Math Club Notes: 2005 May 2

1 Boolean rings

In 228 we learned that a *Boolean ring* is a ring in which $x^2 = x$ for all x.

(We showed that such a ring is commutative. First, $x = x^2 = (-x)^2 = -x$. We also have $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$. Subtracting $x + y$ and rearranging yields $xy = -yx$, and since $-yx = yx$, we're done.)

The only example of a Boolean ring that we saw in class was $\mathbb{Z}_2$ (and, implicitly, direct sums such as $\mathbb{Z}_2 \oplus \mathbb{Z}_2$).

Another example: Take the set $S = \{F, T\}$, meaning "false" and "true" respectively. Define the operation $\veebar$, called "exclusive or" ("xor" to its friends), as follows:

$$p \veebar q = \begin{cases} T & \text{if one of } p \text{ or } q \text{ is true, but not both,} \\ F & \text{otherwise.} \end{cases}$$

Define also the operation $\wedge$, called "and", by

$$p \wedge q = \begin{cases} T & \text{if both } p \text{ and } q \text{ are true,} \\ F & \text{otherwise.} \end{cases}$$

Then $(S, \veebar, \wedge)$ is a Boolean ring.

If you write out the addition and multiplication tables for $(S, \veebar, \wedge)$, you'll see that they're the same as those for $\mathbb{Z}_2$, except that they have F instead of 0 and T instead of 1. That is, $(S, \veebar, \wedge)$ is isomorphic to $\mathbb{Z}_2$.

Another example: let T be the set of all subsets of $\mathbb{Z}$. Define on T the operations

$$A \triangle B = \{x \mid x \in A \veebar x \in B\}$$
$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

These are called, respectively, the symmetric difference and the intersection of A and B. $(T, \triangle, \cap)$ is a Boolean ring. (The simplest proof builds directly from the previous example.)

These examples make sense of the name — Boole was big in symbolic logic and set theory.

Question: Must a Boolean ring have unity?

2 An isomorphism

In 228 we looked at the field

$$\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}.$$

This field is isomorphic to the set of matrices

$$\left\{ \begin{bmatrix} a & 5b \\ b & a \end{bmatrix} \;\middle|\; a, b \in \mathbb{Q} \right\}.$$

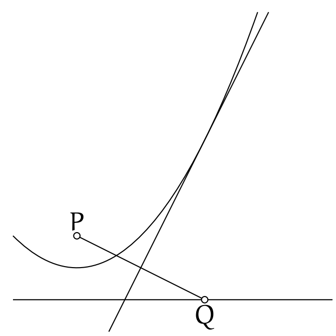
Can you come up with a similar isomorphism for the field

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}\,?$$

3 Parabola tangents

Given a point and a line, the set of points equidistant from that point and that line is called a parabola. (It is understood that distance to the line means perpendicular distance.) The point is called the focus of the parabola; the line is called its directrix.

Take a parabola with focus P. Choose any point Q on its directrix. Then the perpendicular bisector of PQ is tangent to the parabola.



Two facts are needed for the proof. First, that every point on the perpendicular bisector of PQ is equidistant from P and Q. Second, that the perpendicular dropped from a point to a line is the shortest of all segments from that point to that line.

First show that the perpendicular bisector does intersect the parabola. Erect a perpendicular to the directrix at Q; it will intersect the perpendicular bisector of PQ somewhere, say, at S. Then use the first fact above to show that S is on the parabola.

Second, show that no other point on the perpendicular bisector of PQ is on the parabola. Take some other point S' and drop a perpendicular from S' to the directrix. For S' to be on the parabola, we'd need that segment to be congruent to PS'. But PS' is congruent to QS' by the first fact above, so this is impossible by the second fact above.

(Erratum: The above argument establishes only that the line in question has exactly one point in common with the parabola. Alas, lines parallel to the axis of the parabola have one point in common but are not tangents. How can the proof be repaired?)