Instructor: Leo Goldmakher

Williams College
Department of Mathematics and Statistics

MATH 394 : GALOIS THEORY

Solution Set 4

4.1 The goal of this problem is to prove that every ideal of $K[t]$ is principal. Throughout, let I denote an ideal of $K[t]$ such that $\{0\} \subsetneq I \subsetneq K[t]$.

(a) Among all nonzero elements of I, suppose p has minimal degree. (This must exist by the well-ordering of $\mathbb{N}$.) Prove that $I \subseteq \langle p \rangle$. [*You may freely assume the quotient-remainder theorem stated in Lecture 6.*]

Pick $f \in I$. By the quotient-remainder theorem, there exist $q, r \in \mathbb{Q}[x]$ such that

$$f = qp + r$$

with $\deg r < \deg p$. Since I is an ideal and $p \in I$, we must have $qp \in I$ as well, whence $r = f - qp \in I$. But p has minimal degree in I, whence $r = 0$. It follows that any element of I is a multiple of p, as claimed.

(b) Prove that $I = \langle p \rangle$.

Let p be as above. Since $p \in I$ and I is an ideal, any multiple of p belongs to I, i.e. $\langle p \rangle \subseteq I$. Combining this with part (a) yields the claim.

4.2 We explore the structure of finite fields.

(a) Consider the field $\mathbb{F}_7$ with 7 elements. Is it a cyclic group under $+$? Is $\mathbb{F}_7^\times$ a cyclic group under $\times$? Justify your answers.

$\mathbb{F}_7$ as a group under $+$ is generated by 1, so it's cyclic. And $\mathbb{F}_7^\times$ is generated by 3 under multiplication, so it's also cyclic.

(b) Consider the field $L := \mathbb{F}_3[t]/\langle t^2+1 \rangle$ that we constructed in Lecture 7. Is it a cyclic group under $+$? Is $L^\times$ a cyclic group under $\times$? Justify your answers.

Consider the addition and multiplication tables for L:

$+$	0	1	2	t	$t+1$	$t+2$	$2t$	$2t+1$	$2t+2$
0	0	1	2	t	$t+1$	$t+2$	$2t$	$2t+1$	$2t+2$
1	1	2	0	$t+1$	$t+2$	t	$2t+1$	$2t+2$	$2t$
2	2	0	1	$t+2$	t	$t+1$	$2t+2$	$2t$	$2t+1$
t	t	$t+1$	$t+2$	$2t$	$2t+1$	$2t+2$	0	1	2
$t+1$	$t+1$	$t+2$	t	$2t+1$	$2t+2$	$2t$	1	2	0
$t+2$	$t+2$	t	$t+1$	$2t+2$	$2t$	$2t+1$	2	0	1
$2t$	$2t$	$2t+1$	$2t+2$	0	1	2	t	$t+1$	$t+2$
$2t+1$	$2t+1$	$2t+2$	$2t$	1	2	0	$t+1$	$t+2$	t
$2t+2$	$2t+2$	$2t$	$2t+1$	2	0	1	$t+2$	t	$t+1$

Addition table for $L = \mathbb{F}_3[t]/\langle t^2+1 \rangle$

continued on next page...

$\times$	1	2	t	$t+1$	$t+2$	$2t$	$2t+1$	$2t+2$
1	1	2	t	$t+1$	$t+2$	$2t$	$2t+1$	$2t+2$
2	2	1	$2t$	$2t+2$	$2t+1$	t	$t+2$	$t+1$
t	t	$2t$	2	$t+2$	$2t+2$	1	$t+1$	$2t+1$
$t+1$	$t+1$	$2t+2$	$t+2$	$2t$	1	$2t+1$	2	t
$t+2$	$t+2$	$2t+1$	$2t+2$	1	t	$t+1$	$2t$	2
$2t$	$2t$	t	1	$2t+1$	$t+1$	2	$2t+2$	$t+2$
$2t+1$	$2t+1$	$t+2$	$t+1$	2	$2t$	$2t+2$	t	1
$2t+2$	$2t+2$	$t+1$	$2t+1$	t	2	$t+2$	1	$2t$

