Kayla Orlinsky

Algebra Exam Fall 2018

Problem 1. Let $\mathbb{F}_p$ be a finite field with p elements, and consider the group $GL_n(\mathbb{F}_p)$. Write down the order of $GL_n(\mathbb{F}_p)$ and a Sylow p-subgroup.

Solution. If $X \in GL_n(\mathbb{F}_p)$, then X must be an invertible $n \times n$ matrix with elements in $\mathbb{F}_p$. Namely, X must have linearly independent columns. If $[x_i]$ are the columns of X, then the first column x_1 can by anything except the zero vector, which vies $p^n - 1$ possible options.

The second column x_2 can be anything but a multiple of the first column. So once x_1 is chosen, $x_2 \neq ax_1$, there are p vectors that x_2 cannot be. Namely, there are $p^n - p$ choices for x_2.

Inductively, we can see that there are $p^n - p^k$ choices for x_{k+1} $0 \leq k \leq n-1$.

Thus,

$$|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

***Although it was not asked, we can note that the determinant function

$$\det : GL_n(\mathbb{F}_p) \to \mathbb{F}_p^*$$

is a surjective homomorphism with kernel $SL_n(\mathbb{F}_p)$. Namely,

$$\left| \frac{GL_n(\mathbb{F}_p)}{SL_n(\mathbb{F}_p)} \right| = |\mathbb{F}_p^*| = p - 1$$

and so

$$|SL_n(\mathbb{F}_p)| = \frac{|GL_n(\mathbb{F}_p)|}{p-1}.$$

We further note that if instead we were interested in $\mathbb{F}_q$ where $q = p^k$, then we could replace p with q in all instances and achieve the same results.

Finally, we claim that if P that set of all upper triangular matrices with 1 down the main diagonal forms a Sylow p-subgroup.

First, there are

$$\frac{n^2 - n}{2}$$

entries in matrices of this form, and p possible choices for each entry, so $|P| = p^{(n-1)n/2}$.

Since Sylow p-subgroups have order $p^{n-1}p^{n-2}\cdots p$ or $p^{(n-1)n/2}$, we have that P has the right size.

Thus, if P is a subgroup it is a Sylow p-subgroup.

However, this is trivial since products of upper triangular matrices are upper triangular and inveres of upper triangular matrices are also upper triangular.

Since $\det(Y) = 1$ if $Y \in P$, we also get that $Y^{-1} \in P$. Note that the determinant of an upper triangular matrix is the prdouct of the entries down the main diagonal.

Thus, P is a subgroup and so it is a Sylow p-subgroup. ✌

Problem 2. Prove that there are no simple groups of order 600.

Solution. Let G be a group of order $600 = 10 \cdot 10 \cdot 6 = 2^3 \cdot 3 \cdot 5^2$.

Then, by Sylow Theorems, $n_5 \equiv 1 \mod 5$ and $n_5 | 2^3 \cdot 3$.

Namely, $n_5 = 1, 6$.

Now, if G is simple, then $n_5 = 6$ and so since Sylow 5-subgroups are conjugates, G can act on its Sylow 5 subgroups by conjugation.

This action defines a homomorphism

$$\varphi : G \to S_6$$

where $\varphi(g) = \sigma_g$ and $\sigma_g : \mathrm{Syl}_5(G) \to \mathrm{Syl}_5(G)$ with $\sigma_g(P_5) = gP_5g^{-1}$ and P_5 a Sylwo 5-subgroup of G.

Now, since kernels of homomorphisms are normal subgroups in the domain, $\ker\varphi$ must be trivial. Namely, φ must be an embedding.

However, $|S_6| = 6! = 720$, and since $|G| = 600$ which does not divide 720, there cannot be any isomorphic copies of G inside S_6.

This is a contradiction and so G cannot be simple. ✌

Problem 3. Prove that $\mathbb{Z}[\sqrt{10}]$ is integrally closed in its field of fractions, but not a UFD.

