

Math 581

Basic Background Results

Below are some basic results from algebra dealing with fields and polynomial rings which will be handy to recall in 581. This should be a reasonably logical ordering, so that a result here should depend only on previous lemmas, propositions, and/or theorems together with facts from ring theory you should already know. Some relevant definitions are also given here. You should be able to provide proofs of all these results (with the exception of Zorn's Lemma) from your classwork in 520 and towering intellect. For our purposes here, a "ring" is understood to be a commutative integral domain with an identity element. Obviously, you should know what these words mean. The labeling of these results is perhaps somewhat arbitrary.

Stuff on Polynomial Rings

Definition: Let R be a ring and let $f \in R[X]$ be an element of the polynomial ring. Write f uniquely as $a_0 + a_1X + \cdots + a_nX^n$ where either $a_n \neq 0$ or $f = 0$. The *degree* of f is n in the former case, and $-\infty$ in the latter.

Lemma 1: Let $f, g \in R[X]$. Then the degree of fg is equal to the sum of the degree of f and the degree of g (using the usual "rules" for addition with $-\infty$).

Theorem 1 (the division algorithm): Suppose F is a field. Given $f, g \in F[X]$ with $g \neq 0$, there are $q, r \in F[X]$ (the *quotient* and *remainder*, respectively) satisfying $f = qg + r$ and the degree of r is less than the degree of g .

Definition: A ring R is a *Euclidean domain* if there is a function d taking $R \setminus \{0\}$ to the non-negative integers such that:

1. $d(a) \leq d(ab)$ for any non-zero $a, b \in R$; and
2. for any non-zero $a, b \in R$, there exist $q, r \in R$ with $a = qb + r$ and either $d(r) < d(b)$ or $r = 0$.

Corollary 1: The ring $F[X]$ is a Euclidean domain whenever F is a field.

Definition: An ideal $I \subseteq R$ of the form aR for some $a \in R$ is called a *principal ideal*. If all ideals of R are principal, then R is called a *principal ideal domain*.

Theorem 2: The ring $F[X]$ is a principal ideal domain whenever F is a field.

(You can take this as a corollary of **Corollary 1** if you like, or prove it using from first principles and Theorem 1.)

Definition: An element $a \in R$ is a *unit* if it is invertible, i.e., $ab = 1$ for some $b \in R$.

Definition: An element $a \in R$ is *irreducible* if it is not a unit and whenever $a = bc$, then one of b or c is a

unit.

Definition: A ring R is a *unique factorization domain* if any non-zero element is either a unit or a finite product of irreducible elements, and this decomposition is unique up to the order of the irreducible elements and the presence of units.

Definition: If R is a unique factorization domain and $f \in R[X]$, the *content* of f is the greatest common divisor of the coefficients of f . Further, f is called *primitive* if its content is 1.

Lemma 2: If R is a unique factorization domain, then the product of two primitive polynomials in $R[X]$ is primitive.

Lemma 3: If R is a unique factorization domain, then the content of the product of two polynomials in $R[X]$ is the product of their respective contents.

Lemma 4: If R is a unique factorization domain with quotient field F and $f \in R[X]$ is both primitive and irreducible, then it is irreducible as an element of $F[X]$.

Lemma 5: If R is a unique factorization domain and $f \in R[X]$ is primitive, then it can be factored uniquely into a product of irreducible elements of $R[X]$.

Theorem 3: If R is a unique factorization domain, then so is the ring $R[X]$.

Stuff on Fields

Definition: A *partial order* on a non-empty set S is a binary relation on S which is reflexive, anti-symmetric, and transitive. Typically, one uses the notation \leq for a partial order. A partial order in which any two elements are related is called a *linear order*. A *chain* in a partially ordered set is a linearly ordered subset. A *maximal element* of a partially ordered set S is an element $a \in S$ such that, whenever $b \in S$ is related to a , then $b \leq a$.

Zorn's Lemma: Let S be a partially ordered set. Suppose for all chains \mathcal{C} in S , there is a $b \in S$ with $c \leq b$ for all $c \in \mathcal{C}$. Then S has a maximal element.

Corollary 1: Every vector space has a basis.

Corollary 2: Every non-trivial proper ideal in a commutative ring is contained in a maximal ideal.

Result (I don't know what to call this): Let F be a field and suppose $P(X) \in F[X]$ is irreducible. Then the quotient ring $F[X]/(P(X))$ is a field which contains (an isomorphic image of) F and a root of P .

Lemma 0: Let $F \subseteq K$ be fields. Then K is a vector space over F .

Lemma 1: Let R be a commutative ring with identity containing a field K . Let $a \in R$. Then there is a unique ring homomorphism $\phi: K[X] \rightarrow R$ with $\phi(X) = a$ and $\phi(u) = u$ for all $u \in K$.

Lemma 2: Let $F \subseteq K$ be fields and regard $F[X]$ as a subring of $K[X]$. If $f, g \in F[X]$ are relatively prime

in $F[X]$, then they are relatively prime in $K[X]$.