Multiplication table for $L = \mathbb{F}_3[t]/\langle t^2+1\rangle$

- **L is not cyclic under $+$.** Any element of L is of the form $at+b$ where $a, b \in \mathbb{F}_3$, hence has order at most 3. It follows that none of the elements of L can generate all of L under $+$. (In fact, from Lagrange's theorem we deduce that every element has order 3 with the exception of the element 0.)
- **$L^\times$ is cyclic under $\times$.** We can compute the orders of all the elements directly from the multiplication table:

element of $L^\times$	**order under $\times$**
1	1
2	2
t	4
$t+1$	8
$t+2$	8
$2t$	4
$2t+1$	8
$2t+2$	8

From this table we see that $L^\times$ is cyclic, since (for example) $t+1$ generates the group.

(c) Write down a multiplication table for the field $F := \mathbb{F}_2/\langle x^2+x+1\rangle$. Is it a cyclic group under $+$? Is $F^\times$ a cyclic group under $\times$? Justify your answers.

Note that any quadratic polynomial in $\mathbb{F}_2[x]$ can be reduced to a linear polynomial in F by subtracting x^2+x+1. Thus, F consists of the four elements $ax+b$ with $a, b \in \mathbb{F}_2$. Each of these elements has order ≤ 2 under $+$, so F isn't cyclic under $+$.

Under multiplication, $F^\times$ must be cyclic, since it's a group of prime order (namely, 3). Here's a multiplication table:

$\times$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

Multiplication table for $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$

We see that both x and $x+1$ generate $F^\times$.

4.3 The goal of this problem is to prove that all rational roots of a monic polynomial $P \in \mathbb{Z}[x]$ must be integers. For concreteness, let $d := \deg P$, and suppose α is a rational root of P that isn't an integer.

(a) Let $S := \{n \in \mathbb{Z}_{>0} : n\alpha, n\alpha^2, \ldots, n\alpha^{d-1} \in \mathbb{Z}\}$. Explain why $S \neq \varnothing$.

If $\alpha \in \mathbb{Q}$, then $\alpha^k \in \mathbb{Q}$ for all positive integers k. Taking the product of all the denominators of $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ produces an element of S.

(b) Suppose $P(\beta) = 0$. Prove that for any positive integer k, β^k can be expressed as a $\mathbb{Z}$-linear combination of $1, \beta, \beta^2, \ldots, \beta^{d-1}$.

Since P is monic of degree d, we can write $P(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_2x^2 + a_1x + a_0$ with all the $a_i \in \mathbb{Z}$. Thus

$$\beta^d = -a_{d-1}\beta^{d-1} - \cdots - a_2\beta^2 - a_1\beta - a_0.$$

Having established a base case, we can proceed by induction: for any $k > d$, the above equation implies

$$\beta^k = -a_{d-1}\beta^{k-1} - \cdots - a_2\beta^{k-d+2} - a_1\beta^{k-d+1} - a_0\beta^{k-d},$$

and since all the powers of β on the RHS are strictly less than k, we may assume they can all be expressed as a $\mathbb{Z}$-linear combination of $1, \beta, \beta^2, \ldots, \beta^{d-1}$.

(c) Given $n \in S$, construct $n' \in S$ such that $n' < n$. [*Hint. Use that* $0 < \alpha - \lfloor \alpha \rfloor < 1$.]

Given $n \in S$, set

$$n' := n(\alpha - \lfloor \alpha \rfloor)^{d-1}.$$

Clearly $0 < n' < n$; I claim that $n' \in S$. To prove this, it suffices to show that $n'\alpha^k \in \mathbb{Z}$ for all integers $k \geq 0$.

