Mathematics 412

Final preview
14 March 2003

As usual, clarity of exposition is as important as correctness of mathematics.

1. Two miscellaneous questions:

   (a) A friend says, "I've proved that $3x^4+7x+25$ can't be factored as a product of lower degree polynomials with integer coefficients. I've been trying next to factor $3x^4+7x+25$ as a product of lower degree polynomials with rational coefficients. I haven't succeeded. Should I keep trying, or is there a reason why I can't do this?" How do you answer your friend?

   (b) Another friend says, "I've been thinking about the ring $\mathbb{Q}[x]/(x^5-2)$. I know that I can write the elements of this ring in the form $a_0+a_1\gamma+a_2\gamma^2+a_3\gamma^3+a_4\gamma^4$, where each a_i is in $\mathbb{Q}$ and where γ satisfies the 're-write rule' $\gamma^5=2$. I also know that x^5-2 is irreducible in $\mathbb{Q}[x]$, and so $\mathbb{Q}[x]/(x^5-2)$ is actually a field: every nonzero element has a multiplicative inverse. So what is the multiplicative inverse of γ? What is the multiplicative inverse of $1+\gamma$?"

2. Consider the polynomial x^2+3x+1. In each of the rings below, either explain why it is irreducible in that ring, or factor it as a product of irreducible polynomials.

   (a) $\mathbb{Q}[x]$

   (b) $\mathbb{R}[x]$

   (c) $\mathbb{F}_{11}[x]$

3. Let F be a field.

   (a) Suppose that $m(x)$ and $u(x)$ are non-zero polynomials in $F[x]$ and you wish to divide $m(x)$ into $u(x)$. State what the Division Theorem tells you about this situation. You should make an explicit statement about the existence of certain polynomials.

   (b) Suppose that $a(x)$ and $m(x)$ are relatively prime polynomials in $F[x]$. Bezout's Theorem guarantees the existence of polynomials $u(x)$ and $v(x)$ in $F[x]$ such that

   $$a(x)u(x)+m(x)v(x)=1.$$

   Given this, prove that there exist polynomials $r(x)$ and $s(x)$ in $F[x]$, with $\deg r(x) < \deg m(x)$, so that

   $$a(x)r(x)+m(x)s(x)=1.$$

4. In this problem, we will consider polynomials in $\mathbb{F}_3[x]$.

   (a) Prove that the polynomial x^3-x-1 has no root in $\mathbb{F}_3[x]$. Using this, explain why x^3-x-1 is irreducible in $\mathbb{F}_3[x]$.

(b) Construct a ring K that contains $\mathbb{F}_3$, has an element γ satisfying $\gamma^3 = \gamma + 1$, and has exactly 27 elements. Describe explicitly what the elements of K are, describe what the product of any two elements of K is, and explain why K has 27 elements.

(c) Using the strengthened version of Bezout's theorem obtained in Problem 3(b), prove that K is a field; that is, prove that each non-zero element of K has a multiplicative inverse in K. Conclude that you have constructed a field larger than $\mathbb{F}_3$ in which $x^3 - x - 1$ has a root.

5. Suppose that R is a ring with no zero-divisors. Recall that an element a of R is called *irreducible* if a is not zero or a unit in R, and if, for any factorization of a in R as a product rs, either r or s is a unit.

   Suppose that R has a measure of size assigning to each element r in R a non-negative integer $N(r)$, and suppose that the measure of size satisfies the following properties.

   - The zero element of R has size 0; any non-zero element of R has positive size.
   - The smallest size any non-zero element of R has is 3, and the elements of R of size 3 are precisely the units of R.
   - The second smallest size any non-zero element of R has is 5, and each element of R of size 5 is irreducible.
   - For any two non-zero elements r and s of R, the inequality $N(r) \leq N(rs)$ holds. Moreover, if s is not a unit, then $N(r) < N(rs)$.

   Given this, prove that every element a of R that is not zero or a unit in R is either irreducible or a product of irreducible elements of R.

6. Let p be a prime number and suppose that a and b are integers such that $a^2 + b^2 = p$.

   (a) Prove that the Gaussian integer $a + bi$ is irreducible in $\mathbb{Z}[i]$.

   (b) Factor p in $\mathbb{Z}[i]$ as a product of irreducible Gaussian integers, and explain why the factors in your factorization are irreducible.

   (c) Let p be the prime number 1021, which happens to satisfy the equation

   $$11^2 + 30^2 = 1021.$$

   Describe 8 pairs of integers (a, b) that satisfy

   $$a^2 + b^2 = 1021.$$

   (d) State what the unique factorization theorem for $\mathbb{Z}[i]$ says about the possible factorizations of 1021 in $\mathbb{Z}[i]$ as a product of irreducible Gaussian integers. Using this, explain why the eight pairs of integers (a, b) that you found in (c) are the only pairs that satisfy $a^2 + b^2 = 1021$.