Final, Math B504 **Name:** *James Wang*
May 16, 2024

Problem 1:

Let R be an integral domain and let $Q = \text{Frac}(R)$, the quotient field of R.

a) Prove that $(Q/R) \otimes_R (Q/R) = 0$.

Consider arbitrary $\frac{q_1}{r_1} \otimes \frac{q_2}{r_2} \in (Q/R) \otimes_R (Q/R)$ where r_1 and r_2 are nonzero, then by tensor product we have that

$$\frac{q_1}{r_1} \otimes \frac{q_2}{r_2} = (r_2 \cdot \frac{q_1}{r_2 r_1}) \otimes \frac{q_2}{r_2} = \frac{q_1}{r_2 r_1} \otimes (r_2 \cdot \frac{q_2}{r_2}) = 0,$$

because $r_2 \cdot \frac{q_2}{r_2} = 0$ in Q/R.

Since every element of $(Q/R) \otimes_R (Q/R)$ is a finite sum of elements of the form $\frac{q_1}{r_1} \otimes \frac{q_2}{r_2}$, every element is a finite sum of 0. Hence $(Q/R) \otimes_R (Q/R) = 0$.

QED

b) Let N be a left R-module. Prove that every element of the tensor product $Q \otimes_R N$ can be written in terms of simple tensor of the form $(1/d) \otimes n$ for some nonzero $d \in R$ and some $n \in N$.

Since every element of $Q \otimes_R N$ is of the form $\sum_{\text{finite}} \frac{r_i}{s_i} \otimes n_i$, where $r_i, s_i \in R$, $s_i \neq 0$, and $n_i \in N$. Take arbitrary $\frac{r_1}{s_1}, \frac{r_2}{s_2}$ and $\frac{r_3}{s_3}$, we see that

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} + \frac{r_3}{s_3} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} + \frac{r_3}{s_3} = \frac{r_1 s_2 s_3 + r_2 s_1 s_3 + r_3 s_1 s_2}{s_1 s_2 s_3}.$$

We can then conclude that

$$\sum_{\text{finite}} \frac{r_i}{s_i} \otimes n_i = \frac{\sum r_i \cdot \prod_{j \neq i} s_j}{\prod s_i} \otimes \sum n_i = \frac{1}{\prod s_i} \otimes (\sum_i (r_i \cdot \prod_{j \neq i} s_j n_i)).$$

Let $d = \prod s_i$ and $n = \sum_i (r_i \cdot \prod_{j \neq i} s_j n_i)$, then we are done with the proof.

QED

Problem 2:

Consider the $\mathbb{Z}$-module $\mathbb{Q} \oplus \mathbb{Z}$.

a) Prove that $\mathbb{Q} \oplus \mathbb{Z}$ is flat.

Recall we have shown that both $\mathbb{Q}$ and $\mathbb{Z}$ are flat $\mathbb{Z}$-modules (HW 4 Problem 1, and $\mathbb{Z}$ is a projective $\mathbb{Z}$-module so it is flat), and the direct sum of flat modules is still flat (HW 4 Problem 2). Hence $\mathbb{Q} \oplus \mathbb{Z}$ is flat.

$$QED$$

b) Prove that $\mathbb{Q} \oplus \mathbb{Z}$ is not projective.

We have shown that a direct sum of two R-modules is projective if and only if both of them are projective (HW 3 Problem 5). We have, moreover, also shown that $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module (HW 3 Problem 4). Hence $\mathbb{Q} \oplus \mathbb{Z}$ cannot be projective.

$$QED$$

c) Prove that $\mathbb{Q} \oplus \mathbb{Z}$ is not injective.

We have shown that a direct sum of two R-modules is injective if and only if both of them are injective (HW 3 Problem 5). We claim that $\mathbb{Z}$ is not injective. This is because Baer's Criterion suggests that a $\mathbb{Z}$-module is injective if and only if it is divisible, yet $\mathbb{Z}$ is not divisible. Hence $\mathbb{Q} \oplus \mathbb{Z}$ cannot be divisible.

$$QED$$

Problem 3:

Let $\alpha = \sqrt{1+\sqrt{2}} \in \mathbb{C}$. Find the minimal polynomial of α over $\mathbb{Q}$.

We use our classic trick by raising α to its powers until we observe some linear dependence.

$$\alpha = \sqrt{1+\sqrt{2}}$$
$$\alpha^2 = 1+\sqrt{2}$$

Note that this is equivalent to $\alpha^2 - 1 = \sqrt{2}$, and

$$(\alpha^2-1)^2 = 2.$$

By observation, this means $(\alpha^2-1)^2-2=0$, and we claim $f(x) = (x^2-1)^2-2 = x^4-2x^2-1$ is the minimal polynomial. We can easily check that α is a root of $f(x)$, and it remains to show $f(x)$ is irreducible. Indeed, we see that the 4 roots of $f(x)$ in $\mathbb{C}$ are $\pm\sqrt{1\pm\sqrt{2}}$, which are all irrational. This means $f(x)$ does not have any root in $\mathbb{Q}$, and if $f(x)$ were reducible, then it must be a product of two quadratics.

