MAT3004: Coding Theory
Rings

A (commutative) *ring* R is a set R together with operations of addition and multiplication on R, that is, given a, $b \in R$ there are elements $a+b$, $ab \in R$, satisfying the following conditions:

A1 $a+b=b+a$ for all a, $b \in R$. (The commutative law for addition.)

A2 $(a+b)+c=a+(b+c)$ for all a, b, $c \in R$. (The associative law for addition.)

A3 There is an element $0 \in R$ such that $a+0=a$ for all $a \in R$. (There is an additive identity.)

A4 For each $a \in R$ there is an element $-a \in R$ with $a+(-a)=0$. (There exist additive inverses.)

M1 $ab=ba$ for all a, $b \in R$. (The commutative law for multiplication.)

M2 $(ab)c=a(bc)$ for all a, b, $c \in R$. (The associative law for multiplication.)

M3 There is an element $1 \in R$ such that $1a=a$ for all $a \in R$. (There is a multiplicative identity.)

D $a(b+c)=ab+ac$ for all a, b, $c \in R$. (The distributive law.)

A *field* is a (commutative) ring in which each nonzero element has a *reciprocal*. That is: if $a \neq 0$ there is $b \in R$ with $ab=1$ (in this case we write a^{-1} for b).

RJC 11/2/2001