REU APPRENTICE CLASS #7

INSTRUCTOR: LÁSZLÓ BABAI
SCRIBE: DANIEL SCHÄPPI

Thursday, July 7, 2011

1. Characteristic of fields

Definition 1.1. Let F be a field, and let $a \in F$. The *additive order* of a is the smallest integer $n > 0$ such that

$$na = \underbrace{a + \ldots + a}_{n \text{ times}}$$

is equal to 0. If no such integer exists, the additive order of a is ∞.

In $\mathbb{F}_p$, the field of integers modulo p, the additive order of 1 is obviously p. The same is true for $\mathbb{F}_p[i]$, the "field of complex numbers modulo p," so this gives examples where the additive order of 1 is different from the order of the field. In $\mathbb{Q}$ and $\mathbb{R}$, the additive order of any nonzero element is infinite. On the other hand, 0 has additive order 1 in any in any field F.

Problem 65. Prove the **prime property** (without using the fundamental theorem of arithmetic): if p is a prime number, $a, b \in \mathbb{Z}$, then $p \mid ab$ implies $p \mid a$ or $p \mid b$. (Hint: use Problem 72.)

The following exercise follows from Problem 65 by induction on ℓ.

Exercise 1.2. Let p be a prime. If $p \mid a_1 \cdot \ldots \cdot a_\ell$, then $(\exists i)(p \mid a_i)$.

Theorem 1.3 (Uniqueness of prime factorizations)**.** *Let $n \in \mathbb{N}$, and suppose that there are primes $p_1, \ldots p_k$ and $q_1, \ldots, q_\ell$ such that $n = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_\ell$. Then $k = \ell$ and there exists a permutation $\sigma \in S_k$ such that $p_{\sigma(i)} = q_i$ for all $i = 1, \ldots, k$.*

Proof. This is proved by induction on n. The inductive step relies on Exercise 1.2. □

Theorem 1.4. *The additive order of any two nonzero elements of a field is the same.*

Proof. If there is a nonzero element a with additive order n, we can multiply $a + \cdot \ldots + a$ by ba^{-1} to show that any other element b has additive order at most n. □

Theorem 1.5. *Let F be a field such that 1 has finite additive order. Then the additive order of 1 is prime.*

Definition 1.6. The *characteristic* $\mathrm{char}(F)$ of a field F is 0 if all nonzero elements have infinite additive order, and is p if all nonzero elements have additive order p. We say a field has *finite characteristic* if $\mathrm{char}(F) = p > 0$.

Problem 66. Find an infinite field of finite characteristic.

Problem 67. (a) If $\mathrm{char}(F) = 0$, then $F \supseteq \mathbb{Q}$.
(b) If $\mathrm{char}(F) = p > 0$, then $F \supseteq \mathbb{F}_p$.

We developed linear algebra over number fields only, but we could equally well have worked over an arbitrary field.

Exercise 1.7. Suppose $F \subseteq H$ is a subfield. Then the field H is a vector space over F. In particular, if $\dim_F(H) = n$, then $H \cong F^n$ as a vector space over F.

Theorem 1.8. *If F is a finite field, then $|F|$ is a prime power.*

We can use Exercise 1.7 to give an alternative proof of the "First Miracle of Linear Algebra" in the case of a vector spaces over a *finite field*, by using a simple counting argument: if F has q elements and V is n-dimensional, then V has q^n elements.

The finite fields $\mathbb{F}_q$ are also denoted by $\mathrm{GF}(q)$, where G stands for "Galois." Évariste Galois (1811-1832) introduced the notion of groups, introduced fields, studied the the abstract property of "solvability" of groups; studied the group of symmetries of an equation over a field, defined as a group of permutations of the roots (the "Galois group of the equation"), proved (over "Galois fields") that an equation is solvable in radicals if and only if its Galois group is solvable; discovered all finite fields and the linear groups over those fields, and used them to study permutation groups - created abstract algebra, in brief. He died at the age of 20.

