Graduate Algebra
Homework 9

Fall 2014

Due 2014-11-19 at the beginning of class

1. Let R be a PID. Throughout this exercise, $\pi \in R$ represents a prime element, $P(X) \in R[X]$ is an irreducible polynomial and $Q(X) \in R[X]$ is a polynomial whose image in $R/(\pi)[X]$ is irreducible.

   (a) Show that (π), $(P(X))$ and $(\pi, Q(X))$ are prime ideals of $R[X]$.

   (b) Let $\mathfrak{p}$ be a prime ideal of $R[X]$. Show that $\mathfrak{p} \cap R$ is either 0 or (π).

   (c) If $\mathfrak{p} \cap R = (0)$ show that $\mathfrak{p}$ is either 0 or some $(P(X))$. [Hint: Show that $\mathfrak{p}$ gives a prime ideal of $R[X]$ localized at the multiplicative set $R - 0$. What is this localization?]

   (d) If $\mathfrak{p} \cap R = (\pi)$ show that either $\mathfrak{p} = (\pi)$ or $\mathfrak{p} = (\pi, Q(X))$ for some π and $Q(X)$. [Hint: Look at $R[X]/(\pi)R[X]$.]

   (e) What are the prime and maximal ideals of $\mathbb{Z}[X]$?

   Proof. (a): (π) is prime from h1. $(P(X))$ is prime because R is a PID so a UFD and so $R[X]$ is a UFD and in a UFD every irreducible is prime. Finally, $R[X]/(\pi, Q) \cong (R[X]/(\pi))/((\pi, Q)/(\pi)) \cong (R/(\pi))[X]/(Q \mod \pi)$. Now $R/(\pi)$ is a PID (by h1 every ideal of $R/(\pi))$ is the same as an ideal of R containing (π)) and so it is a UFD so $(R/(\pi))[X]$ is a UFD in which the irreducible $Q(X) \mod \pi$ is prime. Thus $R[X]/(\pi, Q)$ is an integral domain so (π, Q) is a prime ideal.

   (b): Consider $i : R \to R[X]$. Then $\mathfrak{p} \cap R = i^*(\mathfrak{p})$ which is a prime ideal of R. R is a PID so $\mathfrak{p} \cap R = (0)$ of (π) for some $\pi \in R$ nonzero.

   (c): R is a PID so $S = R - 0$ is multiplicatively closed. Since $\mathfrak{p} \cap R = 0$ then $\mathfrak{p} \cap S = \emptyset$ so $\mathfrak{p}$ yields a prime ideal $S^{-1}\mathfrak{p}$ of $S^{-1}R[X] = \operatorname{Frac} R[X]$. But $\operatorname{Frac} R[X]$ is a PID as $\operatorname{Frac} R$ is a field so $S^{-1}\mathfrak{p} = (T(X))$ for some $T \in \operatorname{Frac} R[X]$ either 0 or irreducible. If $T = 0$ then $S^{-1}\mathfrak{p} = 0$ and so $\mathfrak{p} = 0$. If T is irreducible in $\operatorname{Frac} R[X]$, let $\alpha \in \operatorname{Frac} R$ such that $P = \alpha T \in R[X]$ with coprime coefficients. (Take α the gcd of the denominators of the coefficients of T divided by the gcd of the numerators of the coefficients of T.)

   Then $S^{-1}\mathfrak{p} = (T) = (P)$ and so $\mathfrak{p} = \{Q(X) | Q(X)/1 \in (P)\}$ so we seek $Q/1 = PU/r$ for $U \in R[X]$ and $r \in R - 0$. But then for some $t \in R - 0$ have $(Qr - PU)t = 0$ and since $R[X]$ is an integral domain we get $Qr = PU$ so $P \mid Qr$. P is irreducible in $R[X]$ because it is so in $\operatorname{Frac} R[X]$ and its coefficients are coprime. Thus $(r, P) = (1)$ and so $P \mid Q$ which implies that $\mathfrak{p} = (P(X))$.

   (d): Suppose $\mathfrak{p} \cap R = (\pi)$. The set of such $\mathfrak{p}$ is, by h1, in bijection with the prime ideals of $R[X]/(\pi) = (R/(\pi))[X]$. But $R/(\pi)[X]$ is a PID and so UFD so its prime ideals are principal of the form $(Q(X))$ where $Q \in R[X]$ is either 0 or irreducible mod π. If 0 then $\mathfrak{p} = (\pi)$ and otherwise $\mathfrak{p}$ is the preimage $(\pi, Q(X))$ of $(Q(X))$.

