Homework 3 Solutions MATH 431, Spring 2015

Sec 27 (6). Find all $c \in \mathbb{Z}/3\mathbb{Z}$ such that $\mathbb{Z}/3\mathbb{Z}/\left\langle x^3+x^2+c\right\rangle$ is a field.

Solution: Let $f(x) = x^3 + x^2 + c$. Since $\mathbb{Z}/3\mathbb{Z}$ is a commutative ring with unity (in fact, a field) then this factor ring is a field if and only if $\langle f(x)\rangle$ is a maximal ideal (Thm 13), and $\langle f(x)\rangle$ is a maximal ideal if and only if $f(x)$ is irreducible over $\mathbb{Z}/3\mathbb{Z}$ (Thm 22). Then we are looking for the values of c such that $f(x)$ is irreducible, or (since it has degree 3) values of c so that $f(x)$ has no roots in $\mathbb{Z}/3\mathbb{Z}$. There are only three options:

(a) $c = 0 \Rightarrow f(x) = x^3 + x^2$, which is definitely not irreducible.

(b) $c = 1 \Rightarrow f(x) = x^3 + x^2 + 1$. Notice that $f(1) = 1^3 + 1^2 + 1 = 3 \equiv 0 \bmod 3$ so this is not irreducible.

(c) $c = 2 \Rightarrow f(x) = x^3 + x^2 + 2$. $f(0) = 2$, $f(1) = 1$, and $f(2) = 2$ so $f(x)$ is irreducible when $c = 2$.

Then $\mathbb{Z}/3\mathbb{Z}/\langle f(x)\rangle$ is a field if and only if $c = 2$.

Sec 27 (14). Mark each of the following statements as True or False. If the statement is False, explain why or give a counterexample.

(a) Every prime ideal of every commutative ring with unity is a maximal ideal. **False.** $\langle x\rangle$ is a prime ideal in $\mathbb{Z}[x]$ but is not maximal because it is properly contained in $\langle x, 2\rangle$ (among others).

(b) Every maximal ideal of every commutative ring with unity is a prime ideal. **True.** (Cor 16 of Part 3 notes.)

(c) $\mathbb{Q}$ is its own prime subfield. **True.**

(d) The prime subfield of $\mathbb{C}$ is $\mathbb{R}$. **False.** The prime subfield of $\mathbb{C}$ is $\mathbb{Q}$.

(e) Every field contains a subfield isomorphic to a prime field. **True.**

(f) A ring with zero divisors may contain one of the prime fields as a subring. **True.** For example, $\mathbb{Z}/6\mathbb{Z}$ contains subrings isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.

(g) Every field of characteristic zero contains a subfield isomorphic to $\mathbb{Q}$. **True.**

(h) Let F be a field. Since $F[x]$ has no zero divisors, every ideal of $F[x]$ is a prime ideal. **False.** The ideal $\left\langle x^2-1\right\rangle$ in $\mathbb{Q}[x]$ is not prime because $(x-1)(x+1) = x^2 - 1 \in \left\langle x^2-1\right\rangle$ but neither $x - 1$ nor $x + 1$ are in $\left\langle x^2-1\right\rangle$.

(i) Let F be a field. Every ideal of $F[x]$ is a principal ideal. **True.** Note that this means that $\left\langle x^2+1, x+7\right\rangle$ can be reduced to a single generator in $\mathbb{Q}[x]$!

(j) Let F be a field. Every principal ideal of $F[x]$ is a maximal ideal. **False.** $\langle f(x)\rangle$ in $F[x]$ is only maximal if $f(x)$ is irreducible over $f(x)$. For example, $\left\langle x^2\right\rangle$ is a principal ideal but is not maximal since $\left\langle x^2\right\rangle \subsetneq \langle x\rangle$.

Sec 27 (16). Find a prime ideal of $\mathbb{Z} \times \mathbb{Z}$ that is not maximal.

Solution: One example would be $\{0\} \times \mathbb{Z}$. A whole family of examples would be $\{0\} \times p\mathbb{Z}$ for any prime p. You can show these are prime since each component is a prime ideal. They are not maximal since you could instead pick $3\mathbb{Z}$ for the first component (for example).

Sec 27 (17). Find a nontrivial proper ideal of $\mathbb{Z} \times \mathbb{Z}$ that is not prime.

Solution: Something like $4\mathbb{Z} \times \mathbb{Z}$ would be a great example. It is not prime since $(2, 9) \cdot (2, -5) = (4, -45) \in 4\mathbb{Z} \times \mathbb{Z}$ but neither $(2, 9)$ nor $(2, -5)$ is in $4\mathbb{Z} \times \mathbb{Z}$.

