MATH H113: Honors Introduction to Abstract Algebra

2016-03-07

- Rings
- Matrix rings
- Polynomial rings

For Wednesday:
Read Sect. 7.2

Homework due Friday:

- Sect. 6.3 (p. 221): 11, 14
- Sect. 7.1 (p. 231): 6, 11, 12, 28
- Sect. 7.2 (p. 238): 2, 9, 12

For 6.3.14: $G_p = \langle u, v | u^p = v^3 = 1, vu = u^a v \rangle$. $a \in \mathbb{Z}$ is such that $\bar{a}$ has order 3 in $(\mathbb{Z}/p\mathbb{Z})^\times$
For 7.2.9: Simplify your answers

Definition: Let R be a ring with a 1.

a. Let $u \in R$. An *inverse* of u is an element $r \in R$ such that $uv = vu = 1$ (two-sided inverse).
b. A *unit* in R is an element that has an inverse (the inverse is unique because if v' is another inverse, then $v' = 1v' = vuv' = v1 = v$).
c. The set of units in R is written $R^\times$, and is a group under the multiplication operation of R.

Examples: $(\mathbb{Z}/m\mathbb{Z})^\times$, $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$, $M_n(\mathbb{R})^\times = GL_n(\mathbb{R})$

Definition: A *division ring* is a ring with $1 \neq 0$ such that every nonzero element is a unit. Example of a noncommutative division ring: the quaternions $= \{a + bi + cj + dka, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1\}$, $ij = k$, $ji = -k$, etc. as in the definition of Q_8.

Definition: A *field* is a commutative division ring (this is equivalent to the def. on p. 34).

Definition: Let R be a ring. A *zero divisor* in R is an element $a \in R$ such that $a \neq 0$ and $ab = 0$ or $ba = 0$ for some $b \neq 0$ in R.
Example: In $M_2(\mathbb{R})$ $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a zero divisor, because $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} =$

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Can an element of a ring be both a zero divisor and a unit? *No.* If u is a unit with inverse v, and $ub = 0$, then $b = vub = 0$, so $b = 0$. Likewise $bu = 0 \implies b = b1 = buv = 0$, so $b = 0$.
Can a nonzero element of a ring be *neither* a unit nor a zero divisor? Yes: $2 \in \mathbb{Z}$.

Definition: A ring is *entire* if:

i. it is commutative
ii. it has $1 \neq 0$, and
iii. it has no zero divisors

An entire ring is also called an *integral domain* (older terminology) (prefer adjectives to nouns).

Examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, or any field.

Definition: A *subring* of a ring R is a subset S of R that is a ring under the addition and multiplication operations inherited from R.
Equivalently: it's an additve subgroup of R that is closed under multiplication *or* it's a nonempty subset of R that is closed under subtraction and multiplication.

Examples:

1. $2\mathbb{Z} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
2. Let R_1 and R_2 be a rings. Then the *direct product* $R_1 \times R_2$ of R_1 and R_2 is the cartesian product $R_1 \times R_2$ (as a set) with component wise addition and multiplication. This is a ring. Then $R_2 \times \{0\}$ and $\{0\} \times R_2$ are subringsof $R_1 \times R_2$. If R_1 and R_2 have 1, then so do $R_1 \times R_2$, $R_1 \times \{0\}$, and $\{0\} \times R_2$.

But their identity element are not the same.
The identity element of $R_1 \times R_2$ is $(1, 1)$
the identity element of $R_1 \times \{0\}$ is $(1, 0)$
the identity element of $\{0\} \times R_2$ is $(0, 1)$

Proposition: Let F be a field. If R is a subgring of F that contains the unity element of F, then R is entire.
Proof: On your homework.
There's also a converse: envery entire ring is isomorphic to a subring of a field containg its identity elemtent. *Later.*

Note: In an entire ring R, you can cancel multiplication by nonzero elements: if $x \in \mathbb{R}$ and $x \neq 0$, then $xa = xb \implies a = b$
Proof: $x(a - b) = 0 \implies a - b = 0$.
More generally: In any ring, if x is $\neq 0$ and not a zero divisor, then $xa = xb \implies a = b$ and $ax = bx \implies a = b$ (same proof(s)).

Matrix rings

Defininition: Let R be a ring and let $n \in \mathbb{Z}_{>0}$. Then $M_n(R)$ is the set of $n \times n$ matrices with entries in R. It is a ring, under the usual addition and multiplication (the (i,k) entry of AB is $\sum_{j=1}^{n} a_{ij}b_{jk}$) operations on matrices.

Note: If R is not commutative, then the theory of determinants won't work.

If R has 1 then so does $M_n(R)$. If S is a subgring of R, then $M_n(S)$ is a subring of $M_n(R)$.
Example: $M_n(2\mathbb{Z}) \subseteq M_n(\mathbb{Z}) \subseteq M_n(\mathbb{Q}) \subseteq \ldots$
Note: $M_n(\mathbb{Z})^\times = \{A \in M_n(\mathbb{Z}) : \det A \in \{\pm 1\}\}$.

- "$\supseteq$" us formula for A^{-1} using minors
- "$\subseteq$" if B is an inverse of A then $(\det B)(\det A) = 1$, so $\det A \in \{\pm 1\}$.

Polynomial Rings

Let R be a commutative ring with 1. **Definition**: An *indeterminate* over R is a variable that you're not saying what it is.
So it satisfies no relation other than $x + a = a + x$, $xa = ax$ $\forall a \in R$ (it acts like a generator of a free group).

Definition: The ring $R[x]$ is the set of all polynomials in x with coefficients in R. These look like $p(x) = \sum_{i=1}^{n} a_i x^i = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ with $a_i \in R$ $\forall i$. Such polynomials can be added an multiplied using the usual rules of polynomials. This forms a ring. We think of R as a subring of $R[x]$: the constant polynomials. Also we think of x as an element of $R[x]$: $x = 1x$.
Other definitions (see book): degree of p, leading term, leading coefficient