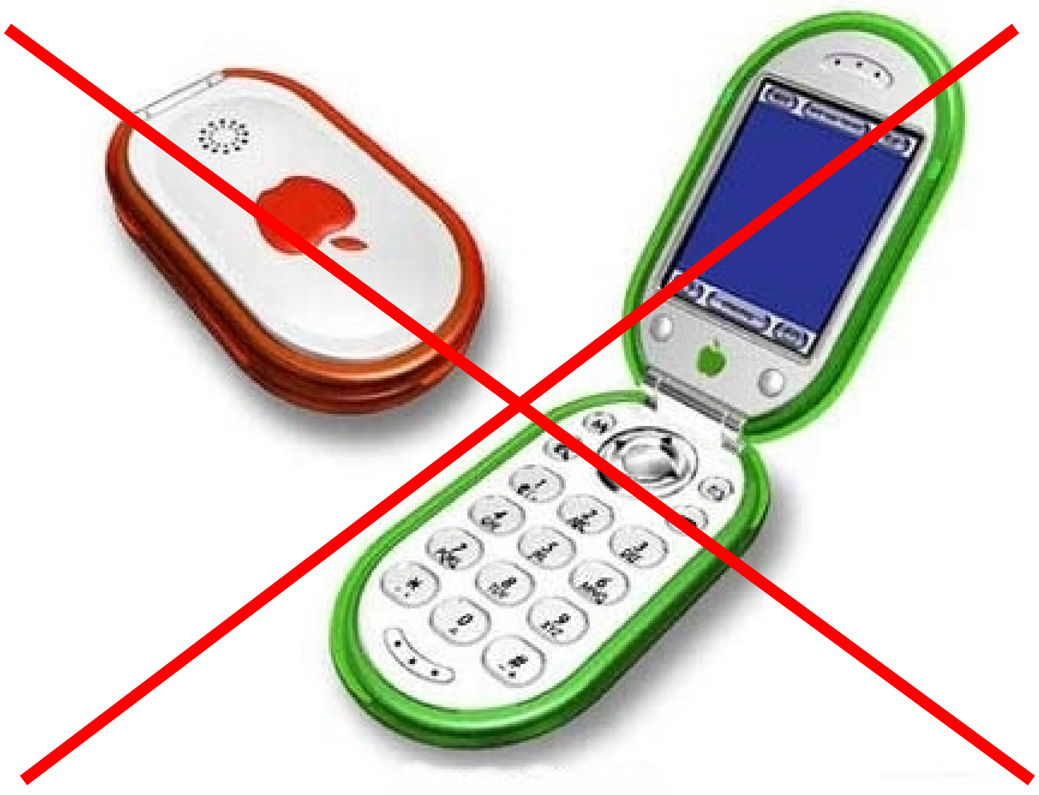
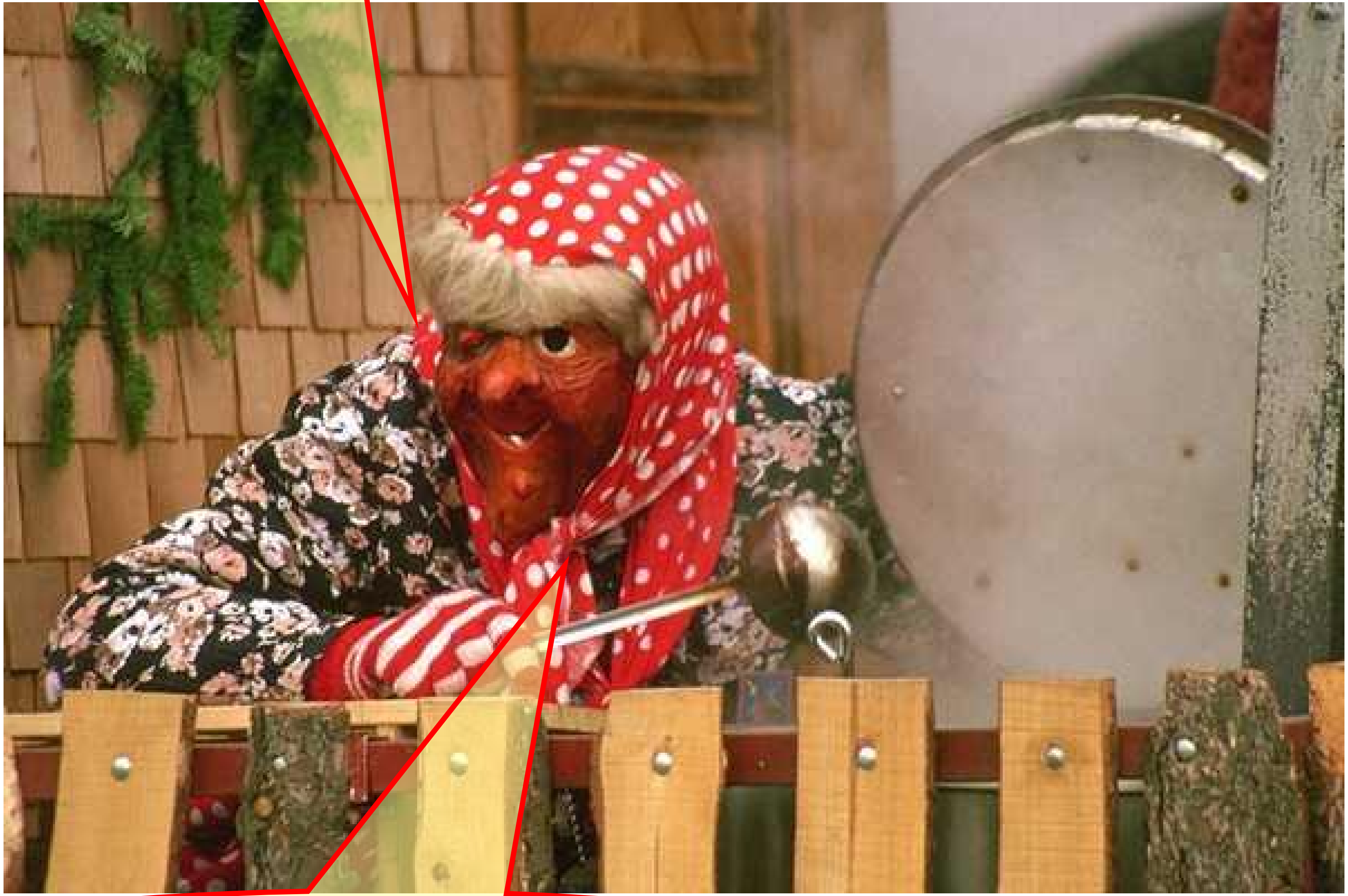
In our classes,

