MATH 3030, Abstract Algebra
Winter 2012
Toby Kenney
Midterm Examination
Monday 18th February: 2:35-3:25 PM

Basic Questions

1. *Let $R = \mathbb{Z}_4 \times \mathbb{Z}_2$. Let I be the ideal of R generated by $(2,1)$.*

   (a) What is the ideal I?

   R is commutative, so we only need to consider multiplication on one side. We see that $(0,1)(2,1) = (0,1)$ and $(1,0)(2,1) = (2,0)$, so I must contain $(0,1)$ and $(2,0)$. I is a subgroup, so it must contain the subgroup generated by these elements, namely $\{(0,0),(0,1),(2,0),(2,1)\}$. This set is closed under multiplication by arbitrary elements of R, so it is the ideal generated by $(2,1)$.

   (b) What is the factor ring R/I?

   R has 8 elements, and I has 4 elements, so R/I has 2 elements. R is unital, so R/I is also unital. The only unital ring with 2 elements is $\mathbb{Z}_2$, so $R/I \cong \mathbb{Z}_2$.

2. *What is $\mathrm{Irr}(\sqrt{3}+\sqrt{5},\mathbb{Q})$?*

   Computing powers of $\sqrt{3}+\sqrt{5}$ gives

$$\begin{aligned} 1 &= 1 \\ \sqrt{3}+\sqrt{5} &= \sqrt{3}+\sqrt{5} \\ (\sqrt{3}+\sqrt{5})^2 &= 8+2\sqrt{15} \\ (\sqrt{3}+\sqrt{5})^3 &= 18\sqrt{3}+14\sqrt{5} \\ (\sqrt{3}+\sqrt{5})^4 &= 124+32\sqrt{15} \end{aligned}$$

   From this we see that $\sqrt{3}+\sqrt{5}$ is a zero of x^4-16x^2+4. This is irreducible, since $\{1,\sqrt{3}+\sqrt{5},(\sqrt{3}+\sqrt{5})^2,(\sqrt{3}+\sqrt{5})^3\}$ are clearly linearly independent over $\mathbb{Q}$, so $\sqrt{3}+\sqrt{5}$ has degree 4 over $\mathbb{Q}$, and is not a zero of any non-zero polynomial of lower degree.

3. *Let α be a zero of $f(x) = x^2 - 2$ in GF(25). Find a generator of the multiplicative group of nonzero elements of GF(25).*

   We know that the multiplicative group of nonzero elements of GF(25) has 24 elements. Furthermore, we see that $\alpha^2 = 2$, $\alpha^4 = 4$ and $\alpha^8 = 1$, so α

has order 8 in this group. We therefore need to find a cube root of α. We try $\alpha+1$, and we get $(\alpha+1)^3 = \alpha^3+3\alpha^2+3\alpha+1 = 2\alpha+1+3\alpha+1 = 2$ Therefore, $\alpha+1$ has order 12. This leads us to try $\alpha(\alpha+1) = \alpha+2$, where we see $(\alpha+2)^3 = \alpha^3+\alpha^2+2\alpha+3 = 4\alpha = \alpha^5$. Since 5 and 8 are coprime, α^5 has order 8, so $\alpha+2$ has order 24, i.e. it is a generator of the multiplicative group.

4. *Compute a composition series for $D_5 \times D_4$. Is $D_5 \times D_4$ solvable?*

   One composition series is $\mathbb{Z}_5 \times \{e\} \leqslant D_5 \times \{e\} \leqslant D_5 \times \mathbb{Z}_2 \leqslant D_5 \times \mathbb{Z}_4 \leqslant D_5 \times D_4$, where the cyclic groups are all groups of rotations.

   It is easy to see that the order of each factor group in this composition series is prime, so the factor group must be abelian. Therefore, $D_5 \times D_4$ is solvable.

Theoretical Questions

5. *Prove that for a field F, every ideal in the polynomial ring $F[x]$ is principal.*

   Let I be an ideal in $F[x]$. If I is the zero ideal, then the result is obvious. Let f be a non-zero polynomial of smallest degree n in I (i.e. all polynomials in I are of degree at least n). We will show that any other polynomial g in I is divisible by f, since by the division algorithm, we have that $g = qf + r$ where either $r = 0$ or the degree of r is less than the degree of f. However, since $g \in I$ and $f \in I$, we have that $r = g - qf \in I$, and since n is the smallest degree of a non-zero polynomial in I, and r has degree less than n, this means that $r = 0$. Therefore, $g = qf$. Since g is an arbitrary element of I, we have shown that I is the principal ideal generated by f.

6. *Show that any finite extension field E of a field F is algebraic over F.*

   Let the dimension of E over F be n. Let $\alpha \in E$, and consider the set $\{1, \alpha, \ldots, \alpha^n\}$. Since this has $n+1$ elements, it can't be linearly independent, so there is some linear combination $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, where $a_0, \ldots, a_n \in F$. This means that α is a zero of $a_0 + a_1x + \cdots + a_nx^n$ in $F[x]$, so α is algebraic over F. Therefore, E is algebraic over F.

7. *Show that any non-zero ring homomorphism between two fields is one-to-one.*

   If $\phi : F \longrightarrow E$ is a non-zero ring homomorphism between two fields, then we know that the kernel of ϕ is an ideal of F. Since F is a field its only ideals are the trivial ideal and the improper ideal. If the kernel of ϕ were the improper ideal, ϕ would be the zero homomorphism, so the kernel of ϕ must be the trivial ideal, which means that ϕ is one-to-one.

8. *Let F be a field. Let $F(\alpha)$ be algebraic over F.*

(a) Show that if $[F(\alpha) : F]$ *is odd, then* $F(\alpha^2) = F(\alpha)$.

Since $\alpha^2 \in F(\alpha)$, we know that $F(\alpha^2)$ is a subfield of $F(\alpha)$. Furthermore, it is easy to see that $\{1, \alpha\}$ is a spanning set for $F(\alpha)$ over $F(\alpha^2)$, so $[F(\alpha) : F(\alpha^2)] \leqslant 2$. Since $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$ is odd, so is $[F(\alpha) : F(\alpha)]$, so it must be 1, i.e. $F(\alpha) = F(\alpha^2)$.

(b) [Bonus] If $[F(\alpha) : F]$ *is not divisible by 3, must* $F(\alpha^3) = F(\alpha)$*? [Give a proof or a counterexample.]*

This is not necessarily the case, since we only have that $[F(\alpha) : F(\alpha^3)] \leqslant 3$, since α is a zero of the polynomial $x^3 - \alpha^3$. However, if this polynomial has a zero in $F(\alpha^3)$, then it is reducible, and α could be of degree 2 over $F(\alpha^3)$. The easiest example of this is if $F = \mathbb{Q}$ and $\alpha = \frac{-1+\sqrt{3}i}{2}$ is a complex cube root of 1. Then $\mathbb{Q}(\alpha^3) = \mathbb{Q}$, and $F(\alpha) \neq F(\alpha^3)$.