Nepal Algebra Project 2017

Tribhuvan University

Module 1 — Problem Set 2 (MW)

Correction

1. Let G be a finite subgroup of the multiplicative group $K^\times$ of a field K. If n is the order of G, then by Lagrange's theorem any element x of G satisfies $x^n = 1$, hence the polynomial $X^n - 1$ has at least n roots in K, namely the elements in G. Since K is a field, this polynomial, which has degree n, has not more than n roots in K. We deduce that G is the set of roots of the polynomial $X^n - 1$ in K:

$$X^n - 1 = \prod_{x \in G} (X - x).$$

There are several proofs of the fact that G is cyclic. One of them is given in Milne, exercise 1.3. Here is another one which uses the fact that *in a finite abelian group of exponent e, there is an element of order e*; this result follows from the structure theorem of finite abelian groups. Recall that the *exponent* of a finite multiplicative group G is the lcm of the orders of the elements in G: it is the smallest integer $e \geq 1$ such that $x^e = 1$ for all $x \in G$.

By Lagrange's theorem, the exponent e of G divides n. Any x in G is a root of the polynomial $X^e - 1$. Since G has order n, we get n roots in the field K of this polynomial $X^e - 1$ of degree $e \leq n$. Hence $e = n$. Since there exists at least one element in G of order e, we deduce that G is cyclic.

2. By Lagrange's Theorem, if there exists a subgroup of order m in a group of order n, then m divides n.

For the converse, we assume that G is cyclic, generated by x, and that m divides n. Let $n = dm$. The element $y_d = x^d$ of G has order m, hence the subgroup H_m generated by y_d is a subgroup of G of order m. This subgroup is cyclic.

For the unicity, we consider a subgroup H of G of order m. An element z of H can be written $z = x^\ell$ with $\ell \in \mathbb{Z}$; since it belongs to H, it satisfies $z^m = 1$, hence $x^{\ell m} = 1$, and therefore n divides ℓm, which means that d divides ℓ. This proves that z belongs to H_m. Therefore $H = H_m$ and the unique subgroup of G of order m is the set of z in G satisfying $z^m = 1$.

3. A field of zero characteristic contains $\mathbb{Q}$, hence is infinite. Therefore a finite field F has a nonzero characteristic; since a field is a domain, this characteristic is a prime number, and the prime field of F is $\mathbb{F}_p$. As a vector space over $\mathbb{F}_p$, F has finite dimension, say r, hence F has p^r elements. If E is a subfield of F, then E contains $\mathbb{F}_p$; let s be the dimension of E as a $\mathbb{F}_p$ vector space. From the multiplicativity of the degrees $[F : E] \cdot [E : \mathbb{F}_p] = [F : \mathbb{F}_p]$ with $[E : \mathbb{F}_p] = s$ and $[F : \mathbb{F}_p] = r$, it follows that s divides r and that the dimension of F as a E–vector space is $[F : E] = r/s$. The subfield E with p^s elements is the set of roots of the polynomial $X^{p^s} - X$.

4. The stem field is defined for irreducible polynomials only. The question should have be phrased:

Are the polynomials $X^2 + 1$ and $X^2 - X + 1$ irreducible
- *over $\mathbb{Q}$?*
- *over $\mathbb{F}_p$ for $p = 2, 3, 5, 7$? For p any prime?*

When the answer is yes, the degree of the stem field over the corresponding field is the degree of the polynomial, namely 2.

Since the polynomials have degree 2 and no root in $\mathbb{Q}$, they are irreducible over $\mathbb{Q}$.

The polynomial $x^2 + 1$ is a square in $\mathbb{F}_2[X]$, namely $(X + 1)^2$, while the polynomial $X^2 - X + 1$ (which is the same as $X^2 - X + 1$) has no root in $\mathbb{F}_2$, hence is irreducible in $\mathbb{F}_2[X]$.

The polynomial $X^2 + 1$ has no root in $\mathbb{F}_3$, hence is irreducible in $\mathbb{F}_3[X]$, while $X^2 - X + 1 = (X + 1)^2$ in $\mathbb{F}_3[X]$.

Assume now that p is a prime ≥ 5.

Since $X^4 - 1 = (X^2 + 1)(X^2 - 1)$, an element in $\mathbb{F}_p$ is a root of $X^2 + 1$ if and only if it has order 4. Similarly, since $X^3 - 1 = (X - 1)(X^2 + X + 1)$, an element in $\mathbb{F}_p$ is a root of $X^2 + X + 1$ if and only if it has order 3, and since

$X^6-1=(X+1)(X-1)(X^2+X+1)(X^2-X+1)$, an element in $\mathbb{F}_p$ is a root of X^2-X+1 if and only if it has order 6.

The multiplicative group $\mathbb{F}_p^\times$ of the field $\mathbb{F}_p$ contains an element of order 4 (respectively 6) if and only if its order $p-1$ il a multiple of 4 (respectively 6). Notice that, since $p-1$ is even, 6 divides $p-1$ if and only if 3 divides $p-1$.

Hence X^2+1 is reducible in $\mathbb{F}_p[X]$ for p congruent to 1 modulo 4 and irreducible for p congruent to -1 modulo 4, while X^2-X+1 is reducible in $\mathbb{F}_p[X]$ for p congruent to 1 modulo 3 and irreducible for p congruent to -1 modulo 3.

