Math 129 HW 2

Bryden Cais

February 18, 2002

1 Minimal Polynomials Over Domains

1. We have the following implications:

   (a) $b \longrightarrow a$: Suppose that $P = ST$ is reducible with $\deg(S) < \deg(P)$. Then since R is a domain and $P(x) = 0$, we must have $S(x) = 0$, say, without loss of generality. Now let $T' \neq T$ be any monic polynomial of the same degree as T (clearly this is possible.) Then $P' = ST'$ has x as a root, is monic, and is of the same degree as P. Thus P is not unique.

   (b) $c \longrightarrow b$: Suppose that P is not unique. Then there exists a monic P' of minimal degree d with x as a root. Thus, $Q := P - P'$ is a polynomial of degree at most $d-1$ not identically zero (not necessarily monic) with $Q(x) = 0$. This shows that there is a linear dependence among $B = \{1, x, \cdots, x^{d-1}\}$ so that B is not an R-basis of $R[x]$.

   (c) $d \longrightarrow c$: It is clear that $B = \{1, x, \cdots, x^{d-1}\}$ spans $R[x]$. To show linear independence, suppose that we have some linear dependence in the form $Q(x) = 0$ with $\deg(Q) < d$. Then by d, we must have $P|Q$, which is impossible since P is of degree d.

   (d) $e \longrightarrow d$: Let $Q \in R[X]$ satisfy $Q(x) = 0$. Then $\varphi(Q) = 0$, so that $Q \in \ker(\varphi.)$ Since $\varphi : R[X]/(P) \longrightarrow R[x]$ is an isomorphism, $\ker(\varphi) = (P)$ and hence $Q \in (P)$, or what is the same, $P|Q$.

   (e) $d \longrightarrow e$: Suppose $Q \in R[X]$ and that $\varphi(Q) = 0$. Then by d, $P|Q$ and hence $Q \in (P)$. Thus, $\ker(\varphi) \subset (P)$. Trivially, $(P) \subset \ker(\varphi)$, so that $\ker(\varphi) = (P)$, and φ induces an isomorphism $R[X]/(P) \longrightarrow R[x]$ by the first isomorphism theorem.

2.

3. Suppose that R is integrally closed.

   (a) Let P be some monic irreducible polynomial in $R[X]$. Since P is irreducible, $R[X]/(P) := A$ is a domain containing R and a root x of P. By item 2, since R is integrally closed, a-f of item 1 hold for A, x. Now let Q be monic of minimal degree with $Q(x) = 0$.

Then by e, $Q|P$, which implies that $P = Q$ since P is monic and irreducible. Thus, by f, we have that P is prime, and hence that any monic irreducible polynimial is also prime.

(b) $R[X]$ is an integral domain since R is. Further, the process of factorization of an element $P \in R[X]$ terminates. To see this, proceed as follows: If P is irreducible, we are done. Otherwise, $P = P_1 P_2$ for some monic $P_1,\ P_2$ each of degree strictly less than P. Thus, by induction on the degree of P we see that factorization must terminate since all monic degree one polynimials are irreducible. Now we appeal to the following fact: If D is an integral domain in which the process of factorization into irreducibles terminates, then D is a UFD if and only if every irreducible element is prime. (See Artin's Algebra, pg. 395). Clearly, each factor in the unique factorization of P is monic and ireducible.

(c) The existence of the gcd and lcm of any two monic polynomials now follows easily. The gcd of $S,\ T$ is defined as $\prod_P P^{\min(v_P(T), v_P(S))}$, while the lcm is $\prod_P P^{\max(v_P(T), v_P(S))}$, where $v_P(Q)$ is the exponent of the irreducible factor P in the unique decomposition of Q, and the products above are over all irreducible elements of $R[X]$. Note that the uniqueness of factorization makes the valuation $v_P(Q)$ well defined, and hence our definitions of gcd and lcm are good.

(d) We know that the BEZOUT property holds in a domain D if and only if D is principal. However, we only know that $R[X]$ is a UFD, and is not necessarily principal. Thus BEZOUT does not necessarily hold.