Solution. Let $a+b\sqrt{10}\in\mathbb{Q}[\sqrt{10}]$. Note that this is the field of fractions of $\mathbb{Z}[\sqrt{10}]$ since for $s,t,p,q\in\mathbb{Z}$,

$$\frac{s+t\sqrt{10}}{p+q\sqrt{10}}=\frac{(s+t\sqrt{10})(p-q\sqrt{10})}{p^2-10q^2}\in\mathbb{Q}[\sqrt{10}].$$

Then we note that $m_{a,b}(x)=(x-a-b\sqrt{10})(x-a+b\sqrt{10})=x^2-2ax+a^2-10b^2$ is the minimal polynomial of $a+b\sqrt{10}$ over $\mathbb{Q}$. $m_{a,b}(x)$ is irreducible over $\mathbb{Q}$ and so it is also irreducible over $\mathbb{Z}$.

Now, if $a+b\sqrt{10}$ is integral over $\mathbb{Z}[\sqrt{10}]$ it satisfies $f(x)$ a monic irreducible polynomial with coefficients in $\mathbb{Z}[\sqrt{10}]$. Since $f(x)$ is irreducible, over $\mathbb{Z}[\sqrt{10}]$, by Gauss' Lemma, $f(x)$ is also irreducible over $\mathbb{Q}[\sqrt{10}]$. However, then $m_{a,b}(x)$ must divide $f(x)$ in $\mathbb{Q}[\sqrt{10}]$ and so by irreducibly, $f(x)=um_{a,b}(x)$ for u a unit. Namely, $m_{a,b}(x)$ has coefficients in $\mathbb{Z}$.

Therefore, $a+b\sqrt{10}$ is integral over $\mathbb{Z}[\sqrt{10}]$ if and only if $m_{a,b}(x)$ has coefficients in $\mathbb{Z}$.

Now, if $-2a\in\mathbb{Z}$ and $a^2-10b^2\in\mathbb{Z}$ then

$$4(a^2-10b^2)=(2a)^2-10(2b)^2\in\mathbb{Z}$$

however, $2a\in\mathbb{Z}$ and so $10(2b)^2\in\mathbb{Z}$.

Since 10 is squarefree, it cannot be that $(2b)^2\notin\mathbb{Z}$ so $2b\in\mathbb{Z}$ as well.

Finally, $4(a^2-10b^2)=(2a)^2-10(2b)^2=4k \qquad k\in\mathbb{Z}$ and so $(2a)^2=2(5(2b)^2+2k)$, since $2b\in\mathbb{Z}$ we get that $(2a)^2$ is even. However, if $2|(2a)^2$ then $2|(2a)$. Namely, $a\in\mathbb{Z}$.

Immediately then, it must be that $b\in\mathbb{Z}$ since again, 10 is squarefree and $10b^2\in\mathbb{Z}$.

Thus, $\mathbb{Z}[\sqrt{10}]$ is integrally closed.

Now, let $N(a+b\sqrt{10})=a^2-10b^2$ be the norm function on $\mathbb{Z}[\sqrt{10}]$. Note that

$$N(xy)=xy\overline{xy}=xy\overline{xy}=x\overline{x}y\overline{y}=N(x)N(y)$$

and that

$$N:\mathbb{Z}[\sqrt{10}]\to\mathbb{Z}.$$

We note that if $N(a+b\sqrt{10})=3$, then

$$\begin{aligned}
a^2-10b^2 &= 3\\
a &= 2n+1 \qquad n\in\mathbb{Z}\\
(2n+1)^2-10b^2 &= 3\\
4n^2+4n+1-10b^2 &= 3\\
2n^2+2n-1 &= 5b^2\\
b &= 2k+1 \qquad k\in\mathbb{Z}\\
4n^2+4n+1-10(2k+1)^2 &= 3\\
4n^2+4n+1-10(4k^2+4k+1) &= 3\\
4[n^2+n-10k^2-10k]-9 &= 3\\
n^2+n-10k^2-10k &= 3\\
n^2+n &\equiv 1 \mod 2
\end{aligned}$$

and this is not possible since if n is odd, then n^2+n is even, and if n is even, then $n^2+n\equiv 0 \mod 2$.

Thus, $N(x)\neq 3$ for all $x\in\mathbb{Z}[\sqrt{10}]$.

Namely, since $N(3)=9$, if 3 were reducible, then we would get

$$N(3)=9=N(ab)=N(a)N(b).$$

However, since $N(a)\neq 3$, and $N(b)\neq 3$, then either a or b is a unit.

