Mike O'Sullivan
Department of Mathematics
San Diego State University Fall 2011

Math 627B: Modern Algebra II

Exam Review

Thursday Nov. 3, 2011

Rings are always commutative and have an identity element. Any homomorphism of rings $\phi : R \longrightarrow S$ must take the identity element of R to the identity element of S.

Topics and suggested problems to prepare for the exam.

I. Groebner bases

II. Formation of fractions (localization).

III. Modules, ideals and homomorphisms.

IV. Unique Factorization Domains

Some things you should be able to do.

1. Description of monomial orders on $k[x_1, \ldots, x_n]$ using vectors in $\mathbb{N}_0^n$ (HW 3).
2. Be able to compute a Groebner basis from a generating set for an ideal. (Clearly the amount of computation involved has to be minimal.) (HW 2)
3. Computing in R/I using a Groebner basis for I (HW 2, 4).
4. Problems on radical ideals and nilpotents (HW 4).
5. Problems on formation of fractions and ideals in $S^{-1}R$ (HW 4).
6. Problems on homomorphisms and ideals (HW 4).
7. The ascending chain condition and finitely generated ideals (HW 4).
8. Problems on unique factorization below.
9. Problems on ideals and modules below.

Problem 1: Let R be a ring, I and J ideals in R. The annihilator of I is the set $\mathrm{Ann}(I) = \{r \in R : ra = 0 \text{ for all } a \in I\}$.

(a) Show that the annihilator of I is an ideal in R.

(b) Compute $\mathrm{Ann}(\langle x^3 - x^2 \rangle)$ in the ring $\mathbb{Q}[x]$. Compute $\mathrm{Ann}(\langle x^3 - x^2 \rangle)$ in the ring $\mathbb{Q}[x]/\langle x^4 - x \rangle$.

(c) The quotient of the ideals I and J, also called the colon ideal of I and J, is $I : J = \{r \in R : ra \in J \text{ for all } a \in I\}$. Show that $I : J$ is indeed an ideal.

(d) The annihilator of an ideal is a special case of the ideal quotient. Explain.

(e) Compute $\langle x^4 - x \rangle : \langle x^3 - x^2 \rangle$ in the ring $\mathbb{Q}[x]$.
Compute $\langle x^3 - x^2 \rangle : \langle x^4 - x \rangle$ in the ring $\mathbb{Q}[x]$.

(f) The previous concepts may be extended to modules. Let M be a module over R. Let

$$\mathrm{Ann}_R(M) = \{r \in R : rm = 0 \text{ for all } m \in M\}$$

Show that $\mathrm{Ann}_R(M)$ is an ideal in R.

(g) Consider R/I as a module over R. Show that $\mathrm{Ann}_R(R/I) = I$.

Problem 2: Let R be a unique factorization domain. It is easy to show that p is irreducible iff up is irreducible for all units u. Furthermore, the relation of being associate is an equivalence relation. Let Irr be a set of representatives for all irreducibles, one for each associate class of irreducibles.

(a) Let K be the quotient field of R. Explain why every element of K may be written, in a unique way, as a product

$$u \prod_{p \in \mathrm{Irr}} p^{e_p}$$

where u is a unit, each $e_p \in \mathbb{Z}$, and only a finite number of e_p are nonzero.

(b) Let $r_1, \ldots, r_t \in R$ and let $d = \gcd(r_1, \ldots, r_t)$. Show that $\gcd(r_1/d, \ldots, r_t/d) = 1$.

(c) Let $m = \mathrm{lcm}(r_1, \ldots, r_t)$. Show that $\gcd(m/r_1, \ldots, m/r_t) = 1$.

(d) Use the unique factorization of $r \in R$ to compute the number of ideals that contain the ideal $\langle r \rangle$ that are both prime and principal. How many are radical and principal?

(e) If $R = \mathbb{C}[x, y]$ the variety of a principal ideal is a curve. Give a geometric interpretation for a factorization of $f(x, y) \in \mathbb{C}[x, y]$. What can you say about the associated varieties? Interpret the previous problem about prime principal ideals in this context.

1 Notes on UFDs

Here is a summary of results from the last two classes.

Theorem 1.1. *Let R be an integral domain. R is a UFD iff*

1. *R satisfies the ascending chain condition on principal ideals.*
2. *Each irreducible in R is also prime.*

Theorem 1.2. *Every PID is also a UFD.*

For the remainder of these notes R is a UFD and K is its field of fractions, $K = (R \setminus \{0\})^{-1}R$. We will use the fact that R and $K[x]$ are UFD's to show $R[x]$ is a UFD.