Lemma 3: Let $F \subseteq K$ be fields. Let $P, Q \in F[X]$ be irreducible and suppose $\alpha \in K$ is a root of both P and Q . Then $Q = aP$ for some $a \in F$.

Definition: Let $F \subseteq K$ be fields. An element $\alpha \in K$ is called *algebraic over F* if $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ is a linearly dependent set for some $n > 0$, considered as a subset of the vector space K over F . The field K is called an *algebraic extension of F* if every element of K is algebraic over F . An element $\alpha \in K$ which is not algebraic over F is called *transcendental over F* .

Lemma 4: An element α is algebraic over F iff α is a root of some irreducible $P \in F[X]$.

Proposition 1: Let K be a field. The following are equivalent:

- i) if α is algebraic over K , then $\alpha \in K$;
- ii) if $P \in K[X]$ is irreducible, then the degree of P is 1;
- iii) if $f \in K[X]$, then f has a root in K .

Definition: A field satisfying the three equivalent statements in the proposition above is called *algebraically closed*.

Theorem 1a: If F is a field, there is some algebraically closed field K containing (an isomorphic copy of) F .

Definition: Let $F \subseteq K$ be fields with K algebraically closed. An *algebraic closure* of F in K is a field $\bar{F} \subseteq K$ that is algebraically closed and algebraic over F .

Proposition 2: Let α be algebraic over F . Let

$$F[\alpha] = \{a_0 + a_1\alpha + \dots + a_m\alpha^m : a_i \in F \text{ for all } i, \text{ and } m \geq 0\}.$$

Then $F[\alpha]$ is a field containing F and α . It is the smallest such field and its dimension over F is finite.

Lemma 5: If α is algebraic over F and β is algebraic over $F[\alpha]$, then β is algebraic over F .

Proposition 3: If K an algebraic extension of F and α is algebraic over K , then $K[\alpha]$ is an algebraic extension of F .

Theorem 2b: If $F \subseteq K$ are fields and K is algebraically closed, then there is an algebraic closure of F in K .

Proposition 4: Let L and K be fields with K algebraically closed. Suppose there is a monomorphism $\phi: L \rightarrow K$. If α is algebraic over L , then ϕ “lifts” to a homomorphism $\bar{\phi}: L[\alpha] \rightarrow K$ with $\bar{\phi} = \phi$ on L . Further, if $P \in L[X]$ is irreducible with α as a root and $\beta \in K$ is any root of $\phi(P)$ in K , then such a $\bar{\phi}$ is given by $\bar{\phi}(\alpha) = \beta$.

Proposition 5: Let F and K be fields with K algebraically closed. Suppose L is an algebraic extension of F and $\phi: F \rightarrow K$ is a monomorphism. Then ϕ lifts to a monomorphism $\phi_L: L \rightarrow K$ with $\phi_L = \phi$ on F .

Theorem 1c: Any two algebraic closures of a field F are isomorphic via an isomorphism that fixes the elements of F .

Definition: Let F be a field. An *extension* of F is any field K which contains (an isomorphic image of) F . The *degree of K over F* , also called the *index of F in K* , is the cardinality of any basis for K as a vector space over F . This will be written $[K : F]$.

Note: As it stands, we have only shown that this definition makes sense for extensions of finite degree. That will suffice for what we need here, though it is true that this definition always makes sense; specifically, any two bases of a vector space have the same cardinality.

Lemma 6: Let $F \subseteq L \subseteq K$ be fields. Then $[K : F] = [K : L][L : F]$.

Definition: Let K be an extension of F and $\alpha \in K$. Then $F(\alpha)$ is the smallest subfield of K that contains F and α . If α is algebraic over F , the *degree of α over F* is the degree of $F(\alpha)$ over F .

Lemma 7: If α is algebraic over F , then $F(\alpha) = F[\alpha]$ and the degree of α over F is finite; α is a root of a unique monic irreducible $P \in F[X]$ of degree equal to the degree of α .

Definition: Let K be an algebraically closed extension of F and let $f \in F[X]$. The *splitting field of f in K* is the smallest subfield of K containing F and all the roots of f in K , in other words, the smallest subfield L of K containing F for which $f \in L[X]$ factors into a product of linear polynomials (we say f *splits* in $L[X]$).

Proposition 6: Let F be a field and $f \in F[X]$. Let \bar{F}_1 and \bar{F}_2 be algebraic closures of F . If $\phi: \bar{F}_1 \rightarrow \bar{F}_2$ is an isomorphism fixing the elements of F , then ϕ takes the splitting field of f in \bar{F}_1 isomorphically to the splitting field of f in \bar{F}_2 .

Lemma 8: Let F be a field and $f \in F[X]$. If the degree of f is n , then the degree over F of any splitting field of f is no larger than $n!$.

