Modern Algebra II Spring 2013
Review Sheet for the First Midterm

A *ring* $(R, +, \cdot)$ (which we usually abbreviate by R) is a set R, together with two binary operations $+$ and $\cdot$, such that $(R, +)$ is an abelian group, $\cdot$ is associative, and the left and right distributive laws hold. The ring R is *commutative* if $\cdot$ is commutative. If there is a multiplicative identity (almost always written as 1) we say that R has a *unity* (the multiplicative identity, necessarily unique). In this case, a *unit* of R is an element with a multiplicative inverse. The set of all units of R is denoted R^*; $(R^*, \cdot)$ is a group. If R is a ring with unity $1 \neq 0$ and every nonzero element of R has a multiplicative inverse (i.e. $R^* = R - \{0\}$), then R is a *division ring* or *skew field*. A commutative division ring is called a *field*. For example, $\mathbb{Z}/n\mathbb{Z}$ is a field $\iff$ $n = p$ is a prime number. We shall usually denote the field $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$.

If $(R, +, \cdot)$ and $(S, +, \cdot)$ are two rings, then R is *isomorphic to* S if there exists a function $f \colon R \to S$ such that f is a bijection and, for all $r_1, r_2 \in R$, $f(r_1 + r_2) = f(r_1) + f(r_2)$ and $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$. Such a function f is called an *isomorphism*. A *homomorphism* is defined in the obvious way (we do not require that f is a bijection). However, if both R and S are rings with unity, we shall require that a homomorphism $f \colon R \to S$ satisfy: $f(1) = 1$. (For an isomorphism this is automatic.) Likewise, a *subring* R' of a ring R (written $R' \leq R$) is a subset R' such that 1) $(R', +)$ is an additive subgroup of the additive group $(R, +)$, and 2) R' is closed under multiplication. However, if R is a ring with unity 1, then we shall always require that $1 \in R'$ as well.

Homomorphisms: Let $f \colon R \to S$ be a (ring) homomorphism. Then $\operatorname{Im} f = f(R)$ is a subring of S. Moreover, $f(0) = 0$, $f(1) = 1$ if R, S have unity (by convention), and in this case if u is a unit in R then $f(u)$ is a unit in S and $f(u)^{-1} = f(u^{-1})$. Moreover, if $\operatorname{Ker} f = \{r \in R : f(r) = 0\}$, then f is injective $\iff$ $\operatorname{Ker} f = \{0\}$.

From now on: R is always assumed to be commutative with unity.

Polynomials: Let R be a ring. The ring $R[x]$ is the ring of all polynomials $f(x) = a_nx^n + \cdots + a_0$ with coefficients in R. Formally we can identify the polynomial $f(x)$ with the infinite sequence of coefficients $(a_0, a_1, \ldots, a_n, \ldots)$, where there exists an N such that $a_i = 0$ for all $i \geq N$. Thus $f(x) = g(x)$ if and only if they have the same coefficients, i.e. define the same sequences. The largest $n \geq 0$ such that $a_n \neq 0$ is the *degree* $\deg f(x)$ of $f(x)$. (The degree of the 0 polynomial is not defined.) If $n = \deg f(x)$, then the coefficient a_n of x^n is called the *leading coefficient* of $f(x)$, and $f(x)$ is *monic* if its leading coefficient is 1. A polynomial is a *constant polynomial* if is zero or has degree 0. Note that, unless R is the zero ring, $R[x]$ is always infinite, even if R is finite.

Addition and multiplication of polynomials are defined in the usual way:

$$\left(\sum_i a_i x^i\right) + \left(\sum_i b_i x^i\right) = \left(\sum_i (a_i + b_i) x^i\right);$$
$$\left(\sum_i a_i x^i\right) \cdot \left(\sum_i b_i x^i\right) = \left(\sum_n \left(\sum_{i+j=n} a_i b_j\right) x^n\right).$$

With these definitions, $R[x]$ becomes a commutative ring with unity, containing (a subring isomorphic to) R where we view $r \in R$ as a constant polynomial. Moreover

$$\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\};$$
$$\deg f(x)g(x)) \leq \deg f(x) + \deg g(x).$$

Polynomials in several variables are defined similarly. If R is a ring, then $R[x_1, \ldots, x_n]$ is the polynomial ring in n variables with coefficients in R. It is easy to see that there is a natural isomorphism $R[x_1, \ldots, x_n] \cong R[x_1, \ldots, x_{n-1}][x_n]$.

