Commutative Algebra in Context **Fall 2020**
Homework 2 **Drew Armstrong**

Complete 1 problem before October 9.

Problem 1. Gauss' Lemma. Let R be a UFD, so that greatest common divisors exist and irreducible elements are prime. To be precise, we write $\gcd(a_1,\ldots,a_n)=d$ to mean that dR is the unique smallest principal ideal containing the ideal $a_1R+\cdots+a_nR$ (which might not be principal). Thus the greatest common divisor is unique up to multiplication by units.

(a) Let $\gcd(a_1,\ldots,a_n)=d$ with $a_i=da_i'$ for some $a_i,d,a_i'\in R$. In this case show that $\gcd(a_1',\ldots,a_n')=1$. It follows that any nonzero polynomial $f(x)\in R[x]$ can be expressed uniquely as $f(x)=c(f)f'(x)$ where $c(f)$ is the gcd of the coefficients (called the *content* of f) and $c(f')=1$. In this case we say that $f'(x)\in R[x]$ is a *primitive polynomial.*

(b) If $c(f)=c(g)=1$ prove that $c(fg)=1$. [Hint: For any irreducible/prime $p\in R$ we have a ring homomorphism $R[x]\to(R/pR)[x]$ denoted by $f(x)\mapsto f_p(x)$. Observe that $c(f)=1$ if and only if $f_p(x)\neq 0(x)$ for all prime $p\in R$.]

(c) Prove that $c(fg)=c(f)c(g)$ for all nonzero $f(x),g(x)\in R[x]$. [Hint: Use (a) and (b).]

(d) Let $\mathbb{F}=\mathrm{Frac}(R)$. Show that any nonzero $f(x)\in\mathbb{F}[x]$ can be expressed uniquely as $f(x)=\alpha f'(x)$ where $\alpha\in\mathbb{F}\setminus 0$ and $f'(x)\in R[x]$ is primitive. [Hint: Choose $a\in R$ such that $af(x)\in R[x]$ and let $\alpha=c(af)$.]

(e) If $f(x)=\prod g_i(x)$ for some $f(x),g_i(x)\in\mathbb{F}[x]$, prove that $f'(x)=\prod g_i'(x)$, where $f'(x),g_i'(x)\in R[x]$ are the unique primitive factors. [Hint: We have $f(x)=\alpha f'(x)$ and $g_i=\beta_i g_i'(x)$ for some $\alpha,\beta_i\in\mathbb{F}\setminus 0$, so that $\alpha f'=(\prod\beta_i)(\prod g_i')$. Multiply both sides by $a\in R$ such that $a\alpha\in R$ and $a(\prod\beta_i)\in R$, then compute the content of each side.]

(f) Prove that an irreducible polynomial $f(x)\in R[x]$ is still irreducible in $\mathbb{F}[x]$. [Hint: An irreducible polynomial in $R[x]$ must be primitive. Use part (e).]

(g) Prove that coprime polynomials $f(x),g(x)\in R[x]$ are still coprime in $\mathbb{F}[x]$ [Hint: If $p|f$ and $p|g$ in $\mathbb{F}[x]$ then part (e) says that $p'|f'$ and $p'|g'$ in $R[x]$.]

Problem 2. R **UFD** $\Rightarrow R[x]$ **UFD.** Let R be a UFD and $\mathbb{F}=\mathrm{Frac}(R)$.

(a) Prove that any nonzero $f(x)\in R[x]$ can be factored as $f(x)=up_1\cdots p_kq_1(x)\cdots q_\ell(x)$, where $u\in R$ is a unit, $p_i\in R$ are irreducible/prime in R and $q_j(x)\in R[x]$ are irreducible in $R[x]$ (hence also primitive). [Hint: Use 1(e) and the fact that $\mathbb{F}[x]$ is Noetherian.]

(b) Prove that every irreducible/prime $p\in R$ is prime in $R[x]$. [Hint: Consider the homomorphism $R[x]\to(R/pR)[x]$ from the proof of 1(b).]