Therefore, 3 is irreducible.

Now, since in $\mathbb{Z}[\sqrt{10}]$,

$$9=3\cdot 3=-(1-\sqrt{10})(1+\sqrt{10}),$$

if $\mathbb{Z}[\sqrt{10}]$ were a UFD, then 3 would be prime, since it is irreducible.

Namely, 3 must divide $1+\sqrt{10}$.

However, if

$$1+\sqrt{10}=3(a+b\sqrt{10}) \implies 1=3a, 1=3b$$

which is not possible for $a,b\in\mathbb{Z}$.

Thus, 3 is not prime and so $\mathbb{Z}[\sqrt{10}]$ is not a UFD. ✌

Problem 4. If F is a field and E/F is an extension, then an element $a \in E$ will be called abelian if $\text{Gal}(F[a]/F)$ is an abelian group. Show taht the set of abelian elements of E is a subfield of E containing F.

Solution. Let S be the set of abelian elements of E. We need to show that S is a subgfield of E and that it contains F.

The latter is immediate since if $a \in F$ then $F[a] = F$ and so

$$\text{Gal}(F[a]/F) = \text{Gal}(F/F) = \{e\}.$$

And since the trivial group is abelian, $a \in S$.

Thus, S certainly contains 0 and 1 since $0 \in F$ and $1 \in F$.

Furthermore, S contains inverses since $F[a] = F[a^{-1}]$ and so if $a \in S$ then

$$\text{Gal}(F[a]/F) = \text{Gal}(F[a^{-1}]/F) \qquad \text{is abelian.}$$

and so $a^{-1} \in S$.

Finally, we check that S is closed under addition and multiplication.

Let $a, b \in S$. We prove a small claim.

Claim 1. There is an injective homomorphism

$$\varphi : \text{Gal}(F[a,b]/F) \to \text{Gal}(F[a]/F) \times \text{Gal}(F[b]/F).$$

Proof. Let $\varphi(\sigma) = (\sigma|_{F[a]}, \sigma|_{F[b]})$ which is the restriction of σ to $F[a]$ and $F[b]$ respectively.

Note that φ is well defined since by assumption, $F[a,b]/F$, $F[a]/F$ and $F[b]/F$ are Galois extensions, and so any automorphism $\sigma : F[a,b] \to F[a,b]$ must preserve the subfields $F[a]$ and $F[b]$.

Therefore, φ is trivially a homomorphism since

$$(\sigma \circ \tau)|_{F[a]} = \sigma(\tau|_{F[a]}) = \sigma|_{F[a]}(\tau|_{F[a]}) = \sigma|_{F[a]} \circ \tau|_{F[a]}$$

because $\tau|_{F[a]} : F[a] \to F[a]$.

Similarly for $(\sigma \circ \tau)|_{F[b]}$.

Finally, if $\varphi(\sigma) = (\text{Id}, \text{Id})$ then σ acts as the identity on $F[a]$ and on $F[b]$ so it must be the identity on $F[a,b]$.

Thus, $\ker \varphi = 0$.

Therefore, there is an isomorphic copy of $\text{Gal}(F[a,b]/F)$ in $\text{Gal}(F[a]/F) \times \text{Gal}(F[b]/F)$. ✌

Since $a, b \in S$, $\text{Gal}(F[a]/F) \times \text{Gal}(F[b]/F)$ is a product of two abelian groups and is therefore abelian.

Finally, $\text{Gal}(F[a,b]/F)$ is therefore abelain and so all subgroups are normal. Therefore, since $F[a-b] \subset F[a,b]$ and $F[ab] \subset F[a-b]$ are both subfields, by the fundamental theorem of Galois theory $F[a-b]/F$ is a Galois extension with abelian Galois group since it is a subgroup of $\text{Gal}(F[a,b]/F)$.

Therefore $a - b \in S$ and similarly $ab^{-1} \in S$.

Thus, S is a subfield of E containing F. ✌

Problem 5. Let K be the splitting field of $x^4 - 2 \in \mathbb{Q}[x]$. Prove that $\text{Gal}(K/\mathbb{Q})$ is D_8 the dihedral group of order 8, (i.e., the group of isometries of the square). Find all subfields of K that have degree 2 over $\mathbb{Q}$.

