MTH 310.002 # Test II Review **Spring 2012**

Absractions versus examples. The purpose of abstraction is to reduce ideas to their essentials, uncluttered by the details of a specific situation. Our lectures built up abstract concepts from concrete examples, but this review will look back the other way.

The Test will focus on quotient rings R/I and their main examples, the modular arithmetic $\mathbb{Z}_n = \mathbb{Z}/(n)$ and the extension field $K = F[x]/(p(x))$.

Rings. Abstract algebra asks: "What is a number system?" Our answer: any set of objects which can be added and multiplied so the usual algebra formulas and manipulations hold. In fact, we need only check the most basic algebra laws (the Axioms), from which all the rest will follow. Formally, a general number system is a *ring*: some set R with some definition of plus and times satisfying: (i) additive closure, (ii) additive associativity, (iii) additive commutativity, (iv) zero element, (v) existence of a negative for any element, (vi) multiplicative closure, (vii) multiplicative associativity, (viii) distributivity of multiplication over addition, (ix) identity element 1.

EXAMPLE: The ring of 2×2 real matrices $R = M_2(\mathbb{R})$ satisfies only these axioms. It is non-commutative, since in general $AB \neq BA$ for two matrices, and it does not have reciprocals, since not every non-zero matrix A has an inverse A^{-1}. However, we can still do some algebra in R: the solution to $AX + B = 0$ is $X = -A^{-1}B$ provided A is invertible.

For number systems with even more of the usual algebra, we require further: (x) mulitiplicative commutativity, which makes a *commutative ring*, or even (xi) existence of a reciprocal a^{-1} for any $a \neq 0$, which makes a *field*.

EXAMPLE: The most basic commutative ring is the integers $\mathbb{Z}$, which is not a field since only the units ± 1 have reciprocals in $\mathbb{Z}$. The most basic fields are the rational numbers (fractions) $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$. In all these fields, almost all algebra is valid, such as the quadratic formula: the solutions to $ax^2 + bx + c = 0$ are $x = \frac{1}{2a}(-b \pm \sqrt{b^2 - 4ac})$, provided there is an element r in our field such that $r^2 = b^2 - 4ac$; otherwise there are no solutions in our field.

Ring constructions. How to find new number systems, especially fields? Several constructions produce larger rings from a given R.

- The ring $M_n(R)$ of $n \times n$ matrices with entries $r_{ij} \in R$, and the usual matrix operations. This is never a field, since it is not commutative.
- Given two (or more) rings R_1, R_2, we can form the product ring $R_1 \times R_2$, the set of all pairs (r_1, r_2) with $r_1 \in R_1$, $r_2 \in R_2$, and operations done on each coordinate individually. This is never a field, since it has zero-divisors $(r_1, 0)$ and $(0, r_2)$.
- The polynomial ring $R[x]$ consists of polynomials of the form $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ with coefficients $a_i \in R$ and the usual operations on functions. If $R = F$ is a field, then $F[x]$ is a commutative ring with no zero-divisors. It is never a field, however, because its only units are constant polynomials $f(x) = c \neq 0$ with $f(x)^{-1} = \frac{1}{c} \in F[x]$.

Quotient rings. Now let R be a commutative ring. To get a field from R, we cut it down by an ideal $I \subset R$. That means we partition R into equivalence classes, subsets of R which each count as a single number in R/I. Each class $[r]$ consists of an element $r \in R$ shifted by all the elements of I:

$$[r] = r + I = \{r + i \text{ for } i \in I\} = \{r' \text{ with } r - r' \in I\}.$$

We say r is a representative of its class, but we could take any other element as a representative: $[r] = [r']$ for any $r' \in [r]$. There is often a special minimal element $r_0 \in [r]$ which we call the *standard form*: $[r] = [r_0]$.

The ring R/I is the set of all such equivalence classes $[r]$, with operations done on representatives: $[r] + [s] = [r + s]$ and $[r][s] = [rs]$. WARNING: The notation $[r][s]$ does *not* mean multiplication of all the elements of $[r]$ and $[s]$. Rather, we take *one* representative of each class, multiply them to get $rs \in R$, then take the class of this rs, namely $[rs] = rs + I$. We must make sure this does not depend on which representatives we choose: if $[r] = [r']$ and $[s] = [s']$, we must have $[r + s] = [r' + s']$ and $[rs] = [r's']$. The properties needed to ensure this are the definition of an ideal.