Suppose that this is the case for a contradiction. Since we can multiply $f(x)$ by any scalar without changing it, we can assume the two quadratics are monic and

$$\begin{aligned} f(x) &= (x^2+b_1x+c_1)(x^2+b_2x+c_2) \\ &= x^4+(b_1+b_2)x^3+(c_1+b_1b_2+c_2)x^2+(b_1c_2+b_2c_1)x+c_1c_2. \end{aligned} \tag{1}$$

This means $b_1+b_2=0$, $c_1+b_1b_2+c_2=-2$, $b_1c_2+b_2c_1=0$, and $c_1c_2=-1$. We see that $b_2=-b_1$, and with substitution we can change the third equality to $b_1(c_2-c_1)=0$, which means $b_1=0$ or $c_2=c_1$. Clearly, $c_2 \neq c_1$, as the fourth equality shows. We can thus assume $b_1=0$. If this is the case, nevertheless, by the second equality we would get $c_1+c_2=-2$, and there is no rational solution to the system $c_1+c_2=-2$ and $c_1c_2=-1$. We have now reached a contradiction, so $f(x)$ must be irreducible, and the minimal polynomial of α over $\mathbb{Q}$ must be $f(x)=x^4-2x^2-1$.

QED

Problem 4:

Assume F is a field and $F(\alpha)$ is a finite field extension of F of odd degree. Prove that $F(\alpha^2) = F(\alpha)$.

We already have the inclusion $F(\alpha^2) \subseteq F(\alpha)$. It remains to show the other inclusion.

We use the Tower Formula by observing $F \subseteq F(\alpha^2) \subseteq F(\alpha)$, so that

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F].$$

We recall the definition of field extensions. $F(\alpha)$ is adding α to F, $F(\alpha^2)$ is adding α^2 into F, and $[F(\alpha) : F(\alpha^2)]$ is the degree of the minimal polynomial of α with coefficients in $F(\alpha^2)$. We see that since $\alpha^2 \in F(\alpha^2)$, it is guaranteed that $x^2 - \alpha^2$ as a polynomial over $F(\alpha^2)$ has α as a root. Hence we can conclude that $[F(\alpha) : F(\alpha^2)] = 1$ or 2. Yet recall that by assumption $[F(\alpha) : F]$ is odd, and by the Tower Formula, if $[F(\alpha) : F(\alpha^2)] = 2$, the multiplication of anything by 2 would force $[F(\alpha) : F]$ to be even. Hence it must be that $[F(\alpha) : F(\alpha^2)] = 1$, which by definition means $F(\alpha^2) = F(\alpha)$.

$$QED$$

Problem 5:

Let p be a prime number.

a) Find the Galois group of $f(x) = x^p - 1$ over $\mathbb{Q}$.

We claim that the Galois group G of $f(x)$ is C_{p-1}, the cyclic group of order $p-1$. We prove this by showing G is isomorphic to $\mathbb{F}_p^\times$, the multiplicative group of units of $\mathbb{F}_p$, which we know is C_{p-1} from discussions in class. First observe that

$$x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1),$$

and the rightmost parenthesis is the minimal polynomial $g(x)$ of $\zeta_p = e^{2\pi i/p}$. We know the $p-1$ roots of $g(x)$ are $\{\zeta_p, \ldots, \zeta_p^{p-1}\}$, and $\mathbb{Q}(\zeta_p)$ is the splitting field of $f(x)$. Take arbitrary $\tau \in G$, since τ is an automorphism of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$, which can be seen as a permutation of the roots by definition, to identify the exact group element τ, we just need to consider $\tau(\zeta_p)$, since where ζ_p gets mapped to completely determines where the other powers of ζ_p get mapped to by the the property of a homomorphism. We use τ_n to denote the group element τ if $\tau(\zeta_p) = \zeta_p^n$. Note that it is impossible for $\tau(\zeta_p) = 1$, because τ must fix the base field $\mathbb{Q}$ and be an isomorphism. Note also that there are $p-1$ choices for $\tau(\zeta_p)$, because $g(x)$ is irreducible in $\mathbb{Q}$, which means the action of G on the roots $\{\zeta_p, \ldots, \zeta_p^{p-1}\}$ is transitive, so there is only one orbit and anything could be mapped to anything. We therefore have a bijective correspondence between G and $\mathbb{F}_p^\times$ since $|G| = |\mathbb{F}_p^\times| = p-1$.

We finally define a homomorphism $\varphi : G \to \mathbb{F}_p^\times$ by $\tau_n \mapsto \zeta_p^n$, and verify that

$$\varphi(\tau_{n_2} \circ \tau_{n_1}) = (\zeta_p^{n_1})^{n_2} = \zeta_p^{n_1 n_2} = \varphi(\tau_{n_2})\varphi(\tau_{n_1})$$

$$QED$$

Note: I remember when we wrote about the cyclotomic polynomials for homework, I saw this proof somewhere and this is how it goes, but I cannot remember the details of the homomorphism.

b) Let $g(x) = x^p - 2 \in \mathbb{Q}[x]$. Determine the splitting field K of $g(x)$ and compute $[K : \mathbb{Q}]$.