Sec 27 (29). Show that N is a maximal ideal in a ring R if and only if R/N is a simple ring (that is a nontrivial ring that has no proper nontrivial ideals).

Proof : We looked at this one in class. The quick outline is to use the Fundamental Homomorphism Theorem to state that there exists a homomorphism $\phi : R \to R'$ such that $\ker \phi = N$ so that $R/N \cong \phi[R]$. Then consider the ideals I of R and their images $\phi[I]$:

- If $I \subseteq N$, then $\phi[I] = \{\phi(x) \mid x \in I \subseteq \ker \phi\} = \{0\}$, the trivial ideal of $\phi[R] \cong R/N$.
- If $N \subsetneq I \subsetneq R$, then $\phi[I]$ will contain nonzero elements of $\phi[R]$, and since $I \neq R$ $\phi[I]$ will be a proper subset of $\phi[R] \cong R/N$. We know that $\phi[I]$ is an ideal of $\phi[R]$ (Thm 7 (6)), so then $\phi[R] \cong R/N$ contains a proper nontrivial ideal $\phi[I]$.

Then R/N has no proper nontrivial ideals (is simple) if and only if N is a maximal ideal in R.

Sec 27 (31). Let F be a field and $f(x), g(x) \in F[x]$. Show that $f(x)$ divides $g(x)$ if and only if $g(x) \in \langle f(x) \rangle$.

Proof : $g(x) \in \langle f(x) \rangle \iff g(x) = f(x)h(x)$ for some $h(x) \in F[x] \iff f(x)$ divides $g(x)$.

Sec 27 (37). Show that for a field F, the set S of all matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right)$ for $a, b \in F$ is a **right ideal** but not a **left ideal** of $M_2(F)$.

Proof : First notice that S meets the first two conditions of Thm 2 of the Part 3 notes: It contains the zero matrix so is nonempty and is closed under subtraction.

Let $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in M_2(F)$. Then

$$\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} ax & bx \\ az & bz \end{smallmatrix}\right) \notin S \text{ but } \left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} ax+bz & ay+bw \\ 0 & 0 \end{smallmatrix}\right) \in S$$

so multiplication on the RIGHT by an element of the ring gives another element of the subring S but multiplication on the LEFT by an element of $M_2(F)$ does NOT give another element of S. Thus, S is a RIGHT ideal but NOT a LEFT ideal.

HW3 (A). Answer the following questions, explaining briefly or giving a counterexample.

(a) Find all prime and maximal ideals in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Which of these ideals principal?

(b) Is $M_2(2\mathbb{Z})$ maximal in $M_2(\mathbb{Z})$? Is it prime? Is it principal?

(c) In $\mathbb{Q}[x]$, is $\langle x^2+2\rangle$ maximal? Is it prime?

(d) In $\mathbb{Q}[x]$, is $\langle x^2\rangle$ maximal? Is it prime?

Solution:

(a) The proper nontrivial ideals of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ are

$$(a)\,\{0\} \times \mathbb{Z}/4\mathbb{Z} \qquad (b)\,\{0\} \times \{0,2\} \qquad (c)\mathbb{Z}/2\mathbb{Z} \times \{0\} \qquad (d)\mathbb{Z}/2\mathbb{Z} \times \{0,2\}$$

Of these, (a) and (d) are maximal. Also, all of these are prime. They are also all principal, with the following generators:

$$(a)\,\{0\} \times \mathbb{Z}/4\mathbb{Z} = \langle(0,1)\rangle \qquad (b)\,\{0\} \times \{0,2\} = \langle(0,2)\rangle \qquad (c)\mathbb{Z}/2\mathbb{Z} \times \{0\} = \langle(1,0)\rangle \qquad (d)\mathbb{Z}/2\mathbb{Z} \times \{0,2\} = \langle(1,$$

(b) It is maximal (and thus prime), and the argument is something like "there's no space" between this ideal and the ring for any other ideals since we're already using a maximal ideal for the entries of our matrices. It is not principal, though. (This might be hard to prove, but it's easy to believe that the ring of matrices can't be generated as multiples of a single element!)

(c) It is maximal (and thus prime) since x^2+2 is irreducible over $\mathbb{Q}$ (Thm 22).

(d) It is not maximal since $\langle x^2\rangle \subsetneq \langle x\rangle$. It is not prime since $x \cdot x \in \langle x^2\rangle$ but $x \notin \langle x^2\rangle$.

HW3 (B). Let F be a field and define $I = \{f(x,y) \in F[x,y] \mid f \text{ has a zero constant term}\}$. I is an ideal in $F[x,y]$; show that it is **not** a principal ideal.

