COMMUTATIVE ALGEBRA HANDOUT 1: REVIEW OF RING THEORY

JC

1. Basics

A *ring* in this course will be a set R equipped with binary operations $+$ and $\times$ and distinguished elements 0 and 1 (which may be equal) such that

(1) $(R, +)$ is an abelian group with 0 as the identity element.
(2) $\times$ is associative and distributes over $+$.
(3) $\times$ is commutative and has 1 as the identity element.

WARNING: In some algebra courses *rings* just have to satisfy the first two axioms. Our rings are always "commutative rings with 1".

It is easy to see that if $R = \{0\}$ and we let $0 + 0 = 0 \times 0 = 0$ then we have a rather trivial ring, the *zero ring*. The axioms above imply that $a0 = 0$, so $R = \{0\}$ if and only if $1 = 0$.

We write $-a$ for the $+$-inverse of a (which always exists since R is a group under $+$) and when it exists we write a^{-1} for the $\times$-inverse of a. Elements of R with an inverse are called *units*, the set of units is denoted $U(R)$ and forms a group under $\times$. If $a = bu$ for a unit u then a is an *associate* of b, the relation of being associate is an equivalence relation.

2. Homomorphisms, subrings and ideals

Let R and S be rings. A *homomorphism (HM)* from R to S is a function $\phi : R \to S$ such that

$$\phi(r + r') = \phi(r) + \phi(r'), \phi(r \times r') = \phi(r) \times \phi(r'), \phi(0_R) = 0_S, \phi(1_R) = 1_S.$$

If ϕ is bijective then the inverse ϕ^{-1} is automatically a HM from S to R. In this circumstance we say that ϕ is an *isomorphism (IM)*.

WARNING: In some algebra courses HMs may not be required to satisfy the last clause.

Notice that if we forget about multiplication ϕ is a group HM from the group $(R, +)$ to the group $(S, +)$.

Let S be a ring and let $R \subseteq S$. R is a *subring* of S iff R is a subgroup of $(S, +)$, R is closed under $\times$ and $1_S \in R$. This is equivalent to saying that R is a ring under the inherited operations and it has the same 0 and 1. We write $R \leq S$ for this. Notice that if R is a subring of S then the inclusion map is a HM from R to S.

WARNING: In some algebra courses subrings are not required to contain the 1 of the ambient ring.

An *ideal* of a ring R is a set $I \subseteq R$ such that I is a subgroup of $(R, +)$ and for all $r \in R$ and $a \in I$, $ra \in I$. In particular $0 \in I$ for any ideal I, $1 \in I \iff I = R$, and $\{0\}$ and R are always ideals of R.

If $\phi : R \to S$ is a HM then the *kernel of* ϕ is the set of $r \in R$ such that $\phi(r) = 0$. $\ker(\phi)$ is an ideal of R. The image of ϕ is $\{\phi(r) : r \in R\}$. $\mathrm{im}(\phi)$ is a subring of S.

Notice that if $\phi : R \to S$ is a *monomorphism* (injective HM) then ϕ sets up an IM between R and $\mathrm{im}(\phi)$. We sometimes identify R with the subring $\mathrm{im}(\phi)$ of S.

If I is an ideal of R we can form a quotient ring R/I as follows. The elements are the additive cosets $a + I$ of I in R, which makes sense as I is a subgroup of $(R, +)$. We define

$$0 = 0 + I, 1 = 1 + I, (a + I) + (b + I) = (a + b) + I, (a + I)(b + I) = ab + I.$$

It is routine to check that this is well-defined and makes R/I into a ring. Also the map $a \mapsto a + I$ is an *epimorphism* (surjective HM) from R to R/I, this is the *quotient HM* for I.

