21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

18- Monday October 10, 2011.

Definition 18.1: A *ring* is a set R equipped with operations $+$ and $\times$ (but the sign for multiplication is usually not written), $(R,+)$ being an Abelian group (with identity 0, and the inverse of x being written $-x$), $\times$ being associative (i.e. $(a\,b)\,c = a\,(b\,c)$ for all $a,b,c \in R$), and *distributive* from both sides with respect to $+$ (i.e. $a\,(b+c) = a\,b + a\,c$ and $(a+b)\,c = a\,c + b\,c$ for all $a,b,c \in R$).

A ring is *commutative* if $\times$ is commutative, i.e. $a\,b = b\,a$ for all $a,b \in R$.

A ring is *unital* if it has a 1 (identity for $\times$, assumed $\neq 0$ for the ring not to be reduced to 0), and in this case a *unit* is any element which has an inverse for multiplication; instead of unital ring, one also uses the terms *unit ring* or *ring with identity*.

A non-zero element $a \in R$ is a *zero-divisor* if there exists a non-zero b (also a zero-divisor) such that $a\,b = 0$. A ring R is an *integral domain* if it is commutative, unital with $1 \neq 0$, and has no *zero-divisor*, so that $a\,b = 0$ implies $a = 0$ or $b = 0$.

A *division ring* is a unital ring for which every non-zero element has an inverse for multiplication (so that it has no zero-divisor).

A *field* is a commutative division ring, i.e. an integral domain for which every non-zero element has an inverse for multiplication.

Remark 18.2: When I was a student (in the mis 1960s), being unital was included in the definition of a ring, and what one now calls a division ring was called a field, so that one stated *Wedderburn's theorem* (which should be called *Dickson–Wedderburn theorem*) as "every finite field is commutative",[1] but now that one has added commutativity in the axioms of fields, it is stated as "every finite division ring is a field".

Lemma 18.3: If a finite ring R with more than one element has no zero-divisor, then it is a division ring (hence it is a field by Wedderburn's theorem).
Proof: $R^* = R \setminus \{0\}$ is non-empty, and multiplication on R^* is regular, so that for $a \in R^*$ the mapping $x \mapsto x\,a$ is injective (because $x\,a = y\,a$ implies $(x-y)\,a = 0$, hence $x - y = 0$), but an injective mapping from a finite set into itself is surjective (hence bijective), so that there is a unique element $\ell_a \in R^*$ satisfying $\ell_a a = a$; one deduces that $\ell_a\,a\,b = a\,b$ for all $b \in R^*$, and since $a\,b$ can be any element of R^* one deduces that all ℓ_a coincide, hence there exists a *left-identity* λ such that $\lambda\,r = r$ for all $r \in R^*$ (and it is also true for $r = 0$). Similarly, using the mapping $x \mapsto a\,x$, one finds a unique element $r_a \in R^*$ such that $a\,r_a = a$, and then all r_a coincide, so that there exists a *right-identity* ρ such that $r\,\rho = r$ for all $r \in R^*$ (and it is also true for $r = 0$). Then $\lambda = \rho$, which one then denotes 1, by considering $\lambda\,\rho$, which is ρ because λ is a left-identity, and which is λ because ρ is a right-identity.

By the same argument, every $a \in R^*$ has a left inverse b satisfying $b\,a = 1$ and a right inverse c satisfying $a\,c = 1$, but $b\,a\,c = (b\,a)\,c = 1\,c = c$ and it also is $= b\,(a\,c) = b\,1 = b$, so that every non-zero element has an inverse.

Remark 18.4: Lemma 18.3 is not true for infinite rings, since even for a field F the polynomial ring $F[x]$ will be shown to be an integral domain, and even a PID (principal ideal domain), or even more an Euclidean domain, but not a field, since only the non-zero constants have an inverse in $F[x]$.

For mappings from a set X into itself, with composition as an associative operation and id_X as identity, an element f has a left inverse g (such that $g \circ f = id_X$) if and only if f is injective, and it has a right inverse h (such that $f \circ h = id_X$) if and only if f is surjective. One way of using this idea for creating a ring R such that some elements have many different left inverses or many different right inverses (but not both), is to consider a field F, the vector space $V = F^{\mathbb{N}^\times}$, and $R = L(V;V)$ the ring of all linear mappings from V into itself: the mapping which to $x = (x_1, x_2, \ldots)$ associates $(0, x_1, x_2, \ldots)$ is linear and injective but not

[1] Joseph Henry Maclagan WEDDERBURN, Scottish-born mathematician, 1882–1948. He worked at Princeton University, Princeton, NJ. Wedderburn's theorem is named after him, but since his first "proof" contained a gap (only discovered later) and DICKSON published another proof after, but before WEDDERBURN published two other proofs, it should be named the Dickson–Wedderburn theorem.

surjective and has for left inverses any linear mapping which to $y = (y_1, y_2, \ldots)$ associates $y_1 v + (y_2, y_3, \ldots)$ where $v \in V$ is an arbitrary vector; the mapping which to $x = (x_1, x_2, \ldots)$ associates $(x_2, x_3, \ldots)$ is linear and surjective but not injective and has for right inverses any linear mapping which to $y = (y_1, y_2, \ldots)$ associates $(\ell(y), y_1, y_2, \ldots)$ where ℓ is an arbitrary linear mapping from V into F, i.e. $\ell(y) = \sum_j \lambda_j y_j$ with $\lambda_j \in F$ for all j but only a finite number of λ_j being $\neq 0$.

