotient $A/\mathfrak{q}_2$. Let $\bar{x}, \bar{y}$ and $\bar{z}$ denote the equivalence classes. Modding A out by $(x - yz)$ yields $k[\bar{y}\bar{z}, \bar{y}, \bar{z}]$. This ring is equal to $k[\bar{y}, \bar{z}]$. Modding out by (y^2) yields $A/\mathfrak{q}_2 = k[\bar{y}, \bar{z}]/(y^2)$. It remains to show that all zero-divisors here are nilpotent elements. The only way for two non-zero elements $f, g \in A/\mathfrak{q}_2$ to multiply to 0 is if y divides both f and g. In other words, both f and g are nilpotent, hence $\mathfrak{q}_2$ is a primary ideal.

Furthermore, we have that $y^2 \in \mathfrak{q}_1$ but $y^2 \notin \mathfrak{q}_1$ and $z \in \mathfrak{q}_1$ but $z \notin \mathfrak{q}_2$. The radicals are distinct, as

$$\sqrt{(x, z)} = (x, z) \text{ and } \sqrt{(y^2, x - yz)} = (y, x - yz),$$

hence $\mathfrak{q}_1 \cap \mathfrak{q}_2$ is a minimal primary decomposition of $\mathfrak{a}$. □

Problem 5

We let k be a field, and X, Y, Z variables. We set

$$A \coloneqq k[X, Y, Z]/(X^2 - Y^3 - 1, XZ - 1),$$

and let $x, y, z \in A$ be the classes of X, Y, Z in A. Fixing $a, b \in k$ we set $t \coloneqq x + ay + bz$ and $B \coloneqq k[t] \subseteq A$. We wish to show that x and y are integral over B for any a, b, and that z is integral over B if and only if $b \neq 0$.

Note first, that in the quotient A, we have that $xz = 1$ and that $y^3 = x^2 - 1$. Our goal is to manipulate the expression for t in such a way that we get rid of y and z and end up with an integral dependence relation for x over B. Multiplying the equation for t by x yields $tx = x^2 + ayx + b$ where the z is gone. Rearrange to get $x^2 + tx + b = ayx$. We now need to get rid of y, and we do this by cubing both sides. This gives us

$$(x^2 - tx + b)^3 + a^3x^3(x^2 - 1) = 0$$

which we recognize as an integral dependence relation for x over B. Note that all coefficients are in B, namely a, b and t. If we now can show that y is integral over $B[x]$, then it follows by transitivity that y is integral over B. Since $y^3 = x^2 - 1$, we can rearrange to get an integral dependence relation for y over $B[x]$, namely $y^3 - x^2 + 1 = 0$. So, y is integral over $B[x]$, and therefore also integral over B.

To show that z is integral over B if and only if $b \neq 0$, we first assume that $b \neq 0$. We then get the integral dependence relation for z over $B[x, y]$, namely $z + (ay + x - t)/b = 0$. By transitivity, z is integral over B. Conversely, to show that z integral over B implies $b \neq 0$, we assume for contradiction that z is integral over B and that $b = 0$. The contradiction we want relies on the fact that $k[x]$ is integrally closed in its field of fractions $k(x)$. We wish to show that z is an element of $k[x]$ by showing that z is integral over $k[x]$. Note first that $z \in k(x)$ as $z = 1/x$.

With a arbitrary and $b = 0$, t reduces to $x+ay$, hence our ring B is contained in the ring $k[x, y]$. Under the assumption that z is integral over B, it must also be integral over $k[x, y]$ using the same dependence relation. Furthermore, y is integral over $k[x]$ as $y^3 - x^2 + 1 = 0$. Consequently, z is integral over $k[x]$. But, now, since $z \in k(x)$ and z integral over $k[x]$, we must have $z \in k[x]$. This means that $1/x \in k[x]$, which is the contradiction we wanted. Hence z is integral over B if and only if $b \neq 0$.