Write

$$(\alpha - \lfloor \alpha \rfloor)^{d-1} = \alpha^{d-1} + b_{d-1}\alpha^{d-2} + \cdots + b_1\alpha + b_0,$$

where all the $b_i \in \mathbb{Z}$. Then

$$\begin{aligned} n'\alpha^k &= n(\alpha^{d+k-1} + b_{d+k-1}\alpha^{d+k-2} + \cdots + b_1\alpha^{k+1} + b_0\alpha^k) \\ &= n(c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{d-1}\alpha^{d-1}) \qquad \text{with all } c_i \in \mathbb{Z}, \text{ by part (b)} \\ &= c_0 n + c_1 n\alpha + c_2 n\alpha^2 + \cdots + c_{d-1} n\alpha^{d-1}. \end{aligned}$$

Since $n \in S$, each term of the above is an integer, whence $n'\alpha^k \in \mathbb{Z}$ for all $k \geq 0$.

(d) In one sentence, explain the contradiction.

S is a nonempty set of positive integers, but part (c) shows it has no least element, contradicting the well-ordering property.

4.4 In class we showed that for any $f \in \mathbb{Q}[x]$ there must exist some $\alpha \in \mathbb{Q}_{>0}$ such that $\alpha f \in \mathbb{Z}[x]$ is primitive. Prove that this α is unique.

Suppose $g := \alpha f$ and $h := \beta f$ are both primitive, where $\alpha, \beta \in \mathbb{Q}_{>0}$. Write $\frac{\alpha}{\beta} = \frac{k}{\ell}$ with $k, \ell \in \mathbb{Z}_{>0}$. Then $g(x) = \frac{k}{\ell}h(x)$. Since the coefficients of $kh(x)$ have gcd k, and $g \in \mathbb{Z}[x]$, we deduce $\ell \mid k$. By the same logic applied to $h(x) = \frac{\ell}{k}g(x)$, we deduce $k \mid \ell$. It follows that $k = \ell$, whence $\alpha = \beta$.

4.5 Prove that the product of two primitive polynomials is primitive.

Given $f, g \in \mathbb{Z}[x]$ such that

$$f(x)g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m$$

isn't primitive. Then there must exist some prime p that divides all the c_k, whence

$$\overline{f}(x)\overline{g}(x) = 0$$

in $\mathbb{F}_p$. (Here, as usual, $\overline{f}$ denotes the reduction of $f \pmod p$ and $\overline{g}$ the reduction of $g \pmod p$.)

Lemma. *If $a, b \in K[x]$ where K is a field and $ab = 0$, then either $a = 0$ or $b = 0$.*

It follows that either $\overline{f} = 0$ or $\overline{g} = 0$. But this means that either all of the coefficients of f are multiples of p, or all coefficients of g are multiples of p; at least one of them is not primitive. This concludes the proof.

4.6 We say a field K is *algebraically closed* iff every polynomial in $K[x]$ has a root in K. (Later this semester, we'll use Galois theory to prove that $\mathbb{C}$ is algebraically closed.) Prove that if K has finitely many elements, it cannot be algebraically closed.

Say K has q elements. Then $K^\times$ has $q-1$ elements and is a group under $\times$, so Lagrange's theorem implies $a^{q-1} = 1$ for all $a \in K^\times$. It follows that $a^q = a$ for all $a \in K$, whence the polynomial $x^q - x + 1$ has no roots in K.

4.7 The goal of this problem is to introduce a new irreducibility test.

(a) Prove that $|f^{-1}(k)| \leq \deg f$ for any nonconstant $f \in \mathbb{Z}[t]$. [Here $f^{-1}(k) := \{n \in \mathbb{Z} : f(n) = k\}$.]

For any $k \in \mathbb{Z}$, set $g_k(x) := f(x) - k$ and note that $a \in f^{-1}(k)$ iff $g_k(a) = 0$. Thus $|f^{-1}(k)|$ is bounded by the number of roots of g_k in $\mathbb{C}$, which is $\leq \deg g_k = \deg f$, as claimed.