If in a unital ring an element x has a left inverse y and a right inverse z, i.e. $y\,x = x\,z = 1$, then one has $z = y$, because $y\,x\,z = (y\,x)\,z = 1\,z = z$, and $y\,x\,z = y\,(x\,z) = y\,1 = y$.

Definition 18.5: A *left-ideal* J of a ring R is an additive subgroup of R such that $r\,j \in J$ for all $r \in R$ and all $j \in J$; a *right-ideal* J of a ring R is an additive subgroup of R such that $j\,r \in J$ for all $r \in R$ and all $j \in J$; an *ideal* of R (also called a *two-sided ideal*) is both a left-ideal and a right-ideal.

If J is an ideal of R, then the quotient group R/J has a ring structure, since $(a + j_1)\,(b + j_2) \in a\,b + J$ for all $j_1, j_2 \in J$.

Remark 18.6: Left-ideals or right-ideals are particular subrings of R,[2] but even if R is unital they are not necessarily unital. If R is a unital ring, any left-ideal or right-ideal containing a unit must coincide with R (since it then contains 1), so that if R is a division ring (or a field) the only left-ideals or right-ideals are $\{0\}$ and R.

If R is unital with multiplicative identity 1_R, it may exist a proper ideal J which is also unital with multiplicative identity $1_J \neq 1_R$: for $R = \mathbb{Z}_n$ with $n = m\,k$ and $(m, k) = 1$, let ℓ satisfy $\ell\,m = 1 \pmod{k}$ (so that one may impose that $\ell \in \{1, \ldots, k-1\}$), then $J = \{0, m, \ldots, (k-1)\,m\}$ is an ideal whose product is defined by $(m\,x)\,(m\,y) = m\,z$ with $z = m\,x\,y \pmod{k}$, so that $1_J = \ell\,m$.[3]

If R is unital and J is an ideal, then the quotient ring R/J is unital, with $1_J = 1_R + J$, but if R is not unital, it is possible that a quotient R/J be unital: if $R_0 = \mathbb{Z}_{20}$ and $R = 2R_0$, which is an ideal of R_0 hence a ring, then R is not unital,[4] but if $J = 5R = 10R_0$ (so that $J = \{0, 10\}$), then R/J is isomorphic to $2\mathbb{Z}_{10} = \{0, 2, 4, 6, 8\}$ which has $1_{2\mathbb{Z}_{10}} = 6$.

Definition 18.7: For a subset X of a ring R, the *ideal generated by* X,[5] denoted (X), is the smallest ideal containing X, i.e. the intersection of all ideals containing X (so that $(\emptyset) = \{0\}$). A *finitely generated ideal* is an ideal (X) for a finite set X, a *principal ideal* is any ideal (a) generated by one element.

A ring R is a *principal ideal ring* if every ideal of R is principal; a *principal ideal domain*, abbreviated *PID*, is an integral domain (i.e. a unital ring which is commutative and has no zero-divisor) in which every ideal is principal.

Lemma 18.8: In a ring R, for $a \in A$, one has $(a) = \left\{r\,a + a\,s + n\,a + \sum_{i=1}^m r_i a\,s_i \mid n \in \mathbb{Z}, m \geq 1, r, r_1, \ldots, r_m, s, s_1, \ldots, s_m \in R\right\}$.
Proof: For $n \in \mathbb{N}^\times$ and $r \in R$, $n\,r$ means $r + \ldots + r$ with n terms, and $(-n)\,r$ means $n\,(-r)$, so that although R may not be unital (so that $1 + \ldots + 1$ does not make sense), $n\,r \in R$ and one checks that the distributivity implies that for all $r, s \in R$ and $m, n \in \mathbb{Z}$ one has $(m\,r)\,(n\,s) = (m\,n)\,(r\,s)$. If J is an ideal containing a, it then contains terms like $r\,a, a\,s, n\,a, r\,a\,s$ for $r, s \in R$ and $n \in \mathbb{Z}$, hence it contains $J_a = \left\{r\,a + a\,s + n\,a + \sum_{i=1}^m r_i a\,s_i \mid n \in \mathbb{Z}, m \geq 1, r, r_1, \ldots, r_m, s, s_1, \ldots, s_m \in R\right\}$. On the other hand, J_a is a subgroup, and for any $\rho \in R$ and $x \in J_a$ one has $\rho\,x \in J_a$ and $x\,\rho \in J_a$, so that J_a is an ideal, which is then the smallest ideal containing a.

Remark 18.9: If R is a commutative unital ring, one then has $(a) = \{r\,a \mid r \in R\}$, and more generally $(a_1, \ldots, a_m) = \left\{\sum_{i=1}^m r_i a_i \mid r_1, \ldots, r_m \in R\right\}$.

---

[2] It is important here not to impose a unit for multiplication in the definition of a ring. Actually, it is a simple way to construct rings which are not unital: in $\mathbb{Z}$ (which is an integral domain), the ideals have the form $n\,\mathbb{Z}$ for $n \in \mathbb{N}$, and for $n \geq 2$ the ring $n\,\mathbb{Z}$ is not unital.

[3] For example, in $\mathbb{Z}_{10}$, $J = \{0, 2, 4, 6, 8\}$ and $1_J = 6$.

[4] Since 1_R would be $2a$ for some a, with the property that $2a \cdot 2x = 2x \pmod{20}$ for all x, which is false for x odd.

[5] One could as well consider the smallest left-ideal containing X, or the smallest right-ideal containing X: they exist, since any intersection of left-ideals is a left-ideal and any intersection of right-ideals is a right-ideal.