Let R be a ring and let $a \in R$. There is a homomorphism $\mathrm{ev}_a \colon R[x] \to R$ defined by: $\mathrm{ev}_a(f(x)) = f(a)$. It is a surjective homomorphism and (one can check directly) its kernel is $(x - a)$. In this way, a polynomial defines a function $R \to R$. (But not every function $R \to R$ arises this way, and two different polynomials can define the same function. In more abstract terms, there is a ring homomorphism $E \colon R[x] \to R^R$, given by associating to $f(x) \in R[x]$ the function from R to R that it defines: $E(f)(r) = f(r)$. But E is not in general injective or surjective.)

More generally, let R be a subring of a ring S and let $a \in S$. Then we again define $\mathrm{ev}_a \colon R[x] \to S$. Its image is denoted $R[a]$ and is a subring of S, the smallest subring containing both R and a. More generally still, if $\varphi \colon R \to S$ is a homomorphism, then we get a homomorphism, also denoted φ, from $R[x]$ to $S[x]$ via $\varphi(\sum_i a_i x^i) = \sum_i \varphi(a_i) x^i$. For example, if $\varphi \colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is reduction mod n, then $\varphi \colon \mathbb{Z}[x] \to (\mathbb{Z}/n\mathbb{Z})[x]$ is the homomorphism obtained by reducing all of the coefficients of a polynomial mod n. Finally, we can combine these homomorphisms as follows: given a homomorphism $\varphi \colon R \to S$

and an element $a \in S$, we define $\mathrm{ev}_{\varphi,a}\colon R[x] \to S$ via

$$\mathrm{ev}_{\varphi,a} = \mathrm{ev}_a \circ \varphi.$$

One can do the same for polynomials in several variables. For example, if R is a subring of a ring S and $a_1, \dots, a_n \in S$, we have $\mathrm{ev}_{a_1,\dots,a_n}\colon R[x_1, \dots, x_n] \to S$. Its image is the subring $R[a_1, \dots, a_n]$.

Definition: Let R be a ring. A *divisor of* 0 in R is an element $r \in R$ such that $r \neq 0$ and there exists $s \in R$, $s \neq 0$, such that $rs = 0$. An element $r \in R$ is *nilpotent* if there exists an $N > 0$ such that $r^N = 0$. A nonzero nilpotent element is a divisor of zero.

Proposition: Let R be a ring. Then R has no divisors of 0 if and only if the *cancellation law holds*: For all $r, s, t \in R$ with $r \neq 0$, if $rs = rt$ then $s = t$.

Definition: A ring R with unity $1 \neq 0$ is an *integral domain* if R has no divisors of 0 (equivalently, the cancellation law holds).

A field is an integral domain. With our conventions on subrings, a subring of an integral domain is an integral domain.

If R is an integral domain, then $R[x]$ is also an integral domain. More precisely, if $f(x), g(x) \in R[x]$ are both nonzero, then $f(x)g(x) \neq 0$ and

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x).$$

For an integral domain R, the units $(R[x])^* = R^*$. In particular, if F is a field, then $F[x]$ is an integral domain (but never a field) and the group of units in $F[x]$ is just F^*, the group of nonzero constant polynomials.

Definition: Let R be an integral domain ring (although much of the following makes sense for more general rings). If there exists an $n \in \mathbb{N}$ such that $n \cdot 1 = 0$, we say that R has *finite characteristic*. The *characteristic* of R is then the smallest $n > 0$ such that $n \cdot 1 = 0$, so that the characteristic of R is the order of 1 in the additive group $(R, +)$. In this case, the characteristic of R is always a prime number. If R has characteristic n, then $n \cdot r = 0$ for all $r \in R$, and in fact every nonzero element of R has order n. If R does not have finite characteristic, we say that R has *characteristic* 0. In this case, every nonzero element of R has infinite order.

Proposition: A finite integral domain is a field.

The field of quotients of an integral domain: Let R be an integral domain. Then there exists a field $Q(R)$ containing R (or more properly a subring isomorphic to R). To construct $Q(R)$, consider the equivalence relation $\sim$ on the set $R \times (R - \{0\})$ defined by

$$(a, b) \sim (c, d) \qquad \iff \qquad ad = bc.$$

The set of equivalence classes $(R \times (R - \{0\})/\sim$ becomes a ring (in fact, a field $Q(R)$) under the operations

$$[(a, b)] + [(c, d)] = [ad + bc, bd]; \qquad [(a, b)] \cdot [(c, d)] = [ac, bd].$$

Note that, for $a, b \in R$ with $b \neq 0$, $[(a, b)] = [(0, 1)] \iff a = 0$, $[(a, b)] = [(1, 1)] \iff a = b$, and, if $a \neq 0$, $[(a, b)]^{-1} = [(b, a)]$. The homomorphism $\phi(r) = (r, 1)$ is an isomorphism from R to a subring of $Q(R)$, and every element of $Q(R)$ is of the form $\phi(r)\phi(s)^{-1}$ for some $r, s \in R$. In fact, F has the following universal property:

Theorem: Let R be an integral domain with field of quotients $Q(R)$. Let F be a field and let $f \colon R \to F$ be an injective homomorphism. Then there exists a unique injective homomorphism $\tilde{f} \colon Q(R) \to F$ such that $\tilde{f} \circ \phi = f$, i.e. $\tilde{f}([(r, 1)]) = f(r)$. (In fact, we define $\tilde{f}([a, b)]) = f(a)f(b)^{-1}$.) Moreover, $\tilde{f}$ is an isomorphism $\iff$ every element of F is of the form $f(a)f(b)^{-1}$ for some $a, b \in R$.

Example: the field of quotients of $\mathbb{Z}$ is $\mathbb{Q}$. If F is a field, the field of quotients of the polynomial ring $F[x]$ is $F(x)$, the *field of rational functions with coefficients in F*. By definition, $F(x)$ consists of all quotients $f(x)/g(x)$, where $f(x), g(x) \in F[x]$ and $g(x) \neq 0$. If R is an integral domain and $Q(R)$ is its field of quotients, then $R[x]$ is an integral domain and the field of quotients of $R[x]$ is $Q(R)(x)$.

Prime fields: Let F be a field. Either F contains a subring isomorphic to $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ or F contains a subring isomorphic to $\mathbb{Z}$ and hence contains the field of quotients $\mathbb{Q}$ of $\mathbb{Z}$. In particular, if p is a prime number, then every field with p elements is isomorphic to $\mathbb{F}_p$. Every field either contains a field isomorphic to the field $\mathbb{F}_p$ with p elements (if F has characteristic p) or contains a field isomorphic to the field $\mathbb{Q}$ of rational numbers (if F has characteristic 0). We call $\mathbb{F}_p$ and $\mathbb{Q}$ the *prime* fields; every field contains a (unique) subfield isomorphic to exactly one of them.

Definition: A subset $I \subseteq R$ is an *ideal* if I is an additive subgroup of R and, for all $a \in I$ and $r \in R$, $ar \in I$. In other words, $RI \subseteq I$ ("the absorbing property").

Proposition: If I is an additive subgroup of R, then coset multiplication defined by $(r+I)(s+I) = rs+I$ is well-defined $\iff$ I is an ideal. In this case, R/I with the induced operations is a ring, the *quotient ring*, and the function $\pi\colon R \to R/I$ defined by $\pi(r) = r+I$ is a homomorphism, the *quotient homomorphism*.

Examples of ideals: 0) For a ring R, R itself and $\{0\}$ are both ideals.

1) the ideals in $\mathbb{Z}$ are the additive subgroups $n\mathbb{Z} = \langle n \rangle$. Here we can always normalize so that $n \geq 0$. However, for a general ring R, it is almost never the case that the ideals of R are just the additive subgroups of $(R, +)$.

2) If R is a ring and I is an ideal in R, then $I = R \iff 1 \in I$. If F is a field and I is an ideal in F, then either $I = \{0\}$ or $I = R$.

2) Definition: Let R be a ring and let $a \in R$. Then the *principal ideal generated by a* (written (a) or aR) is the set $\{ra : r \in R\}$. It is an ideal in R containing a, and every ideal I in R containing a contains (a). An ideal of the form (a) is called a *principal ideal*.

3) More generally, if R is a ring and $a_1, \dots, a_n \in R$, the *ideal generated by $a_1, \dots a_n$* is by definition the ideal

$$(a_1, \dots a_n) = \left\{ \sum_{i=1}^{n} r_i a_i : r_i \in R \right\}.$$

It is an ideal in R, containing $a_1, \dots a_n$, and is the smallest ideal in R with this property. An ideal of the form $(a_1, \dots a_n)$ is called a *finitely generated ideal*.

Proposition: If $f\colon R \to S$ is a homomorphism, then $\operatorname{Ker} f$ is an ideal in R.

Here is a corollary of sorts to the proposition that the kernel of a homomorphism is an ideal; it says that all ideals arise in this way.

