Math 511B - Final Practice

Selected Solutions

(3) Suppose $f(x)$ was reducible. Then as f is of degree m, we know that m must divide the degree of the extension. However, as $(m,n)=1$ we know that $m \nmid n$ as so f must still be irreducible.

(5) (a) Compute the Smith Normal form for L.
(b) Express $\mathbb{Z}^n/\operatorname{Im} L$ as a direct sum of cyclic groups.

(a) $L \to \begin{pmatrix} -1 & 0 & 0 & \cdots & 0 \\ 0 & n & 0 & \cdots & 0 \\ 0 & 0 & n & \cdots & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \cdots & n^2 - n^2 = 0 \end{pmatrix}$ (b) $(\mathbb{Z}/n\mathbb{Z})^{n-2} \oplus \mathbb{Z}$

(7) $\begin{pmatrix} 2 & 4 & -6 \\ 4 & 4 & 8 \\ -6 & -8 & 14 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & -4 & 20 \\ 0 & 4 & -4 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & & \\ & -4 & 0 \\ & 0 & 16 \end{pmatrix}$ and so we have $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$.

(8) (a) Sure, this extension is well known to be Galois. If E and F are the splitting fields of families of separable polynomials, then EF is the splitting field of the big family gotten by throwing together the polynomials that give E and F.

1. (a) **Solution 1** *(b) The intersection is again Galois over k. One way to see this is to say that $E \cap F$ is a subfield of E and is therefore separable over k. The issue is whether or not it is normal. Any $\sigma : E \cap F \to \bar{k}$ that is the identity on k can be extended to a map $E \to \bar{k}$ and therefore takes values in E (because E is normal over k). Symmetrically, it takes values in F. Therefore, the image lies in $E \cap F$. An alternate argument is to exploit the corollary that if the subgroups of $\operatorname{Gal}(L/k)$ that correspond to E and F are H and H', then the subgroup corresponding to the intersection is the group generated by H and H'. If H and H' are both normal subgroups of $\operatorname{Gal}(L/k)$, so is the group that they generate together.*

(9) If f is reducible, say $f = gh$ in $k[x]$, then the action of $\operatorname{Gal}(K/k)$ on the roots of f sends roots of g to roots of g and roots of h to roots of h. Thus the action is not transitive: you can't find an element of $\operatorname{Gal}(K/k)$ that sends an arbitrary α_i to an arbitrary α_j. Suppose that f is irreducible and take two roots α_i and α_j of f. As we know, there are isomorphisms $k[x]/(f(x)) \tilde{\to} k(\alpha_i)$ and $k[x]/(f(x)) \tilde{\to} k(\alpha_j)$ that map x to α_i and α_j, respectively. Taking the composite of one map and the inverse of the other, we obtain $\sigma : k(\alpha_i) \to k(\alpha_j)$ that sends α_i to α_j and is the identity on k. View σ as an embedding $k(\alpha_i) \to K$ and extend it to an automorphism of K. The resulting element of $\operatorname{Gal}(K/k)$ sends α_i to α_j.

(10) $\mathbb{Q}(\zeta)$ is a Galois extension of $\mathbb{Q}$ whose degree is $p-1$. The galois group of the extension is canonically $(\mathbb{Z}/p\mathbb{Z})^*$, a cyclic group of order $p-1$. In the dictionary between elements of $(\mathbb{Z}/p\mathbb{Z})^*$ and automorphisms of $\mathbb{Q}(\zeta)$, the number i mod p corresponds to the automorphism that sends ζ to ζ^i. Since $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta)$, $\mathbb{Q}(\alpha)$ is a cyclic extension of $\mathbb{Q}$ of degree dividing $p-1$. The degree is the number of distinct conjugates $alpha_i := \zeta^i + \zeta^{-i}$ of $\alpha = \zeta + \zeta^{-1}$. Let us calculate the number of disctinct α_i. Certainly α_i depends only on the image of i in $(\mathbb{Z}/p\mathbb{Z})^* \setminus \{\pm 1\}$, i.e., $\alpha_i = \alpha_{-i}$. Conversely, suppose $\alpha_i = \alpha_j$, which is to say $\zeta^i + \zeta^{-i} = \zeta^j + \zeta^{-j}$. We can suppose that we have $1 \leq i, j \leq p-1$ for definitiveness. An important fact here is that the numbers $\zeta, \zeta^2, ..., \zeta^{p-1}$ are linearlly independent of $\mathbb{Q}$. Indeed, a linear dependence amoung them would yield on division by ζ a linear dependence among $1, \zeta, ..., \zeta^{p-2}$, which would contradict the fact that ζ has degree $p-1$ over $\mathbb{Q}$. The important fact implies that $i = \pm j$ which is enough to show that there are $(p-1)/2$ different α_i. Hence $\mathbb{Q}(\alpha)$ has degree $(p-1)/2$ over $\mathbb{Q}$.

(19) Write down all abelian groups of order 1500 using both elementary divisors and invariant factors.