CENTRAL RESULT: The first isomorphism theorem states that if ϕ is a HM and $I = \ker(\phi)$ then R/I is isomorphic to $\mathrm{im}(\phi)$, with an IM being given explicitly by $a + I \mapsto \phi(a)$. A nice way of looking at this: an arbitrary HM from R to S factors into the surjective quotient HM from R to R/I and the injective map from R/I to S which takes $a + I$ to $\phi(a)$.

CENTRAL RESULT: The ideals of R/I are in a natural 1-1 correspondence with the ideals of R containing I. Explicitly if J is an ideal of R/I then the union of the additive cosets of I comprising J is the corresponding ideal in R. This correspondence respects the inclusion relation between ideals.

3. Special classes of rings and ideals

A ring R is an *integral domain (ID)* iff $1 \neq 0$ and the product of two nonzero elements is always nonzero. It is a *field* iff every nonzero element is a unit. Easily every field is an ID but not vice versa.

An ideal I is *prime* iff $I \neq R$ and the product of two elements in P^c is always in P^c. Easily I is prime iff R/I is an ID.

An ideal I is *maximal* iff $I \neq R$ and for every ideal $J \supseteq I$ either $J = I$ or $J = R$. I is maximal iff R/I is a field

In general if $X \subseteq R$ then (X) is the least ideal containing X and consists of all finite linear combinations $\sum_i r_i x_i$ where $r_i \in R$ and $x_i \in X$ (by convention this includes the empty sum with value 0). Abusing notation $(a) = aR$ is the ideal of all multiples of a, such ideals are called *principal* (NOT *principle*).

R is a *principal ideal domain (PID)* iff it is an ID and every ideal is principal. The most significant examples are of course $\mathbb{Z}$ and $F[x]$ for F a field.

In an ID R we say that r is *irreducible* iff r is a nonzero nonunit and $r = st$ implies that one of s and t is a unit (so of course the other is an associate of r). r is *prime* iff r is a nonzero nonunit and whenever r divides st then either r divides s or r divides t. Easily the associates of an irreducible(resp prime) or also irreducible (resp prime), and prime implies irreducible.

R is a *unique factorisation domain (UFD)* iff it is an ID and every nonzero nonunit has a factorisation as a finite product of irreducibles, unique up to permutation and associates. Every PID is a UFD but not vice versa. In a UFD irreducible equals prime.

In any UFD we have a reasonable notion of *greatest common divisor (gcd)*. Namely given a nonempty set X of nonzero nonunits (to avoid trivialities) say that a is a gcd iff a is a common divisor of X (that is divides all elements of X) and all common divisors divide a. In a UFD gcd's exist and are unique up to associates. In a PID the gcd's of X are precisely those a such that $(X) = (a)$.

4. Field of fractions

If R is an ID then we can construct a field which has R as a subfield. The idea is to start with all pairs (a, b) from R with $b \neq 0$ and quotient out by the equivalence relation which makes (a, b) equivalent to (c, d) iff $ad = bc$. Let a/b be the class of (a, b) and define

$$a/b + c/d = (ad + bc)/bd, a/b \times c/d = ac/bd, 0 = 0/1, 1 = 1/1.$$

If F is the set of classes with these operations then it is routine to check that F is a field and the map $a \mapsto a/1$ is a monomorphism from R to F. We usually identify a with $a/1$ so that R is regarded as a subring of F. Moreover any monomorphism $\phi : R \to G$ where G is a field extends uniquely to a monomorphism $\psi : F \to G$ given by $\psi : a/b \mapsto a \times b^{-1}$.

5. Euclidean domains

If R is an ID a *Euclidean function for* R is a function from R to $\mathbb{N}$ such that if $a, b \in R$ with $b \neq 0$ then there exist $q, r \in R$ so that $a = bq + r$ and either $r = 0$ or $\phi(r) < \phi(b)$. In general q and r need not be unique.

R is a Euclidean domain iff it has a Euclidean function. Every Euclidean domain is a PID. If F is a field then the degree function is a Euclidean function for $F[x]$.