(c) Prove that any irreducible (hence also primitive) $q(x)\in R[x]$ is prime in $R[x]$. [Hint: Suppose that $q|fg$ in $R[x]$, hence also in $\mathbb{F}[x]$. Since $q(x)\in\mathbb{F}[x]$ is irreducible by 1(f) and since $\mathbb{F}[x]$ is a PID, we see that $f(x) \in \mathbb{F}[x]$ is prime, hence $q|f$ or $q|g$ in $\mathbb{F}[x]$. But then from 1(e) we have $q|f'$ or $q|g'$ in $R[x]$.]

(d) Combine (a),(b),(c) to prove that $R[x]$ is a UFD.

Remark: By induction it follows that $R[\mathbf{x}]$ is a UFD for any finite set of variables $\mathbf{x}$.

Problem 3. Study's Lemma. If $\mathbb{F}$ is a field then it follows from Problem 2 that $\mathbb{F}[x,y]$ is a UFD. Consider any polynomials $f,g \in \mathbb{F}[x,y]$ where f is irreducible and $f \nmid g$, which implies that f and g have no common prime factor.

(a) Prove that there exist polynomials $a(x,y), b(x,y) \in \mathbb{F}[x,y]$ and $c(x) \in \mathbb{F}[x]$ such that

$$f(x,y)a(x,y) + g(x,y)b(x,y) = c(x).$$

[Hint: Let $\mathbb{F}(x)$ be the fraction field of $\mathbb{F}[x]$ and consider f,g as elements of the larger ring $R = \mathbb{F}(x)[y]$. From 1(f) we know that f is irreducible in R and from 1(g) we know that f,g are coprime in R. Now use the fact that R is a PID to show that $fR+gR = R$.]

(b) Consider the curves $C_f : f(x,y) = 0$ and $C_g : g(x,y) = 0$ in the plane $\mathbb{F}^2$. Use part (a) to show that the intersection $C_f \cap C_g$ consists of finitely many points.

Problem 4. Prime Ideals of $R[x]$ when R is a PID. Let R be a PID. We will show that every prime ideal of $R[x]$ has one of the following three forms:

- The zero ideal.
- Principal prime ideals. These are not maximal.
- Ideals of the form $pR[x] + f(x)R[x]$ where $p \in R$ is prime and the image of $f(x)$ is irreducible in the quotient ring $(R/pR)[x]$. These are the maximal ideals.

(a) Let $P \subseteq R[x]$ be a **non-principal** prime ideal. Show that P contains two coprime elements $f_1, f_2 \in R[x]$. [Hint: Show that P contains an irreducible element f_1. Then show that any $f_2 \in P \setminus f_1R[x]$ is coprime to f_1.]

(b) It follows from Problem 1(g) that f_1, f_2 are coprime in $\mathbb{F}[x]$ where $\mathbb{F} = \mathrm{Frac}(R)$. Use this to show that $P \cap R = pR$ for some nonzero prime $p \in R$. [Hint: The hard part is to show that $P \cap R \neq 0$. Use the fact that $\mathbb{F}[x]$ is a PID to show that $f_1a + f_2b = c$ for some $a,b,c \in R$ with $c \neq 0$. This is similar to Problem 3(a).]

(c) Now let $f(x) \mapsto f_p(x)$ denote the ring homomorphism $\varphi : R[x] \to (R/pR)[x]$ defined by reducing each coefficient mod p. Show that $\varphi[P] = f_p(x)(R/pR)[x]$ for some $f(x) \in R[x]$ such that $f_p(x) \in (R/pR)[x]$ is irreducible, and conclude that $P = pR[x] + f(x)R[x]$. [Hint: Since R/pR is a field we know that $(R/pR)[x]$ is a PID.]

(d) Show that $P = pR[x] + f(x)R[x]$ is maximal. [Hint: Show that the quotient $R[x]/P$ is isomorphic to the quotient $(R/pR)[x]/f_p(x)(R/pR)[x]$, which is a field.]