Formally, an ideal I must have additive closure ($i, j \in I \Rightarrow i + j \in I$) and multiplicative absorption ($i \in I$, $r \in R \Rightarrow ir \in I$). The main examples of ideals are the *principal ideals*, the multiples of a fixed element $r \in R$: we denote $I = (r) = \{rq \text{ for } q \in R\}$.

The larger the ideal I, the smaller and neater the quotient ring R/I. An extreme example is $I = (0) = \{0\}$ with $R/(0) \cong R$. The other extreme is $I = (1) = \{1q \text{ for } q \in R\} = R$ with $R/(1) \cong \{0\}$, a degenerate ring containing only a zero element. A *maximal ideal* is just short of $(1) = R$, meaning the only ideal larger than I is R itself.

I is maximal if and only if R/I is a field. PROOF ($\Rightarrow$) : Let I be maximal. If $[a] \neq [0] \in R/I$, then $a \notin I$ and $I + (a) = \{i + aq \text{ for } i \in I, q \in R\}$ is an ideal bigger than I, so it must be R. In particular $1 \in I + (a)$, meaning $1 = i + aq$ for some $q \in R$. Thus $[1] = [i] + [a][q] = [a][q]$ and $[q] = [a]^{-1} \in R/I$. Hence R/I is a field.

Quotients of the integers. We repeat everything in the previous section for the special case $R = \mathbb{Z}$. To get a finite ring from $\mathbb{Z}$, we cut it down by an ideal I. Here the only ideals are the principal ideals $I = (n) = \{nq \text{ for } q \in \mathbb{Z}\}$, all multiples of a fixed n. The smallest ideal is $I = (0) = \{0\}$, the largest is $I = (1) = \mathbb{Z}$. We have $(a) \subset (b)$ whenever $b \,|\, a$. The maximal ideals are $I = (p)$ where p has no divisors except itself and 1, namely p a prime.

To quotient $R = \mathbb{Z}$ by a given $I = (n)$, we partition $\mathbb{Z}$ into classes. For example, for $I = (3)$, we get the following partition:

$[0] = I$		$[1] = 1 + I$		$[2] = 2 + I$	
0		1		2	
3	-3	4	-2	5	-1
6	-6	7	-5	8	-4
9	-9	10	-8	11	-7
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

$\mathbb{Z}$ is the union of these classes: $\mathbb{Z} = [0] \cup [1] \cup [2]$. Any of the elements in a class produces the same class: $[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$ is the same set as $[7] = \{\ldots, 1, 4, 7, 11, 15, \ldots\}$. The top elements $0, 1, 2$ in each class are the usual standard forms (the nicest representatives), though an equally nice choice would be $0, 1, -1$.

Now we change perspective on the classes: instead of thinking about the many elements inside, we consider each class as a single object, a "number" in $R/I = \mathbb{Z}/(3) = \{[0], [1], [2]\}$. To add or multiply two of these objects, we add or multiply one representative from each, and take the resulting class. For $[2][2]$, we compute $(2)(2) = 4$ and take its class $[4] = [1]$; or equally well take $-1 \in [2]$ and compute $(-1)(-1) = 1$ and take its class $[1]$.

WARNING: This is not the same as multiplying every element in one class by every element in the other: for example $[0][0] = [0] = \{3q \text{ for } q \in \mathbb{Z}\}$, but $(I)(I) = \{(3q)(3q') = 9qq' \text{ for } q, q' \in \mathbb{Z}\}$, a much smaller set.

If p is prime, then $I = (p)$ is a maximal ideal, and $\mathbb{Z}/(p) = \mathbb{Z}_p$ is a field. To compute $[a]^{-1}$: if $[a] \neq [0] \in \mathbb{Z}/(p)$, then $a \notin (p)$ and $p \not| \, a$. In this case $\gcd(a, p) = 1$ and the Euclidean Algorithm allows us to write $as + pt = 1$, so $[a][s] = [1]$ and $[a]^{-1} = [s] \in \mathbb{Z}/(p)$.

