Odds and Ends

1. Gauss' Lemma.

Definition. Let R be a UFD. We say that $f \in R[x]$ is *primitive* if the gcd of its coefficients is 1.

Lemma. If R is a UFD, the product of two primitive polynomials $f, g \in R[x]$ is also primitive.

Proof. Suppose not, and some prime p divides all the coefficients of fg. Then in $(R/\langle p\rangle)[x]$ we have that $\bar{f}\bar{g} = 0$, where $\bar{f}$ and $\bar{g}$ are the images of f and g in $(R/\langle p\rangle)[x]$. But $(R/\langle p\rangle)[x]$ is a domain, so either $\bar{f} = 0$ or $\bar{g} = 0$, so either p divides all the coefficients of f or all the coefficients of g, so either f is not primitive or g is not primitive. □

Corollary. Let R be a UFD and let Q be its field of fractions. If a polynomial $f \in R[x]$ factorises as $f = gh$ in $Q[x]$, then it also factors as $f = g_1h_1$ in $R[x]$, with factors that are Q-multiples of the original factors: $g_1 = ag$ and $h_1 = a^{-1}h$, with $a \in Q$.

Proof. Without loss of generality f is primitive, or else, divide f and g by the gcd of the coefficients of f. Find $a, b \in Q$ such that $g_1 = ag$ and $h_1 = bh$ are in $R[x]$ and are primitive and note that $abf = (ag)(bh)$ is primitive by Gauss' lemma. Also, abf is a multiple of f and f is primitive. It follows that $f = abf$ (up to a unit, which can be swallowed by either a or b to make the equality strict). So $ab = 1$, so $b = a^{-1}$, so $g_1 = ag$ and $h_1 = a^{-1}h$. □

2. Eisenstein's Criterion.

Theorem (Eisenstein). If R is a UFD and Q is its field of fractions, $f = \sum_{k=0}^{n} a_k x^k \in R[x]$ is a polynomial with coefficients in R, $p \in R$ is a prime, and $p \nmid a_n$, $p \mid a_{n-1}, \dots, a_0$, and $p^2 \nmid a_0$, then f is irreducible in $Q[x]$.

Proof. Suppose not. By the previous corollary we can assume that $f = gh$ where $g = \sum b_i x^i$ and $h = \sum c_j x^j$ are both in $R[x]$ and are of positive degrees (or else they'd be units in $Q[x]$). Comparing the constant terms in $f = gh$ and noting that p divides a_0 exactly once, we find that p divides exactly one of b_0 and c_0. Without loss of generality, $p \mid b_0$ yet $p \nmid c_0$. By induction, $p \mid b_k$ for all $k < n$. Indeed, suppose $p \mid b_0, \dots, b_{k-1}$, then $p \mid a_k - \sum_{j=0}^{k-1} b_j c_{k-j} = b_k c_0$, and as $p \nmid c_0$, we have that $p \mid b_k$. So p divides the coefficient of the leading term of g (whose degree is less than n), and so it divides the coefficient of the leading term of $f = gh$. But that contradicts the assumption that $p \nmid a_n$. □

3. GCDs are Absolute.

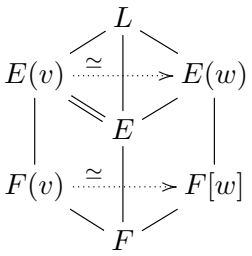
Proposition. Given a field extension E/F, if $a, b \in F[x]$ then $\gcd_E(a, b) = \gcd_F(a, b)$.

Proof. Let $g_F := \gcd_F(a, b)$. Clearly $g_F \mid a$ and $g_F \mid b$ in $F[x]$ and hence in $E[x]$. Also, there exists $s, t \in F[x]$ such that $g_F = sa + tb$, so anything that divides a and b (in $E[x]$ or anywhere else) also divides g_F. So g_F satisfies the definition of a greatest common divisor in $E[x]$, and so $g_F = \gcd_E(a, b)$. □

4. Splitting Fields are Absolute.

Lemma (compare with Hungerford's Theorem 10.15 on page 355). If E is a splitting field of some polynomial f over F and some irreducible polynomial $p \in F[x]$ has a root v in E, then p splits in E.