Solution: $1500 = 2^2 \cdot 3 \cdot 5^3$, and so there will be a total of six of each:

Elementary Divisors: $Z_4 \oplus Z_3 \oplus Z_{5^3}$, $Z_4 \oplus Z_3 \oplus Z_{5^2} \oplus Z_5$, $Z_4 \oplus Z_3 \oplus (Z_5)^3$, $(Z_2)^2 \oplus Z_3 \oplus Z_{5^3}$, $(Z_2)^2 \oplus Z_3 \oplus Z_{5^2} \oplus Z_5$, $(Z_2)^2 \oplus Z_3 \oplus Z_5 \oplus Z_5 \oplus Z_5$

Invariant Factors: Z_{1500}, $Z_{300} \oplus Z_5$, $Z_{60} \oplus Z_5 \oplus Z_5$, $Z_{750} \oplus Z_2$, $Z_{150} \oplus Z_{10}$, $Z_{30} \oplus Z_{10} \oplus Z_5$

(20) Assume that g is the generator of G. Define a map $\mathbb{Z}[x] \to \mathbb{Z}G$ by $f(x) \to f(g)$. This is a "substitution" homomorphism which has been seen before as a ring homomorphism. It is surjective by the definition of the group algebra as the set of all linear integral combinations of the elements of G, which in this case consists of the powers of g. Now the kernel of this homomorphism contains x^{n-1} since $g^n = 1$. We thus obtain a ring homomorphism $\mathbb{Z}[x]/(x^n - 1) \to \mathbb{Z}G$. We now see that this map is $1-1$ since every element of $\mathbb{Z}[x]/(x^n - 1)$ is uniquely represented as a polynomial of degree less than or equal to $n-1$ mod $x^n - 1$ and every element of $\mathbb{Z}G$ is uniquely represented as a linear combination of $1, g, ..., g^{n-1}$.

(21) We define a bilinear map $I \times I \to R$ by $(a, b) \to ab$. As usual multiplication gives a bilinear map. This induces a homomorphism $I \otimes_R I \to R$ given by $a \otimes b \to ab$ and so in general $\sum_{i=1}^n a_i \otimes b_i \to \sum_{i=1}^n a_i b_i$. Since $\sum_{i=1}^n a_i b_i \neq 0$ implies the element mapping into it cannot be zero we see $\sum_{i=1}^n a_i \otimes b_i \neq 0$, the contrapositive of what was asked.

(22) (a) Consider the projection $M \to M/N$ is clearly surjective. So any chain of submodules in M/N comes from a chain of submodules of M. As M is Noetherian, M/N is also noetherian.

(b) Assume that S is a finitely generated Z-module. Then every submodule is finitely generated and so each ideal is finitely generated as we can always view and ideal as a submodule. Let $I_1 \subseteq I_2 \subseteq \cdots$ be a chain of ideals and let $I = \cup I_i$. Note that I is an ideal. But I is finitely generated as a modue by say $a_1, ..., a_n$. Since $a_i \in N$ for all i, each a_i lies in one of the ideals in the chain, say

I_{j_i}. Let $m = \max\{j_1, ..., j_n\}$. Then $a_i \in I_m$ for all i so the ideal they generate is contained in I_m, i.e. $I \subseteq I_m$. This implies $I_m = I = I_k$ for all $k \geq m$ which proves noetherian.

(c)Take $\mathbb{Q}$ as a $\mathbb{Z}$-module.

(24) (a) Let $N = \mathbb{Z}$ and take the abelian groups $A = \mathbb{Z}$, $B = \mathbb{Z}$, and $C = \mathbb{Z}_4$. Then the sequence

$$0 \longrightarrow A \overset{\cdot 4 = f}{\longrightarrow} B \overset{\overline{4} = g}{\longrightarrow} C \longrightarrow 0$$

is clearly exact. Now we consider the sequence

$$0 \longrightarrow \mathrm{Hom}(\mathbb{Z}_4, \mathbb{Z}) \longrightarrow \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \overset{\cdot 4}{\longrightarrow} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \longrightarrow 0$$

which is isomorphic to

$$0 \to 0 \to \mathbb{Z} \overset{h = \cdot 4}{\to} \mathbb{Z} \to 0$$

but we then have $\mathbb{Z}/\operatorname{Im}(h) \cong \mathbb{Z}_4$ and thus is not exact as $\ker \neq im$ there.

(b) If we take N to be an injective $\mathbb{Z}$-module or if you just want to think of it as a group then it will work for any divisible abelian group. To make the sequence exact we are asking that just like in the Tor computation that $Tor_1 = 0$ we are now taking homs instead of tensor products and making the same construction. Just as finding $Tor(P, M)$ for a projective (in this case free) $=0$ for all $n \geq 1$ as a resolution for P is $0 \to P \to P \to 0$. A proposition (which is not too hard to prove) in Dummitt and Foote (section 17.1 proposition 9) states that for an R-module Q (or in our case an abelian group) the following are equivalent:

(1) Q is injective (or just a divisible abelian group)

(2) $\mathrm{Ext}^1_R(A, Q) = 0$ for all R-modules A

(29) If $f : A \to A$ is an R-module homomorphism such that $ff = f$, then $A = \ker f \oplus \operatorname{Im} f$.