2. Polynomials vs. polynomial functions

We can define abstract polynomials over any field, for example, $\mathbb{F}_q$:

$$\mathbb{F}_q[x] = \{a_0 + a_1x + \ldots + a_nx^n \mid a_i \in \mathbb{F}_q\}$$

Two such polynomials $f = \sum a_ix^i$ and $g = \sum b_ix^i$ are equal if their corresponding coefficients are equal, that is, if $a_i = b_i$ for all i. To each polynomial f we can associate a *polynomial function* $\widetilde{f}\colon \mathbb{F}_q \to \mathbb{F}_q$, given by $\alpha \mapsto f(\alpha)$. We have $\widetilde{f} = \widetilde{g}$ if and only if $(\forall\alpha \in \mathbb{F}_q)\big(f(\alpha) = g(\alpha)\big)$. Is it true that two polynomials are equal if and only if their associated polynomial functions are the same? Clearly not: there are infinitely many polynomials, but the number of functions $\mathbb{F}_q \to \mathbb{F}_q$ is only q^q. In order to give explicit examples of different polynomials with the same associated function we use some basic group theory.

Problem 68 (Lagrange's Theorem)**.** Let G be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$.

Problem 69. Let G be a group. Prove that for any $a \in G$, $\mathrm{ord}(a) = |\langle a\rangle|$.

Corollary 2.1. *Let G be a group and $a \in G$. Then $a^{|G|} = 1$.*

Applying this to $\mathbb{F}_q^\times$, we find that for all $a \in \mathbb{F}_q^\times$, the equation $a^{q-1} = 1$ holds. Thus $a^q = a$ for all $a \in \mathbb{F}_q$, which shows that the polynomial functions of x^q and x are equal. Thus the implication $\widetilde{f} = \widetilde{g} \Rightarrow f = g$ is false for finite fields.

Problem 70. Prove: if F is an infinite field, then two polynomials over F are equal if and only if the corresponding polynomial functions are equal.

3. Arithmetic of integers and polynomials

Definition 3.1 (Divisibility)**.** For $a, b \in \mathbb{Z}$ we say that a divides b, denoted by $a \mid b$, if $(\exists x \in \mathbb{Z})(b = xa)$.

Note in particular that $0 \mid 0$.

Definition 3.2. We say that $d \in \mathbb{Z}$ is a greatest common divisor of $a, b \in \mathbb{Z}$ if:

(1) it is a common divisor, i.e., $d \mid a$ and $d \mid b$.
(2) if d' is a common divisor, then $d' \mid d$.

For example, 16 and 28 have greatest common divisors 4 and -4. In the partial order of divisibility, 0 is the largest: $(\forall x)(x \mid 0)$.

Exercise 3.3. Show that the greatest common divisor is unique up to sign.

Notation 3.4. We write $\gcd(a, b)$ for the positive greatest common divisor of a and b.

Note that with the above definition it is no longer evident that any two numbers must have a greatest common divisor.

Problem 71. Prove from first principles (without using the fundamental theorem of arithmetic) that for all $a, b \in \mathbb{Z}$, there exists a greatest common divisor d, and that there exist $x, y \in \mathbb{Z}$ such that the equation

$$d = ax + by$$

holds. (Hint: it suffices to show that there is a linear combination of a and b which is a common divisor of a and b.)

Problem 72. Use Problem 71 to show that $\gcd(ac, bc) = |c| \gcd(a, b)$.

If F is a field, then $F[x]$ is a commutative ring with an identity element. It makes sense to define divisibility and greatest common divisors in any ring.

Definition 3.5. Let F be a field and let $f, g \in F[x]$. We say that f divides g if $(\exists h \in F[x])(g = hf)$.

Note that for integers, $a \mid 1$ implies that $a = 1$ or $a = -1$. For polynomials we have $f \mid 1$ if and only if f is a nonzero constant polynomial, i.e., if and only if $\deg(f) = 1$. These are precisely the invertible elements in the ring $F[x]$. For example, we have $(x + 1) \mid (x^2 - 1)$, and $7(x + 1) \mid (x^2 - 1)$ if $\mathrm{char}(F) \neq 7$.

Problem 73. Show that Problem 71 also holds for polynomials over a field.