2 Galois

We know that $\mathrm{Aut}(L)|dim_{\mathbf{Q}L}$, and since $K_1,\ K_2$ must be subfields of L, we see that $dim_{\mathbf{Q}}(L)$ is divisible by 3 and is at most 9. Moreover, we have the following well known fact: If K_1 and K_2 are galois extensions with galois groups $G,\ H$ respectively, then $\mathrm{Gal}(K_1K_2)$ injects into $G \times H$ and is isomorphic to the group $\{(\sigma,\tau) \in G \times H\}$ where $\sigma,\ \tau$ agree on the intersection of $K_1,\ K_2$. Now if $K_1,\ K_2$ are both degree three extensions then their intersection is either trivial or the all of $K_1K_2 = K_1 = K_2$. If the intersection is trivial (that is, only $\mathbf{Q}$) then the galois group of the composite is $G \times H$. This gives rise to extensions of degree $3,\ 9$. The only way to obtain a degree 6 extension is as follows: If both $K_1,\ K_2$ are galois, then we are in the above situation. If only one is galois, then we obtain a degree 9 extension with automorphism group of size 3. Thus, both extensions $K_1,\ K_2$ must not be galois. If there is no automorphism sending K_1 to K_2 then we obtain a degree 9 extension with automorphism group of size 3. If there is some non trivial automorphism sending K_1 to K_2 then the composite field has one nontrivial automorphism. By the brimitive element theorem, we may write $K_i = \mathbf{Q}(\alpha_i)$ for $i = 1, 2$. Since there is some automorphism sending

K_1 to K_2, we see that α_1, α_2 are roots of the same minimal polynomial. Since this polynomial is cubic, the extension given by the composite K_1K_2 is galois and of size bigger than 3 since K_1 and K_2 are not equal. However, it cannot be a degree 9 extension since K_2 cannot have degree 3 over K_1 (because of the nontrivial automorphism), so that it is a degree 6 extension with galois group S_3. This discussion shows that the possible values for the pair $(dim_{\mathbf{Q}}L, \mathrm{Aut}(L))$ are $(3,1),\ (3,3),\ (6,6),\ (9,1),\ (9,3),\ (9,9)$. Below are some examples:

1. $(3,1)$: Let $K_1 = K_2 = \mathbf{Q}(\sqrt[3]{2})$. Then clearly $L = K_1K_2 = K_1$, and we have the values stated.

2. $(3,3)$: Let $K_1 = K_2 = \mathbf{Q}(\eta)$, where $\eta = e^{2\pi i/9} + e^{-2\pi i/9}$ is a root of the irreducible polynomial $P = X^3 - 3X + 1$. Then since the other two roots of P are $\eta^2 - 2,\ 2 - \eta - \eta^2$, we see that K_1K_2 is a degree 3 galois extension of $\mathbf{Q}$, which gives the claimed pair.

3. $(6,6)$: Let $K_1 = \mathbf{Q}(\sqrt[3]{[2]}),\ K_2 = \mathbf{Q}(\omega\sqrt[3]{2})$. Then K_1K_2 is the splitting field of $x^3 - 2$ and is hence a degree 6 extension with galois group of size 6.

4. $(9,1)$: Let $K_1 = \mathbf{Q}(\sqrt[3]{2}),\ K_2 = \mathbf{Q}(\sqrt[3]{3})$. Then K_1K_2 is a degree 9 extension (since $\sqrt[3]{3} \notin K_1$) with trivial automorphism group.

5. $(9,3)$: Let $K_1 = \mathbf{Q}(\sqrt[3]{2}),\ K_2 = \mathbf{Q}(\eta)$. Then K_1K_2 is a degree 9 extension (since $\sqrt[3]{2} \notin K_2$) with automorphism group of size three (each automorphism sends η to another root of its minimal polynomial while fixing $\sqrt[3]{2}$.

6. $(9,1)$: Let $\zeta = e^{2\pi i/26}$ be a 26^{th} root of unity. Then the three roots of the polynomial $x^3 - x^2 - 4x - 1$ are $\rho_1 = \zeta + \zeta^{-1} + \zeta^5 + \zeta^{-5},\ \rho_2 = \phi(\rho_1),\ \rho_3 = \phi(\rho_2)$, where ϕ is the automorphism of $\mathbf{Q}(\zeta)$ sending ζ to ζ^7. Further, the discriminant of the above polynomial is 169, so that it has galois group C_3. Let $K_1 = \mathbf{Q}(\rho_1)$ and $K_2 = \mathbf{Q}(\eta)$. Clearly, $K_1,\ K_2$ intersect only in $\mathbf{Q}$ (since 26, 9 are relatively prime,) so that the above discussion tells us that the extension K_1K_2 is of degree 9 with galois group $C_3 \times C_3$, of size 9 as claimed.