Solution. Let K be the splitting field of

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - 2^{1/4})(x + 2^{1/4})(x - 2^{1/4}i)(x + 2^{1/4}i)$$

Then $K = \mathbb{Q}(2^{1/4}, i)$ clearly.

Now, we note that $2^{1/4}$ has minimal polynomial $x^4 - 2$ over $\mathbb{Q}$ and i has minimal polynomial $x^2 + 1$. Since $i \notin \mathbb{Q}(2^{1/4})$ because it is not in $\mathbb{R}$ and $\mathbb{Q}(2^{1/4}) \subset \mathbb{R}$, then this must the minimal polynomial of i over $\mathbb{Q}(2^{1/4})$.

Namely,

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(2^{1/4})][\mathbb{Q}(2^{1/4}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Now, because $x^4 - 2$ is separable and K is its splitting field, $K/\mathbb{Q}$ is Galois.

Therefore, $G = \text{Gal}(K/\mathbb{Q})$ is of order 8.

Let $\sigma \in G$ be defined by $\sigma(2^{1/4}) = 2^{1/4}i$ and $\sigma(i) = i$.

Then σ clearly has order 4 since

$$\sigma^4(2^{1/4}) = \sigma^3(2^{1/4}i) = \sigma^2(-2^{1/4}) = \sigma(-2^{1/4}i) = 2^{1/4}.$$

Let $\tau \in G$ be defined by $\tau(2^{1/4}) = 2^{1/4}$ and $\tau(i) = -i$. Then τ has order 2.

Finally,

$$\sigma(\tau(2^{1/4}i)) = \sigma(-2^{1/4}i) = 2^{1/4}$$
$$\tau(\sigma(2^{1/4}i)) = \tau(-2^{1/4}) = -2^{1/4}$$

and so σ and τ do not commute.

Therefore, G is non-abelian and so clearly

$$G \cong D_8 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle.$$

Now, the subfields F of K which have degree 2 over $\mathbb{Q}$ correspond by the Galois Correspondence Theorem, to the subgroups of G which have index 2. Namely, to the subgroups of G of order 4.

Note that $\langle \sigma \rangle$, $\langle \tau, \sigma^2 \rangle$, $\langle \tau\sigma, \sigma^2 \rangle$ all have order 4.

One can check that these are the only subgroups of order 4. Namely, if H were another subgroup of order 4 containing σ or σ^3, then H would be the first subgroup.

Similarly, if H contains σ^2, then it must contain at least one of the $\tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3$ and these would all result in either the second or third subgroup listed.

Thus, no such fourth H exists.

Finally, σ fixes i and so

$$\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q}(i)) \rightsquigarrow \mathbb{Q}(i)$$

σ^2 fixes i and $\sqrt{2}$ since

$$\sigma^2((2^{1/4})^2) = \sigma((2^{1/4}i)^2) = \sigma(-(2^{1/4})^2) = -(2^{1/4}i)^2 = (2^{1/4})^2$$

, and τ fixes $\sqrt{2}$, so

$$\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q}(\sqrt{2})) \rightsquigarrow \mathbb{Q}(\sqrt{2})$$

and $\tau\sigma$ and σ^2 both fix $\sqrt{2}i$ since

$$\tau\sigma((2^{1/4})^2 i) = \tau(-(2^{1/4})^2 i) = (2^{1/4})^2 i$$

and σ^2 fixes $\sqrt{2}$ and i, so

$$\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q}(i\sqrt{2})) \rightsquigarrow \mathbb{Q}(i\sqrt{2}).$$

✌

Problem 6. Let F be a field, and suppose A is a finite-dimensional F-algebra. Write $[A, A]$ for the F-subspace of A spanned by elements of the form $ab - ba$ with $a, b \in A$. Show that $[A, A] \neq A$ in the following two cases:

(a) When A is a matrix algebra over F;

(b) When A is a central division algebra over F.

(Recall that a division algebra over F is called central if its center is isomorphic with F).

Solution.

(a) Let $A = M_n(F)$ the algebra of $n \times n$ matrices with coefficients in F.

Now, we note that

$$\mathrm{tr}(XY - YX) = \mathrm{tr}(XY) - \mathrm{tr}(YX) = \mathrm{tr}(XY) - \mathrm{tr}(XY) = 0$$

where $\mathrm{tr}(X)$ is the trace of X.