Solution: Hopefully it is clear that the ideal $I = \langle x,y\rangle = \{xf(x,y) + yg(x,y) \mid f,g \in F[x,y]\}$. To show that this cannot be represented as a principal ideal with a single generator, we would have to use a proof by contradiction. Instead, let's just convince ourselves that there's no reasonable generator for this ideal. If we just use $\langle x\rangle$, we get polynomials with no constant term but there's no way to get the polynomial $y \in I$ as a multiple of x (so $\langle x\rangle \subsetneq I$). So we have to use both x and y in a generator. Try $\langle xy\rangle$ and $\langle x+y\rangle$; in the both cases, we can't get the polynomials x or y as multiples of these generators, so we once again don't have enough elements to be all of I. We could get fancier with picking a generator, but it should be clear there's no way to get what we need this way, so we really do need both generators. Thus, I is NOT a principal ideal.

HW3 (C).

(a) Let R be a commutative ring with unity. Prove that $\langle f(x)\rangle$ is a prime ideal in $R[x]$ if and only if $f(x)$ is irreducible in $R[x]$.

(b) Let F be a field. Prove that any prime ideal in $F[x]$ is also a maximal ideal.

Proof :

(a) Let's prove this by instead proving the contrapositive: Prove that $\langle f(x)\rangle$ is NOT a prime ideal in $R[x]$ if and only if $f(x)$ is NOT irreducible in $R[x]$.

Suppose $g(x) \in \langle f(x)\rangle$; then $g(x) = (f(x))^k h(x)$ for some $h(x) \in R[x]$ where $k \in \mathbb{Z}^+$ is chosen to be maximal (so $h(x) \notin \langle f(x)\rangle$). Now suppose $f(x)$ is not irreducible so $f(x) = f_1(x)f_2(x)$ for $f_1(x), f_2(x) \in R[x]$. Then $g(x) = f(x)h(x) = f_1(x)f_2(x)h(x) = f_1(x)\big(f_2(x)h(x)\big)$. Since the $f_i(x)$ are proper factors of $f(x)$ (i.e., $\deg(f_i) < \deg(f)$), neither $f_i(x)$ contains a factor of $f(x)$. Then $g(x) \in \langle f(x)\rangle$ but neither $f_1(x)$ nor $f_2(x)h(x)$ are multiples of $f(x)$ (are in $\langle f(x)\rangle$), so if $f(x)$ is not irreducible then $\langle f(x)\rangle$ is not prime. (Now notice that all of our statements could be reversed, so this proves the if and only if!)

(b) Since F is a field, $F[x]$ is a principal ideal domain. Thus, all ideals in $F[x]$ are of the form $\langle f(x)\rangle$ for some $f(x) \in F[x]$. Notice that a field F is also a commutative ring with unity. Then $\langle f(x)\rangle$ is prime if and only if $f(x)$ is irreducible over F by part (a), but $\langle f(x)\rangle$ is maximal in $F[x]$ if and only if $f(x)$ is irreducible by Thm 22. Using both of these two if and only if statements, any prime ideal of $F[x]$ is maximal.

HW3 (D). Let R be a commutative ring with unity and let I be an ideal of R. We call an ideal of R **primary** if for all $a, b \in R$ when $ab \in I$ then either $a \in I$ or $b^n \in I$ for some $n \in \mathbb{Z}^+$. Prove that every zero divisor in R/I is nilpotent if and only if I is a primary ideal. (Recall that an element x of some ring S is **nilpotent** if there exists a $n \in \mathbb{Z}^+$ such that $x^n = 0$.)

Proof : Suppose $a, b \in R$ such that $a + I, b + I \in R/I$ are zero divisors. Then $a, b \notin I$ (so $a + I, b + I \neq 0 + I$) and $(a + I)(b + I) = ab + I = 0 + I$ so $ab \in I$. Since $a + I, b + I$ are zero divisors, by hypothesis we have that $a + I$ and $b + I$ are nilpotent, so there exist $n, m \in \mathbb{Z}^+$ such that $(a+I)^n = a^n + I = 0 + I$ and $(b+I)^m = b^m + I = 0 + I$. Then $a^n, b^m \in I$ as well. Then in this particular case we have that for $a, b \notin I$, when $ab \in I$ then a^n or b^m in I. On the other hand, if a or b was in I originally, we would also have $ab \in I$ by the definition of an ideal. Then if every zero divisor of R/I is nilpotent, if $ab \in I$ either a^n or b is in I, which makes I a primary ideal by definition.

All of the statements we made were by definition or reversible, so turn all your arrows around to show that if I is primary then every zero divisor is nilpotent.