   (e): $\mathbb{Z}$ is a PID so its prime ideals are (0), (p), $(P(X))$ and $(p, Q(X))$ where p is a prime, $P \in \mathbb{Z}[X]$ is irreducible and $Q(X) \in \mathbb{Z}[X]$ is irreducible mod p. Among these maximal are the (p, Q). Indeed, in the other cases the quotient is not a field. Let's show that $\mathbb{Z}[X]/(p, Q(X)) \cong \mathbb{F}_p[X]/(Q(X))$ is a field. $\mathbb{F}_p$ is a field, $\mathbb{F}_p[X]$ is a PID and $(Q(X))$ is a prime ideal of this PID. It is contained in some maximal ideal $(T(X))$ with T irreducible. But then T divides Q and by irreducibility of Q we deduce that $Q = T$ so (Q) is a maximal ideal of $\mathbb{F}_p[X]$. $\square$

2. Let $R = \mathbb{C}[X,Y]$. [Hint: This is an application of the previous problem.]

   (a) Show that the prime ideals of $\mathbb{C}[X,Y]$ are (0), $(P(X,Y))$ for an irreducible $P(X,Y) \in \mathbb{C}[X,Y]$ and $(X-a, Y-b)$ for some $a,b \in \mathbb{C}$. Show that the maximal ideals are $(X-a, Y-b)$.

   (b) Show that $\mathfrak{p} = (Y^2 - X^3 - X^2)$ is a prime ideal and that if $a, b \in \mathbb{C}$ such that $b^2 = a^3 + a^2$ then $\mathfrak{p} \subset (X-a, Y-b)$.

   (c) Let $\mathfrak{q} = (X-a, Y-b)$. Show that the prime ideals of the localization $R_{\mathfrak{q}}$ are: (0), $\mathfrak{q}R_{\mathfrak{q}}$ and $(P(X,Y))R_{\mathfrak{q}}$ for any irreducible polynomial $P(X,Y) \in \mathbb{C}[X,Y]$ such that $P(a,b) = 0$.

Proof. (a): $\mathbb{C}[X]$ a PID then the previous problem yields the prime ideals of $\mathbb{C}[X,Y]$: (0), $(P(X))$ for an irreducible $P(X) \in \mathbb{C}[X]$, $(P(X,Y))$ for an irreducible $P(X,Y) \in \mathbb{C}[X,Y]$, and $(P(X), Q(X,Y))$ with P irreducible and $Q(X,Y)$ irreducible in the quotient $\mathbb{C}[X,Y]/(P(X))$. But P irreducible in $\mathbb{C}[X]$ implies $P(X) = X - a$ for some $a \in \mathbb{C}$ in which case $\mathbb{C}[X,Y]/(P(X)) = \mathbb{C}[X,Y]/(X-a) \cong \mathbb{C}[Y]$ and thus $Q(X,Y)$ irreducible in $\mathbb{C}[Y]$ means it is of the form $Q \mod P = Y - b$ for some $b \in \mathbb{C}$. Finally the list in the problem is complete as $X - a$ is an example of irreducible $P(X,Y)$.

(b): If $P(X,Y) = Y^2 - X^3 - X^2$ we need to show that $P(X,Y) \equiv 0 \pmod{X-a, Y-b}$. But $Y \equiv b \pmod{X-a, Y-b}$ and $X \equiv a \pmod{X_a, Y-b}$ and the conclusion follows.

(c): The prime ideals of the localization $R_{\mathfrak{q}}$ are in bijection with the prime ideals $\mathfrak{r}$ of R such that $\mathfrak{r} \subset \mathfrak{q}$. Then $\mathfrak{r}$ is either (0), $(S(X,Y))$ for S irreducible or $(X-c, Y-d)$, from the classification. In the second case need $S(X,Y)$ to be a linear combination of $X-a$ and $Y-b$ so $S(a,b) = 0$. In the third case we need $c = a$ and $d = b$. $\square$

3. Consider the ring $\mathbb{Z}[\zeta_3]$.

   (a) Show that $\mathbb{Z}[\zeta_3]$ is a Euclidean domain. [Hint: Mimick the proof from the $\mathbb{Z}[i]$ case.]

   (b) Show that the units are $\mathbb{Z}[\zeta_3]^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$. [Hint: Show that $z \in \mathbb{Z}[\zeta_3]$ is a unit iff $|z| = 1$.]

Proof. (a): Let $d(z) = |z|^2$. Pick $x, y \in \mathbb{Z}[\zeta_3]$ and let q the element of $\mathbb{Z}[\zeta_3]$ closest in Euclidean distance to $x/y \in \mathbb{C}$. The elements of $\mathbb{Z}[\zeta_3] \subset \mathbb{C}$ form a lattice consisting of unit side length equilateral triangles. Thus $|x/y - q| \leq 1/\sqrt{3}$ as inside an equilateral triangle of side 1 the farthest one can be from the closest vertex is by being in the center, at distance $1/\sqrt{3}$. Take $r = x - qy \in \mathbb{Z}[\zeta_3]$ in which case $d(r) = |x - yq|^2 = |y|^2|x/y - q|^2 \leq d(y)/3 < d(y)$. We deduce that d is a Euclidean function.