(b) Given $f \in \mathbb{Z}[t]$, consider the set

$$P_f := \{n \in \mathbb{Z} : |f(n)| = 1 \text{ or prime}\}.$$

Suppose f is monic and non-constant. Prove that if $|P_f| \geq 2\deg(f) + 1$ then f is irreducible over $\mathbb{Q}$.

Suppose f were reducible over $\mathbb{Q}$. By Gauss' Lemma, we may write $f = gh$ for some nonconstant polynomials $g, h \in \mathbb{Z}[t]$. For any $n \in P_f$ we have $f(n) = \pm 1$ or $\pm p$ for some prime p, whence either $g(n) = \pm 1$ or $h(n) = \pm 1$. Thus,

$$|P_f| \leq \#\{n \in \mathbb{Z} : g(n) = \pm 1\} + \#\{n \in \mathbb{Z} : h(n) = \pm 1\}.$$

By part (a), we deduce

$$|P_f| \leq 2\deg g + 2\deg h = 2\deg f$$

contradicting the hypothesis.

(c) Use the above to prove that $x^4 - 2x^3 + 9x - 1$ is irreducible over $\mathbb{Q}$.

It can be manually verified that magnitude of the polynomial is 1 or prime for all 9 integer inputs of magnitude ≤ 4. By part (b) we conclude that the polynomial must be irreducible.

4.8 We've discussed seven irreducibility tests (including the one above). Try to use each of these to determine irreducibility of the following polynomials over $\mathbb{Q}$. If a test doesn't work, briefly described what you tried to make it work.

(a) $f(x) = 1 + x + x^2 + x^3 + x^4$

Rational root test. This tells us the only potential rational roots are ± 1, neither of which is a root of f. Thus if f factors over $\mathbb{Q}$, it must be into the product of two quadratics.

Reduction to $\mathbb{Z}$. From above, we know that if f is reducible, then any factorization of f over $\mathbb{Q}$ must be into two quadratics. We further know that we may make both of these have coefficients in $\mathbb{Z}$. Write

$$f(x) = (x^2 + ax + b)(x^2 + cx + d);$$

since $f(0) = 1$, we deduce $b = d = \pm 1$. Similarly, $f(-1) = 1$ implies $(1-a+b)(1-c+d) = 1$, whence $a = c$. Finally, comparing linear coefficients implies $2ab = ad + bc = 1$, which is impossible. Thus, f must be irreducible.

Eisenstein. Note that $f(x) = \frac{x^5-1}{x-1}$, whence

$$f(x+1) = \frac{(x+1)^5 - 1}{x} = x^4 + 5x^3 + 10x^2 + 10x + 5.$$

By Eisenstein at 5, this is irreducible, so $f(x)$ must be as well.

Reduction (mod p). Note that f is its own reduction (mod 2). I claim it's irreducible over $\mathbb{F}_2$. First, it clearly has no roots in $\mathbb{F}_2$, so if it factors it must factor as two quadratics:

$$1 + x + x^2 + x^3 + x^4 = (x^2 + ax + 1)(x^2 + cx + 1)$$

over $\mathbb{F}_2$. Note that $x^2 + 1$ is reducible over $\mathbb{F}_2$, whence $a = c = 1$. But the linear term of $(x^2 + x + 1)^2$ is 0, not 1!

Perron's test. I'd love to hear whether you discovered a clever way to apply this!

Schur's test. I'd love to hear whether you discovered a clever way to apply this!

Lots of prime outputs? We apply the test from the previous problem. It can be checked that $f(x) = 1$ for $x = 0, -1$, and prime for $x = 1, \pm 2, -3, -5, 7, 12$. These nine values guarantee that f is irreducible.

(b) $g(x) = x^4 - 2x^3 + 9x - 1$

Similar.