1. **Solution 2** *I claim that* $\ker f = \operatorname{Im}(Id - f)$ *where* $Id - f : A \to A$. " $\subseteq$ " *Let* $a \in \ker f$. *Then* $f(a) = 0$, *so* $a - f(a) = a$. *So* $a = (Id - f)(a)$, *i.e.* $a \in \operatorname{Im}(Id - f)$.

   " $\supseteq$ " *Let* $a \in \operatorname{Im}(Id - f)$. *Then* $a = (Id - f)(b)$ *for some* $b \in B$. *Then* $f(a) = f(Id - f)(b) = f(b - f(b)) =$

   $f(b) - f(f(b)) = f(b) - f(b) = 0$

(31) Describe all semisimple rings of order 144.

1. **Solution 3** *As any finite ring is Artinian. Therefore our structure theorem says that* $R \cong I_1 \oplus \cdots \oplus I_n$, *i.e. R is isomorphic to the direct sum of finitely many ideals, each* I_i *being represented by and* $n_j \times n_j$ *matrix over a skew field. However a theorem of Weddeburn says all finite division rings must be fields.* $144 = 2^4 3^2$. *So* $M \cong M_2(F_2) \oplus F_9$, $M_2(F_2) \oplus F_3 \oplus F_3$, $F_{16} \oplus F_{19}$, ... *there are 12 total, 10 are commutative and* 2 *are not.*

(32) Determine the abelian group $G = (a, b : 30a = 42b = 70(a + b) = 0)$ as a direct sum of cyclic groups.

$\begin{pmatrix} 30 & 0 \\ 0 & 42 \\ 70 & 70 \end{pmatrix} \to \begin{pmatrix} 2 & 0 \\ 0 & 210 \\ 0 & 0 \end{pmatrix}$ and so we get $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{210}$.

(33) If D is a division ring show that all elements, with one exception are quasi-regular. What is the exception?

First note that -1 is the element of r that is not q.r. as $-1 * r = -1 + r + (-1) r = -1 \neq 0$. Now take $b \neq -1$ which implies $b + 1 \neq 0$. So there is an $a \in R$ such that $a (b + 1) = 1$ implies $ab + a = 1$ implies $a - 1 + ab = 0$ implies $a - 1 + b + (a - 1) b = 0$ implies $(a - 1) * b = 0$ and thus b is l.q.r. and by a similar argument we can show it is r.q.r. and thus is q.r.

(34) Determine the Galois group over $\mathbb{Q}$ of $f(x) = x^3 - 3x + 1$.

First note that $f(x)$ is irreducible by noting no roots over $\mathbb{Q}$ as no roots over $\mathbb{Z}$, or reduce mod 2, or find $f(x + 1)$ and use Eisenstein. We now can compute the determinant and get $-4p^3 - 27q^2 = 108 - 27 = 81$, a perfect square. As $f(x)$ is irreducible over $\mathbb{Q}$, we get A_3.

(35) If $R = 2\mathbb{Z}$, the ring of even integers, show that the ideal $I = (6)$ is modular but the ideal $J = (4)$ is not modular.

Modular means there is an $e \in R$ such that for all $r \in R$, $r - re \in I$. Take $e = 4 \in R$. All even integers can be written as $2x$. So $r - r \cdot 4 = 2x - 2x(4) = -6x \in (6)$. All elements of (4) can be written as $4y$ with $y \in \mathbb{Z}$. $2x - 2x(e) = 2x(1 - e)$. So assume $2x(1 - e) = 4y$. As $\mathbb{Z}$ is an ID we have $x(1 - e) = 2y$. As x can be odd, e must be odd and this is a contradiction as $e \in 2\mathbb{Z}$.

(36) True or false

(a) A simple Artinian ring is left noetherian.

(b) The radical of a ring is a radical ring.

Solution: (a) True (b) True

(37) (First I guess I should have said that R is also a finitely generated group. If A is a finitely generated $\mathbb{Z}$-module then we have that

$A \cong \mathbb{Z}^n \oplus \bigoplus_i \mathbb{Z}/(n_i)\mathbb{Z}$ and $R \cong \mathbb{Z}^m \oplus \bigoplus_j \mathbb{Z}/(m_j)\mathbb{Z}$ and so we get

$\mathbb{Z}^{mn} \oplus \bigoplus_i (\mathbb{Z}/(n_i)\mathbb{Z})^m \oplus \bigoplus_j (\mathbb{Z}/(m_j)\mathbb{Z})^n \oplus \bigoplus_{i,j} \mathbb{Z}_{\gcd(n_i, m_j)}$

(38) Describe all semisimple rings having 10,000 elements.

$10,000 = 2^4 5^4$ and so some possibilities are by the usual theorems

1. **Solution 4** $M_2(\mathbb{F}_2) \times M_2(\mathbb{F}_5)$, $M_2(\mathbb{F}_2) \times \mathbb{Z}_{5^4}$, ... , $\mathbb{Z}_2^4 \times \mathbb{Z}_5^4$.