all the mobile phones should be switched off !



上课啦！



The class is begin!

.

第三章 环和域

.

群是有一个代数运算的代数系统　但是，我们在数学特别是在高等代数中，遇到过很重要的讨论对象，例如，数、多项式、函数以及矩阵和线性变换等，都有两个代数运算，　这一事实说明，在近世代数中研究有两个代数运算的代数系统，也具有非常重要的现实意义。在有两个代数运算的代数系统中，最基本最重要的就是环与域。

这一部分主要介绍环与域的定义和初步性质，以及一些常见的重要的环与域。

第 16 讲

第 三 章　环与域

§1　环的定义与性质　(2课时)

本讲的教学目的和要求:

本讲开始在群论的基础上讨论具有两个二元运算的代数体系—环的基本性质. 环也是近世代数中一类重要的、基本的代数体系. 由于它具有两个二元运算, 所以不可避免地会涉及到在群论中没有接触的概念. 在群的讨论中, 无论在思考问题, 提出问题

的基本想法,还是在分析问题、解决问题的主要手法方面，对于近世代数来说，都具有普遍的典型的意义。可以说基本上体现了近世代数研究问题的格调与模式。这些对于环的讨论会有重要的启发和借鉴作用。

本讲主要介绍环的概念—环的主要特性及它与群的联系和区别。在教学还将引出一批环的类别以及讨论环在两个运算方面所具有的基本性质。由于是刚刚引入一种新的代数体系，所以受到内容的限制，这一讲中不会碰到什么难点。但重点是要弄清楚环这种代数体系中两种运算的谐调关系。