We know that the p roots of $g(x)$ in $\mathbb{C}$ are $\{\sqrt[p]{2}, \zeta_p \sqrt[p]{2}, \ldots, \zeta_p^{p-1} \sqrt[p]{2}\}$, so the splitting field K of $g(x)$ is $K = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$, where $\zeta_p = e^{2\pi i/p}$. Since $g(x)$ is irreducible over $\mathbb{Q}$ by the Eisenstein Criterion, we know $[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = p$. By our knowledge of the roots of unity, moreover, we know $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Clearly $\mathbb{Q}(\zeta_p) \nsubseteq \mathbb{Q}(\sqrt[p]{2})$, because $\mathbb{Q}(\zeta_p)$ is complex and $\mathbb{Q}(\sqrt[p]{2})$ is real. Hence we can conclude $[K : \mathbb{Q}] = p(p - 1)$.

$$QED$$

Problem 6:

Find the Galois groups of the following polynomials over the given fields.

a) $x^8 - x$ over $\mathbb{Q}$

Since the factorization into irreducibles is $x^8 - x = x(x^7 - 1)$ over $\mathbb{Q}$, we know the splitting field of $x^8 - x$ over $\mathbb{Q}$ is the same as that of $x^7 - 1$. Note that we can just use Problem 5a) to conclude the Galois group is C_6.

QED

b) $x^8 - x$ over $\mathbb{F}_2$

Since the factorization into irreducibles is $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$ over $\mathbb{F}_2$, let α be a root of $h(x) = x^3 + x + 1$, then we obtain the relation $\alpha^3 = \alpha + 1$, and $h(\alpha^2) = 0$ because upon substitution $h(\alpha^2) = (\alpha^2)^3 + \alpha^2 + 1 = (\alpha^3)^2 + \alpha^2 + 1 = (\alpha+1)^2 + \alpha^2 + 1 = 0$. We can conclude $\alpha \neq \alpha^2$ because otherwise $\alpha = 0$ or 1, which would contradict the fact that $h(x)$ is irreducible...

Note: I tried a lot of approaches from this point on, but can't seem to get very far. If I had to guess, I would say the Galois group is C_3.

QED

c) $x^4 - 1$ over $\mathbb{F}_7$

Since the factorization into irreducibles is $x^4 - 1 = (x^2+1)(x+1)(x-1)$ over $\mathbb{F}_7$, we know the splitting field of $x^4 - 1$ over $\mathbb{F}_7$ is simply $\mathbb{F}_7(\alpha)$, where α is a root of $x^2 + 1$. This is because $\alpha^2 = -1$, so $\pm\alpha$ are both roots of $x^2 + 1$. Since $[\mathbb{F}_7(\alpha) : \mathbb{F}_7] = 2$, we can conclude the Galois group is C_2.

QED

Problem 7:

Find all irreducible quadratic polynomials over $\mathbb{F}_3$.

Note: I could not remember what exactly was discussed in class on May 1st, but I did recall an important result from Theorem 15.7.3 in Artin (page 459) that could solve this problem, which I believe is relevant to our discussion in class.

The Theorem states that given a prime p and let $q = p^r$ where r is a positive power, the irreducible factors of the polynomial $x^q - x$ over the prime field $\mathbb{F}_p$ are the irreducible polynomials in $\mathbb{F}_p[x]$ whose degrees divide r.

In our situation, let $p = 3$ and $r = 2$, then $q = 3^2 = 9$. We can then change the problem to finding the irreducible polynomials in $\mathbb{F}_3$ whose degrees divide 2, which is equivalent to finding the irreducible factors of the polynomial $x^9 - x$ in $\mathbb{F}_3$.

Clearly, all the degree 1 polynomials in $\mathbb{F}_3$ are irreducible, which are x, $x+1$, and $x+2$. This means there must be 3 irreducible quadratic polynomials so that when multiplying these 6 irreducible polynomials together we get to degree 9.

Consider a degree 2 polynomial $ax^2 + bx + c$ in $\mathbb{F}_3$. Since our coefficients are in a field, we can always multiply ax^2 by a^{-1} to make it monic, and recall that multiplying a ring element by a unit does not change it. We then get three choices for each of b and c. Together, we know there are nine possible degree 2 polynomials in $\mathbb{F}_3$.

We also know the product of any two of the three degree 1 polynomials is reducible, which are x^2, $x^2 + x$, $x^2 + 2x$, $x^2 + 2x + 1$, $x^2 + 2$, and $x^2 + x + 1$. This means the irreducible quadratic polynomials over $\mathbb{F}_3$ are the other three monic degree 2 polynomials, which are $x^2 + 1$, $x^2 + x + 2$, and $x^2 + 2x + 2$.

QED