5. **(a)**. The polynomial X^4+1 has no rational roots. There are several ways of checking that it is not the product of two quadratic polynomials with rational coefficients: we can split it over $\mathbb{C}$ and check that no product of two linear factors has rational coefficients. We can also write it as a product of two quadratic polynomials X^2+aX+b and X^2+cX+d and check that the solutions (a,b,c,d) are not rational numbers. Hence it is irreducible over $\mathbb{Q}$.
(b) The multiplicative group $F_q^\times$ is cyclic of order $q-1$, it contains a subgroup of order 8 if and only if q is congruent to 1 modulo 8. Now a root of X^4+1 is a root of X^8-1 which is not a root of X^4-1, hence it is nothing else than an element of order 8 in the multiplicative group $F_q^\times$.
(c) The polynomial X^4+1 splits in $\mathbb{F}_2[X]$ as $(X+1)^4$.

Assume p is odd. Assume also that X^4+1 is irreducible over $\mathbb{F}_p$. Its stem field is an extension of $\mathbb{F}_p$ of degree 4, hence has p^4 elements, it contains a field with p^2 elements (namely the roots of $X^{p^2}-X$) in which the polynomials X^4+1 has a root (because p^2 is congruent to 1 modulo 8). This is a contradiction. Hence X^4+1 is reducible over the finite field $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$.

6. Let $\sigma : F_1 \to F_2$ be a homomorphism of fields. The image of the prime field F of F_1 is the prime field of F_2, the restriction of σ to F produces an isomorphism between these prime fields, hence they have the same number of elements.

If F is a finite field, from $\sigma(1)=1$ one deduces by induction $\sigma(x)=x$ for any $x\in F$, hence σ is an F–homomorphism.

If $F=\mathbb{Q}$, from $\sigma(1)=1$ one deduces by induction $\sigma(a)=a$ for any $a\in\mathbb{Z}$. For $a/b\in\mathbb{Q}$ we have $b\sigma(a/b)=\sigma(a)=a$, hence $\sigma(a/b)=a/b$ for all $a/b\in F$, hence again σ is an F–homomorphism.

7. **(a)** When σ is an F–homomorphism $F(\alpha_1)\to F(\alpha_2)$, for $f\in F[X]$ we have $\sigma\big(f(\alpha)\big)=f(\sigma(\alpha))$. Hence if there exists an F–homomorphism $\sigma : F(\alpha_1)\to F(\alpha_2)$ such that $\sigma(\alpha_1)=\alpha_2$, for $f\in F[X]$ we have $f(\alpha_1)=0$ if and only if $f(\alpha_2)=0$ (recall that a homomorphism of fields is injective).
(b) If α_1 and α_2 are transcendental over F, then $F(\alpha_1)$ and $F(\alpha_2)$ isomorphic to the field of rational fractions $F(X)$, there is a unique F–isomorphism $\sigma_1 : F(X)\to F(\alpha_1)$ which maps X to α_1 and there is a unique F–isomorphism $\sigma_2 : F(X)\to F(\alpha_2)$ which maps X to α_2. Now the unique F–isomorphism $\sigma : F(\alpha_1)\to F(\alpha_2)$ which maps α_1 to α_2 is $\sigma_2\circ\sigma_1^{-1}$.
(c) The proof of $(ii)\to(i)$ has been given in the answer to (a) above. Conversely, if α_1 and α_2 have the same irreducible polynomial f, then both $F(\alpha_1)$ and $F(\alpha_2)$ are F–isomorphic to $F[X]/(f)$.

Assume that there exists an F–homomorphism $\sigma : F(\alpha_1)\to F(\alpha_2)$ such that $\sigma(\alpha_1)=\alpha_2$. For $P/Q\in F(X)$ with $Q(\alpha_1)\neq 0$, we have $Q(\alpha_2)=\sigma(Q(\alpha_1))\neq 0$ and $\sigma(P(\alpha_1)/Q(\alpha_1))=P(\alpha_2)/Q(\alpha_2)$, which proves the unicity of σ.

8. The field $F(\alpha,\beta)$ contains $F(\alpha)$ and $F(\beta)$, by the multiplicativity of the degrees the degree $[F(\alpha,\beta):F]$ is a multiple of $[F(\alpha):F]$ (which is n) and of $[F(\beta):F]$ (which is m); since n and m are relatively prime this degree is a multiple of mn. It follows that $F(\alpha,\beta)$ is an extension of $F(\alpha)$ of degree m, an extension of $F(\beta)$ of degree n and an extension of F of degree mn.

9. **(a)** For a polynomial $f(X_1,X_2)\in\mathbb{F}_2[X_1,X_2]$, we have $f(X_1,X_2)^2=f(X_1^2,X_2^2)$.
(b) Set $K=\mathbb{F}_2(T_1^2,T_2)$. Since T_1 does not belong to K but T_1^2 belongs to K, and since $K(T_1)=E$, we have $[E:K]=2$. In the same way, T_2 does not belong to F but T_2^2 belongs to F; since $F(T_2)=K$, we have $[K:F]=2$. By the multiplicativity of the degrees we deduce $[E:F]=[E:K][K:F]=4$.
(c) Any element of F has degree 1 or 2 over F, while the extension has degree 4. Hence the extension is not simple.