一、环的定义及例子

定义 1　设 $<R,+,\cdot>$

(1)　$<R,+>$ 是一个加群；

(2)　$<R,\cdot>$ 是一个半群；

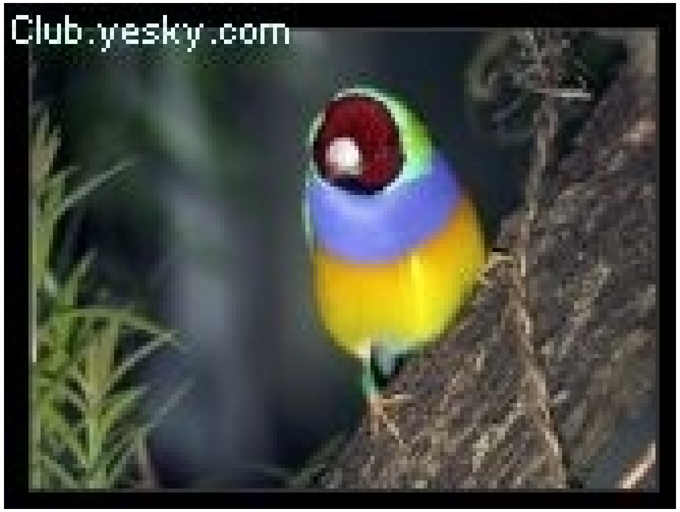
(3) R

$$a(b+c)=ab+ac \qquad (b+c)a=ba+ca.$$

$\forall a,b,c \in R$

那么称$<R,+,\cdot>$

R



注意 1：

1、乘法的说明

与群的运算类似，当进行乘法运算对 $a \cdot b$ 时，乘法运算的符号通常省略不写．即将 $a \cdot b$ 记作 ab.

2、分配律的说明

这两个分配律分别称为左分配律与右分配律.

3、 上定义中说到$\{R;+\}$ $\{R;+\}$

$\forall a \in R$ a $a - a$

$\{R;\cdot\}$ R

例 1 $< R,+,\cdot >$ Z

Z $< R,+,\cdot >$

Z

.

同理有理数集 Q、实数集 R 对通常的数的加法和乘法构成环，分别称为有理数环和实数环，复数集 C 对通常的复数的加法和乘法构成环，称为复数环。

我们通常把由数集构成的环称为数环.

例2 偶数集$2Z=\{\cdots,-6,-4,-2,0,2,4,6,\cdots\}$

例3 设$Z[i]=\{a+bi\mid\forall a,b\in Z\}$

例 4 任取定一个数域F F

$$F[x]=\{a_n x^n + a_{n-1}x^{n-1} + \square + a_1 x + a_0 \mid a_i \in F, n \in Z, n \geq 0\}$$

这个环$<F[x],+,\cdot>$ x

.

实际上，在例 4 中，若将数域F

Z

$$Z[x]=\{b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0 \mid b_i\in Z, n\in Z, n\geq 0\}$$

例 5　取出数域F　　n

$$M_n(F)=\{A=(a_{ij}) \mid a_{ij}\in F, 1\leq i,j\leq n\}$$

$< M_n(F),+,\cdot >$　n　n

.

在例 5 中, 若用数环替代数域F

$$F$$

$$M_n(2Z)=\{A=(a_{ij})\mid a_{ij}\in 2Z,1\le i,j\le n\}$$

.

例 6 在第二章里, 我们曾讨论模m

$< Z_m,+ > Z_m = \{[0],[1],\square ,[m-1]\}$ Z_m

为使Z_m Z_m

$$[i]\cdot[j]=[i\cdot j]$$

显然, 这里也采用了 “钟表计数法” . 试证明

$< Z_m,+,\cdot >$

.

证　（1）由第一章知，剩余类的加法是Z_m

$$<Z_m,+>$$

$$[i]\cdot[j]=[i\cdot j] \qquad Z_m$$

假设$i'\in[i], j'\in[j]$ $\qquad [i'[=[i],[j']=[j]$

$$[i']\cdot[j']=[i'\cdot j']$$

.

（1），（2）两式的左端是相等的，即

$$[i']\cdot[j']=[i]\cdot[j]$$

如果它们的右端不一样，就有

$$[i']\cdot[j']\neq[i]\cdot[j]$$

那么，规则“ •”就不是$\bar{Z}_m$

$\bar{Z}_m$