3 Quadratic Extensions

1. $d = 0$. The element $X \in \mathbf{Z}[X]/X^2$ is nilpotent since $X^2 = 0$ but $X \neq 0$.

2. $d = 1$. Then $X - 1 \in \mathbf{Z}[X]/(X^2 - 1)$ is a zero divisor, however there are no nonzero nilpotent elements since $\mathbf{Z}[X]/(X^2 - 1) \simeq \mathbf{Z}[X]/(X - 1) \oplus \mathbf{Z}[X]/(X + 1)$.

3. $d = -3$. Certainly $R = \mathbf{Z}[X]/(X^2 + 3) \simeq \mathbf{Z}(\sqrt{-3})$ is a domain since $\mathbf{Z}(\omega)$ is a UFD. However, it is not integrally closed since $\omega \in K_R \notin R$.

4. $d = -5$. $R = \mathbf{Z}[X]/(X^2 + 5) \simeq \mathbf{Z}(\sqrt{-5})$ is integrally closed (since $5 \equiv 1 \bmod 4$), but it is not principal since it is not a UFD.

5. $d = -1$. $\mathbf{Z}/(X^2+1) \simeq \mathbf{Z}[i]$ is a Euclidean Domain and hence principal.

4 Finite Fields and Irreducibility

1. Let $P \in \mathbf{Z}[X]$ be monic and suppose that there exists some prime p such that $\bar{P} \in \mathbf{F}_p[X]$ is irreducible. If P were reducible in $\mathbf{Z}[X]$, say $P = ST$ ($\deg(S) > 0$, S, T monic) then we would have $\bar{P} = \bar{S}\bar{T}$ in $\mathbf{F}_p[X]$, with $\deg(S) = \deg(\bar{S})$, $\deg(T) = \deg(\bar{T})$, which shows that P is reducible in $\mathbf{F}_p[X]$ for every prime p. Since there is some prime for which it is not reducible, it must be irreducible in $\mathbf{Z}[X]$.

2. $P(X) = X^4 + 1$ is irreducible iff $P(X+1) = X^4 + 4X^3 + 6X^2 + 4X + 2$ is. By Eisenstein's criterion (with $p = 2$), $P(X+1)$ is irreducible. Notice that P has a root in $\mathbf{F}_2$ so that it is reducible in $\mathbf{F}_2[X]$. For any odd prime p, we easily have that $p^2 \equiv 1 \bmod 8$. Thus, -1 is always a fourth power in $\mathbf{F}_{p^2}$. Hence, P has a root in $\mathbf{F}_{p^2}$ for any p. Now if P were irreducible in $\mathbf{F}_p[X]$ then the degree of the field extension $\mathbf{F}_p(x)/\mathbf{F}_p$ where x is a root of P would be 4. But we know that P splits completely in the degree 2 extension $\mathbf{F}_p^2/\mathbf{F}_p$, since its roots are precisely the four fourth roots of unity. This gives a contradiction and hence P is reducible for every prime p.

3. It is not difficult to see that $P(X) = X^4 - 10X^3 + 21X^2 - 10X + 11$ has no roots in $\mathbf{Z}$. (Any rational root must have denominator dividing 1 and numerator dividing 11.) Thus, if P splits, it must be the product of two monic quadratics. Notice, however, that in $\mathbf{F}_7[X]$, we have $\bar{P}(X) = (X+3)(X^3+X^2+4X+6)$, which cannot be rearranged to give the product of two quadratics. Thus, P is irreducible.

4. Now let $P = X^{72} - X + 47$. In $\mathbf{F}_{47}$, we have $\bar{P} = X(X-1)\frac{(X^{71}-1)}{(X-1).}$ Since 71 is prime, the polynomial $\frac{(X^{71}-1)}{(X-1)}$ is irreducible in $\mathbf{Z}[X]$ and hence in $\mathbf{F}_p[X]$ fpr any prime p. Thus, if P splits in $\mathbf{Z}[X]$ it must be the product of two polynomials (not necessarily irreducible), of degrees $1, 71$ or $2, 70$. Examining $\bar{P} \in \mathbf{F}_2[X]$, however, shows that it is the product of four factors of degrees $4, 13, 23, 32$. There is no way that these factors can be combined to produce two factors of degrees $2, 70$, or $1, 71$. We therefore see that P must be irreducible.

5 Question of the day:

Since 2003 is prime, $\frac{X^{2003}-1}{X-1}$ is an irreducible degree 2002 polynomial.