(b): If $u \in \mathbb{Z}[\zeta_3]^\times$ then $uv = 1$ so $|u|^2|v|^2 = 1$. But for $u = a + b\zeta_3$, $|u|^2 = a^2 + ab + b^2 \in \mathbb{Z}$ so $|u|^2 = 1$. Reciprocally, if $|u| = 1$ it follows that $u\overline{u} = 1$ and certainly $\overline{u} \in \mathbb{Z}[\zeta_3]$. We solve $|u|^2 = a^2 + ab + b^2 = (a + b/2)^2 + 3b^2/4 = 1$. On the LHS each square is positive and cannot be > 1 so $3b^2 \leq 4$ so b is either 0 or ± 1. If $b = 0$ then $a^2 = 1$ so $u = a + b\zeta_3 = \pm 1$. If $b = \pm 1$ then we get $a^2 + ab = 0$ so $a = 0$ or $a = -b$. Thus $u = \pm\zeta_3$ or $u = \pm(1 + \zeta_3) = \pm\zeta_3^2$. $\square$

4. Let R be a commutative ring. A commutative ring is said to be **reduced** if it has no nonzero nilpotent elements.

   (a) Suppose that for every prime ideal $\mathfrak{p}$ the localization $R_{\mathfrak{p}}$ is reduced. Show that R is reduced. [Hint: For a given x look at $\{y | xy = 0\}$?]

   (b) Show that $R = \mathbb{Z}/6\mathbb{Z}$ is not an integral domain but each localization $R_{\mathfrak{p}}$ is an integral domain.

Proof. (a): If $0 \neq x \in \mathrm{Nil}(R)$ then $x^n = 0$ for some n so $x \in \mathrm{Nil}(R_{\mathfrak{p}})$ for all prime ideals $\mathfrak{p}$ of R. Look at $A = \{y \in R | xy = 0\}$. Then A is an ideal. Since $x \neq 0$ it follows that $A \neq R$ and so it is contained in a maximal ideal $\mathfrak{m}$ of R. Then $x/1 = 0$ in $R_{\mathfrak{m}}$ which implies that $xy = 0$ for some $y \in R - \mathfrak{m}$ which contradicts the fact that $y \in A$.

(b): The prime ideals of $R = \mathbb{Z}/6\mathbb{Z}$ are (2) and (3) ((0) is not as R is not a domain). Let's show, e.g, that $R_{(2)}$ is a domain, in fact a field. The elements are $\{a/b | a = 0, 1, 2, 3, 4, 5, b = 1, 3, 5\}$. If $a = 0, 2, 4$ then $a/b = (3a)/(3b) = 0/3b = 0$ as $3b \in \{1, 3, 5\}$ and so the nonzero elements of $R_{(2)}$ are $\{a/b | a, b = 1, 3, 5\}$ which is visibly a group. The $R_{(3)}$ case is analogous. $\square$

5. Let R be a commutative ring. A proper (i.e., not 0 or R) ideal I of R is said to be **good** if the image of $R^\times \cup 0$ in R/I is all of R/I.

   (a) Suppose R is a PID with no proper good ideals. Show that R cannot be a Euclidean domain. [Hint: Otherwise, among the proper ideals $I = (a)$ of R choose one with $d(a)$ minimal. Show that I is good.]

   (b) You may assume that the ring $R = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID, that $R^\times = \{\pm 1\}$, and that 2 and 3 are prime in R. Show that R is not a Euclidean domain. [Hint: Are there good ideals?]

Proof. (a): Let $I = (a)$ as in the hint. Pick $x \in R$ and write $x = qa + r$. If $x \in I$ then $x + I = I$ is the image of $0 + I$ as desired. If $x \notin I$ then $r \neq 0$. Moreover, $d(r) < d(a)$ so the ideal (r) cannot be proper as otherwise it would contradict the choice of a. Thus $(r) = R$ and so $r \in R^\times$. But then $x + I = r + I$ as desired.

(b): We show there are no good ideals. Suppose $I = (a)$ is good. Thus the image of $\{-1, 0, 1\} = R^\times \cup 0$ in $R/(a)$ is all of $R/(a)$. Take $2 \in R$. Then 2 is congruent mod (a) to one of $-1, 0, 1$ and so a divides one of $1, 2, 3$. Since (a) is proper it cannot divide 1. Thus $a \mid 2$ or $a \mid 3$ and so either $(a) = (2)$ or $(a) = (3)$.

Write $\alpha = \sqrt{-19}$. Then $(1 + \alpha)/2$ is congruent mod (a) to one of $-1, 0, 1$. Thus a must divide $w + (1 + \alpha)/2$ for $w \in \{-1, 0, 1\}$. It is elementary to see that neither 2 nor 3 divides any of these elements. Indeed, if $a(u + v(1 + \alpha)/2) = w + (1 + \alpha)/2$ then we deduce

$$a(u + v/2) = w + 1/2$$
$$av/2 = 1/2$$

Since $a, v \in \mathbb{Z}$ it follows that a must be invertible so neither 2 nor 3 works. $\square$