Proof. Let L be a splitting field of p over E. We need to show that if w is a root of p in L, then $w \in E$ (so all the roots of p are in E and hence p splits in E). Consider the two extensions



$$E = E(v)/F(v) \quad \text{and} \quad E(w)/F(w).$$

The "smaller fields" $F(v)$ and $F(w)$ in these two extensions are isomorphic as they both arise by adding a root of the same irreducible polynomial p to the base field F. The "larger fields" $E = E(v)$ and $E(w)$ in these two extensions are both the splitting fields of the same polynomial f over the respective "small fields", as E is obtained from F by adding all the roots of f, and so $E(v)$ and $E(w)$ are obtained from $F(v)$ and $F(w)$ by adding those same roots. Thus by the uniqueness of splitting extensions, the isomorphism between $F(v)$ and $F(w)$ extends to an isomorphism between $E = E(v)$ and $E(w)$, and in particular these two fields are isomorphic and so $[E : F] = [E(v) : F] = [E(w) : F]$. Since all the degrees involved are finite it follows from the last equality that $E(w) = E$. Therefore $w \in E$. □

Theorem. A finite extension E/F is a splitting extension iff whenever an irreducible $p \in F[x]$ has a root in E, it fully splits in E.

Proof. The $\Rightarrow$ side is the previous lemma. For $\Leftarrow$, if $E = F(\{\alpha_i : 1 \le i \le n\})$, then $f = \prod_i \mathrm{minpoly}_F(\alpha_i)$ fully splits in E and all the α_i's are roots of f. So E is a splitting field of f. □

5. The Primitive Element Theorem.

In this section all fields are of characteristic 0.

Weird Lemma. If λ is the only common root of two polynomials f, g in the splitting field of fg, then λ is a member of the smallest field E generated by the coefficients of f and g.

Proof. $\gcd(f,g) = (x-\lambda)^k$ is in $E[x]$. So $x^k + k\lambda x^{k-1} + \ldots$ is in $E[x]$, so $k\lambda \in E$, so $\lambda \in E$ as $\operatorname{char} E = 0$. □

Theorem. If E/F is a finite extension, then there is some $\gamma \in E$ such that $E = F(\gamma)$ (γ is called "a primitive element" for the extension E/F).

Proof. It's enough to show that whenever $\alpha, \beta \in E$ then there is $\gamma \in E$ such that $F(\alpha,\beta) = F(\gamma)$. Let $f, g \in F[x]$ be polynomials such that $f(\alpha) = g(\beta) = 0$, and let $\alpha = \alpha_1, \ldots, \alpha_n$ and $\beta = \beta_1, \ldots, \beta_m$ be all the roots of f and g respectively in some splitting field of fg.

The Lucky Case. If the gaps $\alpha_i - \alpha_j$ between the roots of f are all different from the gaps $\beta_i - \beta_j$ between the roots of g, shift g by $\gamma = \beta - \alpha$; namely set $h(x) = g(x+\beta-\alpha) = g(x+\gamma) \in F(\gamma)[x]$. Now f and h have exactly one root in common, α. So by the lemma, α belongs to the field generated by the coefficients of f and of h, so $\alpha \in F(\gamma)$ and also $\beta = \alpha + \gamma \in F(\gamma)$. We also have that $\gamma = \beta - \alpha \in F(\alpha,\beta)$, so $F(\alpha,\beta) = F(\gamma)$.

The General Case. F is infinite, so we can find $0 \neq c \in F$ such that after rescaling, we are in the lucky case. Namely, find $0 \neq c \in F$ such that $\{\alpha_i - \alpha_j\} \cap \{c(\beta_i - \beta_j)\} = \emptyset$, set $g_c(x) \coloneqq g(c^{-1}x)$, and use the lucky case to find γ such that $F(\gamma) = F(\alpha, c\beta) = F(\alpha,\beta)$. □

Confession. I would have never found this proof alone and that deeply annoys me. One way to learn how to do research in mathematics is to try to understand definitions and proofs not only at the bare minimum level, but at the level where you think, "that's exactly what I would have done myself". With the Primitive Element Theorem, I still fail.