ALGEBRAIC NUMBER THEORY

ISHAN LEVY

1. Basic Facts

Theorem 1.1 (Chevalley-Warning). *Suppose that K is a* $\operatorname{char} p$ *finite field, and $f_i \in K[x_1, \ldots, x_n]$ where $\sum \deg f_i < n$. Then the number of common solutions to $f_i = 0$ is $0 \pmod p$.*

Proof. Note that $\sum_{x \in K} x^i$ is 0 unless $q-1|i \neq 0$. Now look at the characteristic function $g = \prod f_i^{q-1}$. It suffices to show $p| \sum_{x \in K} g$ but this follows from our note and the assumption about degrees. □

In particular this implies that finite fields are quasi-algebraically closed or C_1 fields, which means that for any homogeneous non-constant polynomial in n variables of degree d has a nontrivial solution if $d < n$. C_k is defined similarly except with $d^k < n$.

Lemma 1.2. *If G is a group that is the union of subgroups H_1, H_1, then $H_1 \subset H_2$ or $H_2 \subset H_1$.*

Proof. If the conclusion doesn't hold, then let $a \in H_1 - H_2, b \in H_2 - H_1$. ab can be in neither, so $H_1 \cup H_2 \neq G$. □

Lemma 1.3. *If V is an F-vector space that is the union of n proper affine subspaces V_i, then F is finite, and $n \geq |F|$. If the V_i are subspaces, then $n > |F|$.*

Proof. We can consider a subspace spanned by at least one vector not in each V_i, reducing to the finite-dimensional case. Now suppose F is infinite. We take one of the V_i of the form $\sum c_i x_i = d$ and choose a value b so that $\sum c_i x_i = b$ is not covered by a single V_i. Then we can intersect with this affine plane and induct. Thus F is finite. The other statements follow from counting elements. □

Theorem 1.4 (Primitive Element). *A finite separable field extension K/F is simple.*

Proof. WLOG the field is infinite. For each pair of distinct embeddings $\sigma_i, \sigma_j : K \hookrightarrow \bar{K}$, we can consider the proper F subspace of K of x such that $\sigma_i(x) = \sigma_j(x)$. Then by Lemma 1.3, there are elements not in any of these subspaces, which are primitive. □