Definition 1.3. Let R be a UFD and let $f_0 + f_1x + f_2x^2 + \cdots + f_dx^d \in R[x]$. The content of $f(x)$ is $c(f) = \gcd(f_0, \ldots, f_d)$. We say f is primitive when $c(f) = 1$.

Proposition 1.4. *The product of primitive polynomials is primitive.*

Proposition 1.5. *Each nonzero non-unit $f(x) \in R[x]$ can be factored as $cf^*(x)$ where $c \in R$ and $f^*(x)$ is primitive. This factorization is unique up to unit multiples of c and f^*.*

Proposition 1.6 (Content of a product)**.** *Let $f(x)$, $g(x)$ and $h(x)$ be nonzero nonunits in $R[x]$.*

1. *For $f(x)$ and $g(x)$ nonzero nonunits in $R[x]$, $c(fg) = c(f)c(g)$ and $(fg)^*(x) = f^*(x)g^*(x)$.*
2. *If $f(x)$ divides $h(x)$ then $c(f)$ divides $c(h)$ and $f^*(x)$ divides $h^*(x)$.*
3. *If $f(x)$ divides $h(x)$ and $\deg(f(x)) = \deg(h(x))$ then $f^*(x) = h^*(x)$.*

Proposition 1.7. *$R[x]$ satisfies the ACC on principal ideals.*

Proposition 1.8. *For $a(x) \in K[x]$ there are $c, d \in R$ with $\gcd(c, d) = 1$ such that $da(x)/c$ is primitive. Furthermore, c and d are unique up to unit multiples of d and c.*

We will write $a^*(x)$ for the unique primitive polynomial $da(x)/c$ in $R[x]$ (up to unit multiple) in the proposition.

Proposition 1.9. *Let $g^*(x)$ be primitive in $R[x]$.*

1. *g is reducible in $R[x]$ iff $g(x)$ is reducible in $K[x]$.*
2. *If $a(x)$ in $K[x]$ divides $g(x)$ then $a^*(x)$ divides $g(x)$ (this is in $R[x]$!).*

Proof. Suppose $g(x)$ is reducible in $R[x]$. Since $g(x)$ is primitive it has no factors in R (such a factor would have to divide all coefficients of $g(x)$. Thus any factorization of $g(x)$ involves polynomials of strictly lower degree. This gives a nontrivial factorization in $K[x]$.

Suppose $g(x) = a_1(x)b_1(x)$ is a nontrivial factorization in $K[x]$. Notice this implies that $dega_i(x) < \deg(g(x))$. Let c_1, d_1, and c_1, d_2 satisfy the property of Proposition 1.9. Then

$$\frac{d_1d_2}{c_1c_2}g(x) = \frac{d_1a_1(x)}{c_1}\frac{d_2a_2(x)}{c_2}$$

Right hand side is primitive in $R[x]$, so the left had side is also. Since $g(x)$ is primitive in $R[x]$, $(d_1d_2)/(c_1c_2)$ must be a unit in R. Thus

$$g(x) = \frac{c_1c_2}{d_1d_2}\frac{d_1a_1(x)}{c_1}\frac{d_2a_2(x)}{c_2}$$

is a factorization of $g(x)$ in $R[x]$ into polynomials of degree less than $\deg(g(x))$.

The last paragraph shows that if $a(x)$ divides $g(x)$ (with $g(x)$ primitive in $R[x]$) then $a^*(x)$ (an element of $R[x]$!) divides $g(x)$. □

Theorem 1.10. *If R is a UFD then so is $R[x]$.*

Proof. By Proposition 1.7 $R[x]$ satisfies the ACC on principal ideals, so we only have to show that irreducible implies prime in $R[x]$.

Let $p(x)$ be irreducible in $R[x]$ and suppose that $p(x)$ divides $f(x)g(x)$ in $R[x]$.

If $\deg p(x) = 0$ then $c(p) = p(x)$ and $c(p)$ is an irreducible element of R. Now $c(p)$ divides $c(f)c(g)$ so it must divide one of the factors, so $p(x)$ divides either $f(x)$ or $g(x)$.

If $\deg(p(x)) > 0$ then, $p(x)$ must be primitive, since otherwise the factorization of Proposition 1.5 is nontrivial. Proposition 1.6 shows that $p(x)$ divides $f^*(x)g^*(x)$, so we may assume that $f(x)$ and $g(x)$ are primitive. Now Proposition 1.9 shows that $p(x)$ is irreducible in $K[x]$ as well. Since $K[x]$ is a UFD, $p(x)$ is prime in $K[x]$. Thus $p(x)$ divides $f(x)$ or $g(x)$. Suppose it is $g(x)$. Since we may assume $g(x)$ is primitive, Proposition 1.9 says that $p(x)$ divides $g(x)$. □