(e) Finally, show that principal prime ideals of $R[x]$ are not maximal. [Hint: Every principal prime has the form $pR[x]$ for prime $p \in R$ or $f(x)R[x]$ for irreducible $f(x) \in R[x]$. In the first case, consider $pR[x] + xR[x]$. In the second case, consider $pR[x] + f(x)R[x]$ where p does not divide the leading coefficient of $f(x)$.]

Problem 5. Nullstellensatz for Curves in the Plane. In this problem we assume that $\mathbb{F}$ is algebraically closed. We say that $C \subseteq \mathbb{F}^2$ is an *algebraic curve* if it has the form $C_f : f(x, y) = 0$ for some nonzero polynomial $f(x, y) \in \mathbb{F}[x, y]$.

(a) Prove that $\mathbb{F}$ is infinite. Use this to show that for any polynomial $f(x, y) \in \mathbb{F}[x, y]$ the curve $C_f : f(x, y) = 0$ has infinitely many points in $\mathbb{F}^2$. [Hint: Assume for contradiction that $\mathbb{F}$ is finite and consider the polynomial $1 + \prod_{a\in\mathbb{F}}(x - a)$.]

(b) For any $f, g \in \mathbb{F}[x, y]$ with f irreducible, show that $C_f \subseteq C_g$ implies $f|g$. [Hint: Use part (a) and Study's Lemma.]

(c) We say that a curve C is *irreducible* if it cannot be expressed as a union of curves. Show that there is a bijection between irreducible curves $C \subseteq \mathbb{F}^2$ and principal prime ideals of $\mathbb{F}[x, y]$. [Hint: If $f = gh$ is reducible then $C_f = C_g \cup C_g$ is reducible. Conversely, if $C_f = C_g \cup C_h$ is reducible, let p be a prime factor of g. Then part (b) implies that $p|f$, hence f is reducible. Finally, if $f, g \in \mathbb{F}[x, y]$ are both irreducible, use part (b) to show that $C_f = C_g$ if and only if $f(x)\mathbb{F}[x, y] = g(x)\mathbb{F}[x, y]$.

(d) Show that there is a bijection between points of $\mathbb{F}^2$ and maximal prime ideals of $\mathbb{F}[x, y]$. [Hint: For any point $(a, b) \in \mathbb{F}^2$, let $\mathfrak{m}_{a,b} \subseteq \mathbb{F}[x, y]$ be the kernel of the evaluation homomorphism $f(x, y) \mapsto f(a, b)$, which is maximal because evaluation is surjective onto $\mathbb{F}$. Show that $\mathfrak{m}_{a,b} = (x - a)\mathbb{F}[x, y] + (y - b)\mathbb{F}[x, y]$. Conversely, use Problem 4 and the fact that $\mathbb{F}$ is algebraically closed to show that every maximal ideal of $\mathbb{F}[x, y]$ has the form $\mathfrak{m}_{a,b}$ for some point $(a, b) \in \mathbb{F}^2$.]

(e) **Strong Nullstellensatz.** Show that every prime ideal of $\mathbb{F}[x, y]$ is equal to the intersection of the maximal ideals that contain it. Geometric meaning:

A curve is determined by its points.

Of course this statement is geometrically obvious, but it takes a lot of work to establish that the algebra matches the geometry.

[Hint: This is vacuously true for maximal primes. The intersection of all maximal ideals $\cap\mathfrak{m}_{a,b}$ is the set polynomials that vanish at all points $(a, b) \in \mathbb{F}^2$, i.e., just the zero polynomial. Now let $P \subseteq \mathbb{F}[x, y]$ be a nonzero, nonmaximal prime. From Problem 4 we know that $P = f(x)\mathbb{F}[x, y]$ for some irreducible f. Let C_f be the corresponding irreducible curve and let I_f be the intersection of the maximal ideals $\mathfrak{m}_{a,b}$ for all points $(a, b) \in C_f$. Thus I_f consists of polynomials that vanish at all points of C_f. Certainly $f(x)\mathbb{F}[x, y] \subseteq I_f$. Conversely, if $g \in I_f$ then use part (b) to show that $g \in f(x)\mathbb{F}[x, y]$.]