Quotients of polynomial rings. For a field F, to get a field extension $K \supset F$, we cut down $R = F[x]$ by an ideal $I = (p(x))$ to get $K = R/I = F[x]/(p(x))$. (Again, the only ideals of $F[x]$ are principal ideals.)

We partition $F[x]$ into classes. For example, For $R = F[x] = \mathbb{Z}_2[x]$ and $I = (p(x)) = (x^2 + x + 1)$, we get the partition:

$[0] = I$	$[1] = 1 + I$	$[x] = x + I$	$[x{+}1] = x{+}1 + I$
0	1	x	$x + 1$
$p(x) = x^2{+}x{+}1$	$1{+}p(x) = x^2{+}x$	$x{+}p(x) = x^2{+}1$	$x{+}1{+}p(x) = x^2$
$xp(x) = x^3{+}x^2{+}x$	$1{+}xp(x) = x^3{+}x^2{+}x{+}1$	$x{+}xp(x) = x^3{+}x^2$	$x{+}1{+}xp(x) = x^3{+}x^2{+}1$
$(x{+}1)p(x) = x^3{+}1$	$1{+}(x{+}1)p(x) = x^3$	$\vdots$	$\vdots$
$\vdots$	$\vdots$		

We know that all polynomials $f(x)$ are in one of these classes because the division algorithm will give $f(x) = p(x)q(x) + r(x)$ with $\deg r(x) < \deg p(x) = 2$, meaning $r(x) = ax + b$; thus $f(x) \in [r(x)] = [ax + b]$. We take the remainder $r(x) = ax + b$ as the standard form in its class, and write $[f(x)] = [ax + b]$. Since $a, b \in \mathbb{Z}_2$, there are $2^2 = 4$ distinct classes. (For a general finite field $\mathbb{Z}_p$ and a general irreducible $p(x)$ of degree n, the standard forms are all polynomials $r(x)$ of degree $\leq n - 1$, and each of their n coefficients can be chosen in $\mathbb{Z}_p$. Hence $|R/I| = |K| = p^n$.)

In the quotient ring $R/I = F[x]/(p(x))$, each "number" is a class $[f(x)]$. We can compute products by multiplying $[f(x)][g(x)] = [f(x)g(x)]$, then reducing $f(x)g(x)$ via division by $p(x)$.

If $p(x)$ is an irreducible polynomial (no factors other than constants c and $c\,p(x)$), then $(p(x))$ is a maximal ideal, and $F[x]/(p(x)) = K$ is a field. We can compute reciprocals $[f(x)]^{-1}$ the same way as for $\mathbb{Z}/(p)$: if $[f(x)] \neq [0]$, then $p(x) \nmid f(x)$. In this case, $\gcd(f(x), p(x)) = 1$, and the Euclidean Algorithm allows us to write $f(x)g(x) + p(x)q(x) = 1$, so $[f(x)][g(x)] = [1]$, and $[f(x)]^{-1} = [g(x)]$.

After we are used to the definition of the field K, we introduce a more practical, compact notation. We write $\alpha = [x]$ and drop the brackets for coefficients, so that $[ax + b] = a\alpha + b$ for $a, b \in \mathbb{Z}_2$. Thus, $K = \{0, 1, \alpha, \alpha{+}1\}$. Since $[x^2 + x + 1] = [0]$, we have $\alpha^2 + \alpha + 1 = 0$, or $\alpha^2 = \alpha + 1$. This relation allows us to compute products without long division, reducing higher powers of α to linear expressions. We still need the Euclidean algorithm to divide, however, by computing $1/(a\alpha + b) = [ax + b]^{-1}$.

For a general irreducible $p(x) \in F[x]$, the field $K = F[x]/(p(x))$ contains a copy of F (namely, the constant polynomials), and also a root $\alpha = [x]$ to the equation

$p(y) = 0$. (Here I have used a new variable y to avoid confusion with the x involved in building K.) EXAMPLE: For $x^2 + 1 \in \mathbb{R}[x]$, we get the field $K = \mathbb{R}[x]/(x^2 + 1)$ is isomorphic to the complex numbers $\mathbb{C}$, since a standard form $a\alpha + b \in K$ corresponds to $b + ai \in \mathbb{C}$, with parallel addition and multiplication resulting from the relations $\alpha^2 = -1 \in K$ and $i^2 = -1 \in \mathbb{C}$.