Fundamental Homomorphism Theorem: Let $f\colon R \to S$ be a homomorphism. Then there is a unique isomorphism $\tilde{f}\colon R/\operatorname{Ker} f \to f(R)$ such that $f = i \circ \tilde{f} \circ \pi$, where $\pi\colon R \to R/\operatorname{Ker} f$ is the quotient homomorphism ($\pi(r) = r + \operatorname{Ker} f$), and $i\colon f(R) \to S$ is the inclusion. In diagrams:

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \pi\big\downarrow & & \big\uparrow i \\ R/\operatorname{Ker} f & \xrightarrow{\tilde{f}} & f(R). \end{array}$$

Symbolic adjunction of elements: if R is a subring of a ring S, and $s \in S$, we have defined the subring $R[s]$ of S as the image of the evaluation homomorphism $\mathrm{ev}_s \colon R[x] \to S$. It is the smallest subring of S containing both R and s. Given a polynomials $f(x) \in R[x]$, we can also consider "abstractly" adding an element α to R, satisfying the relations $f(\alpha) = 0$, by taking the quotient ring $R[x]/(f(x))$. If $(f(x)) \cap R = \{0\}$, in other words if $(f(x))$ contains no nonzero constant polynomials (which holds for instance if R is an integral domain and $\deg f(x) \geq 1$), then the composition of homomorphisms $R \to R[x] \to R[x]/(f(x))$ is injective, and thus we can view R as a subring of $R[x]/(f(x))$. Let $\alpha = x + (f(x))$ be the coset containing x. Then every element of $R[x]/(f(x))$ can be expressed as $r_0 + r_1\alpha + \cdots + r_N\alpha^N$, where N is some positive integer and $r_0, \ldots, r_N \in R$, viewed as a subring of $R[x]/(f(x))$. Finally, α satisfies $f(\alpha) = 0$.

Definition: Let R be a ring. An ideal I in R is a *prime ideal* if $I \neq R$ and, for all $r, s \in R$, if $rs \in I$ then either $r \in I$ or $s \in I$.

Proposition: Let R be a ring and let I be an ideal in R. Then R/I is an integral domain if and only if I is a prime ideal.

Definition: Let R be a ring. An ideal I in R is a *maximal ideal* if $I \neq R$ and, if J is an ideal in R containing I, then either $J = I$ or $J = R$.

Proposition: Let R be a ring and let I be an ideal in R. Then R/I is a field if and only if I is a maximal ideal.

Corollary: A maximal ideal is a prime ideal.

Example: in $\mathbb{Z}$, an ideal $(n) = \langle n \rangle$, where $n \geq 0$, is a prime ideal if and only if $n = 0$ or $n = p$ is a prime number. It is a maximal ideal if and only if $n = p$ is a prime number. If F is a field and $R = F[x_1, x_2]$, then the ideals (0) and (x_1) are prime ideals in R but are not maximal, whereas (x_1, x_2) is a maximal ideal in R (it is the kernel of the surjective homomorphism $\mathrm{ev}_{0,0} \colon F[x_1, x_2] \to F$).

Theorem (Long division with remainder): Let F be a field, and let $f(x) \in F[x]$, $f(x) \neq 0$. Then for all $g(x) \in F[x]$, there exist **unique** polynomials $q(x), r(x) \in F[x]$, with $r(x) = 0$ or $\deg r(x) < \deg f(x)$, such that $g(x) = f(x)q(x) + r(x)$.

Remark: If R is an arbitrary ring, the above theorem is still true provided we assume that $f(x)$ is **monic**.

Corollary 1: Let F be a field, and let $f(x) \in F[x], f(x) \neq 0$. If $\deg f(x) = n$, then every coset of $(f(x))$ has a unique representative of the form $r(x)$, with $r(x) = 0$ or $\deg r(x) < n$. Thus every coset in $F[x]/(f(x))$ can be uniquely written as $r(x) + (f(x))$ with $r(x) = 0$ or $\deg r(x) < n$.

Corollary 2 (can also be seen directly): Let F be a field, and let $f(x) \in F[x]$ and $a \in F$. Then there exists a polynomial $q(x)$ such that $f(x) = (x-a)q(x) + f(a)$. In particular, $f(a) = 0 \iff (x-a) \mid f(x)$. (In more abstract language, $\operatorname{Ker} \operatorname{ev}_a = (x-a)$, the principal ideal generated by $x-a$.)

Corollary 3: Let F be a field, and let $f(x) \in F[x], f(x) \neq 0$. If $\deg f(x) = n$, then $f(x)$ has at most n roots in F.

This corollary is still true if we replace $F[x]$ by $R[x]$, where R is an integral domain, but fails if R is a more general ring or R is a division ring.

Theorem (Existence of a primitive root): Let F be a field and let G be a finite subgroup of $(F^*, \cdot)$. Then G is cyclic. In particular, if F is a finite field, then F^* is cyclic.

Examples: $G = (\mathbb{Z}/p\mathbb{Z})^*$, G is the n^{th} roots of unity μ_n in $\mathbb{C}^*$.