Definition: If α is algebraic over F , α is called *separable over F* if α is a root of a polynomial $f \in F[X]$ with distinct roots in a splitting field (i.e., the number of distinct roots equals the degree of f). An extension K of F is called *separable over F* if every element of K is separable over F . A field is called *perfect* if every algebraic extension is separable.

Definition: The *formal derivative*, f' , of $f(X) = a_0 + a_1X + \dots + a_nX^n \in F[X]$ is given by

$$f'(X) = a_1 + 2_F a_2 X + \dots + n_F a_n X^{n-1} \in F[X],$$

where $i_F \in F$ is the sum of the multiplicative identity 1_F with itself i times:

$$i_F = \underbrace{1_F + \dots + 1_F}_{i \text{ times}}.$$

Lemma 9: The formal derivative satisfies the usual constant multiple, sum, and product rules for derivatives.

Proposition 7: Let $P \in F[X]$ be irreducible and suppose $\text{char}(F) = 0$. If the degree of P is n , then P has n distinct roots in any splitting field of P over F . In particular, any field of characteristic 0 is perfect.

Theorem 2a: If F is a finite field, then $|F| = p^n$ for some $n > 0$ and some prime p . The non-zero elements of F form a cyclic group of order $p^n - 1$ and F is a splitting field for $X^{p^n} - X$ over $\mathbb{Z}/p\mathbb{Z}$.

Theorem 2b: If p is a prime and $n > 0$, then there is exactly one field (up to isomorphism) with p^n elements.

Theorem 2c: Any finite field is perfect.

Definition: An extension K of F is called *simple* if $K = F(\alpha)$ for some $\alpha \in K$. If K is a simple extension of F , a *primitive element* of K is an element $\alpha \in K$ with $K = F(\alpha)$.

Primitive Element Theorem: If K is a finite separable extension of F , then it is a simple extension of F .

Lemma 10: Let K be a splitting field over F and let $P \in F[X]$ be irreducible. If K contains a root of P , then P splits in $K[X]$.

Definition: Let K be an extension of F . The *Galois group of K over F* is the set of automorphisms of K that leave F fixed. We write $G(K, F)$ for this set. If $f \in F[X]$, the Galois group of f is $G(K, F)$, where K is any splitting field of f over F .

Note: The Galois group really is a group under composition of functions. The Galois group is well-defined (up to isomorphism) for any $f \in F$ by **Proposition 5**. If $\alpha, \beta \in K$ are roots of an irreducible $P \in F[X]$, then there is a $\sigma \in G(K, F)$ with $\sigma(\alpha) = \beta$ by **Proposition 3** and **Proposition 4**, provided that K is a finite extension of F . Further, if $\alpha \in K$ is a root of $f \in F[X]$ and $\sigma \in G(K, F)$, then $\sigma(\alpha)$ is a root of f .

Lemma 11: If K is a finite simple extension of F , then $|G(K, F)| \leq [K : F]$.

Note: **Lemma 11** is true for arbitrary finite extensions.

Proposition 8: If K is a finite separable extension of F , then $|G(K, F)| = [K : F]$ iff K is a splitting field for some $f \in F[X]$ over F .

Definition: If K is an extension of F and $H < G(K, F)$, the *fixed field of H* is the subfield of K consisting of all $\alpha \in K$ which are fixed by all elements of H . We will write K_H for this fixed field.

Proposition 9: Let K be a finite separable extension of F and let $H < G(K, F)$. Then $|H| = [K : K_H]$ and $H = G(K, K_H)$.

Definition: An extension K of F is a *Galois extension* if $K_{G(K, F)} = F$. An algebraic extension K is a *normal extension* if whenever $f \in F[X]$ and K contains a root of f , then f splits in $K[X]$.

Theorem 3: Let K be a finite separable extension of F . Then the following are equivalent:

- i) K is a Galois extension of F ;
- ii) K is a normal extension of F ;
- iii) K is a splitting field of some $f \in F[X]$;

iv) $[K : F] = |G(K, F)|$;

v) if L is any extension of K and $\sigma \in G(L, F)$, then $\sigma(K) = K$.

Lemma 12: If K is an algebraic Galois extension of F , then K is a separable extension of F .

The Fundamental Theorem of Galois Theory: Let K be a finite Galois extension of F .

i) For any $H < G(K, F)$, $H = G(K, K_H)$.

ii) For any intermediate field L , $L = K_{G(K, L)}$.

iii) The correspondence $H \longrightarrow K_H$ is a one-to-one correspondence between the subgroups of $G(K, F)$ and the subfields between K and F .

iv) Under this correspondence, the normal subgroups of $G(K, F)$ correspond to the normal extensions of F contained in K , and if L is such an extension, then

$$G(L, F) \cong G(K, F)/G(K, L).$$

Eisenstein's Criterion: Let $P(X) = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$ and suppose there is a prime p with $p|a_i$ for $i = 0, \dots, n-1$, $p \nmid a_n$, and $p^2 \nmid a_0$. Then $P \in \mathbb{Q}[X]$ is irreducible.