Ideals and homomorphisms. There is another way to think of "cutting down" a ring R to a smaller ring S: take a surjective homomorphism $\phi : R \to S$. This turns out to be the same as taking a quotient. We have a natural *projection homomorphism* $\pi : R \to R/I$ given by $\pi(r) = [r]$, and any surjective homomorphism is essentially of this form:

THEOREM: Let $\phi : R \to S$ be a surjective homomorphism of rings. Then the kernel $I = \mathrm{Ker}(\phi) = \{r \in R \text{ s.t. } \phi(r) = 0\}$ is an ideal of R, and $R/I \cong S$.

EXAMPLE. Define $\phi : F[x] \to F$ by $f(x) = f(a)$ for a fixed $a \in F$. Clearly ϕ is a surjective homomorphism. Its kernel is $I = \mathrm{Ker}(\phi) = \{f(x) \text{ s.t. } f(a) = 0\}$, an ideal. In fact, the Linear Isomorphism Theorem tells us that $f(a) = 0$ if and only if $x-a$ is a factor of $f(x)$, so that the kernel is the principal ideal $I = (x-a) = \{(x-a)q(x) \text{ for } q(x) \in F[x]\}$. Indeed, we have $F[x]/I = F[x]/(x-a) \cong F$, since the standard forms are just constant polynomials $r(x) = c$.

Exercises

1. Consider the field $\mathbb{Z}_{17} = \mathbb{Z}/(17)$.
   (a) Find the reciprocals $1^{-1}, 2^{-1}, \ldots, 16^{-1} \in \mathbb{Z}_{17}$.
   (b) Make a table of squares in $\mathbb{Z}_{17}$ in reduced form (e.g. $6^2 = 36 = 2$, so $\sqrt{2} = 6 \in \mathbb{Z}_{17}$. Explain the symmetry of this table: it begins 1, 4, 9, ..., and ends ..., 9, 4, 1.
   (c) Solve the equation $2x^2 + 4x + 1 = 0$ for $x \in \mathbb{Z}_{17}$.
2. A field K with 8 elements
   (a) Construct such a field K as an extension field of $\mathbb{Z}_2$. Take an irreducible polyomial $p(x)$ of degree 3, and let $K = \mathbb{Z}_2/(p(x))$. Write the 8 elements as standard forms in the compact notation (α instead of $[x]$, no brackets on coefficients).
   (b) Find the reciprocal of each element in K.

(c) Factor $p(y)$ completely into linear factors in $K[y]$. Hint: One root of $p(y)$ is $y = \alpha$. Check that $y = \alpha^2$ is another root.

3. It is difficult to write down a real solution to $x^3 + x + 1 = 0$. Assuming α is such a solution, consider the ring:

$$K = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \text{ for } a_i \in \mathbb{Q},\ n \geq 0\}.$$

(a) Consider the homomorphism $\phi : \mathbb{Q}[x] \to K$ given by $\phi(f(x)) = f(\alpha)$. Find the kernel of ϕ. Hint: It is clear that $p(x) = x^3 + x + 1 \in \text{Ker}(\phi)$, so the principal ideal $(p(x)) \subset \text{Ker}(\phi)$. Now note that $p(x)$ is irreducible in $\mathbb{Q}[x]$, so $(p(x))$ is a maximal ideal. Could there be any more elements of $\text{Ker}(\phi)$?

(b) Use a theorem to that conclude that $K \cong \mathbb{Q}[x]/(x^3 + x + 1)$, and that K is a field.

(c) Assuming part (b), show that any element of K can be written in the form $a_0 + a_1\alpha + a_2\alpha^2$.

(d) Find the reciprocal $\frac{1}{\beta} = b_0 + b_1\alpha + b_2\alpha^2$ of the element $\beta = 1 + \alpha^2$ by the Euclidean Algorithm applied to $x^2 + 1$ and $x^3 + x + 1$.