Therefore, $[A, A] \subsetneq A$ since there are clearly matrices in A with nonzero trace.

(b) Let A be a central division algebra over F.

We prove several small claims.

> **Claim 2.** The center with A, B both F-algebras (F a field), $Z(A \bigotimes_F B) = Z(A) \bigotimes_F Z(B)$.
>
> *Proof.* $\boxed{\subset}$ Let $x \in Z(A \bigotimes_F B)$, then x commutes with all elementary tensors. WLOG we can write $x = \sum_{j=1}^n \alpha_j (a_j \otimes b_j)$ where the a_j and b_j are linearly independent, then
>
> $$\begin{aligned} x(a \otimes 1) &= \sum_{j=1}^n \alpha_j (a_j \otimes b_j)(a \otimes 1) \\ &= \sum_{j=1}^n \alpha_j (a_j a \otimes b_j) \\ &= (a \otimes b)x \\ &= \sum_{j=1}^n \alpha_j (a a_j \otimes b_j) \end{aligned}$$
>
> and so
>
> $$\sum_{j=1}^n \alpha_j ((a_j a - a a_j) \otimes b_j) = 0$$

and since the b_j are linearly independent, this forces $a_j a - a a_j = 0$ for all j.

Thus, $a_j \in Z(A)$ for all j.

Similarly, checking $x(1 \otimes b)$ we get that $b_j \in Z(B)$ for all j.

Thus, $x \in Z(A) \bigotimes_F Z(B)$

$\boxed{\supset}$ This is immediate since if $x \in Z(A) \bigotimes_F Z(B)$ then $x = \sum_{j=1}^n \alpha_j(a_j \otimes b_j)$ with $a_j \in Z(A)$ and $b_j \in Z(B)$ so x will commute with all elementary tensors since

$$x(a\otimes b) = \sum_{j=1}^n \alpha_j(a_j \otimes b_j)(a\otimes b) = \sum_{j=1}^n \alpha_j(a_j a \otimes b_j b) = \sum_{j=1}^n \alpha_j(a a_j \otimes b b_j) = (a\otimes b)x.$$

Therefore, $x \in Z(A \bigotimes_F B)$ ✌

Claim 3. If A is a central simple algebra, and B is simple then $A \bigotimes_F B$ is simple where F is a field and A, B are F-algebras.

Proof. Let I be an ideal of $A \bigotimes_F B$.

Then there exists an $x \in I$ with $x = \sum_{j=1}^n \alpha_j(a_j \otimes b_j)$ where n is minimal and the b_j are linearly independent.

Then $a_j \neq 0$ for all j and so the two sided ideal $I_1 = (a_1)$ is a nonzero ideal of A, so namely, $I_j = A$ since A is simple.

Therefore, $1 = t_1 a_1 s_1$ for some $t_1, s_1 \in A$.

Thus,

$$x' = (t_1 \otimes 1)x(s_1 \otimes 1) = \alpha_1(1 \otimes b_1) + \sum_{j=2}^n \alpha_j(t_1 a_j s_1 \otimes b_j) \in I$$

since I is a two sided ideal.

Now, let $a \in A$ be arbitrary, then

$$x_0 = (a \otimes 1)x' - x'(a \otimes 1) = \sum_{j=2}^n \alpha_j(a t_1 a_j s_1 - t_1 a_j s_1 a \otimes b_j)$$

which is in I and is of length strictly smaller than x. Thus, $x_0 = 0$ and so because the b_j are linearly independent, this forces $a t_1 a_j s_1 - t_1 a_j s_1 a = 0$ for all j. Therefore, since a was arbitrary, $t_1 a_j s_1 \in Z(A) = F$ because A is central.

However, then $x' = 1 \otimes b$ for some $b \in B$.

However, then $1 \otimes (b) \subset I$ where (b) is a two sided ideal of B. However, since B is also simple, $(b) = B$ and so $1 \otimes B \subset I$.

Therefore, $(A \otimes 1)(1 \otimes B) = A \otimes B \subset I$

So $A \bigotimes_F B$ is simple. ✌

Finally, let $\overline{F}$ be the algebraic closure of F. Let $C = A \otimes_F \overline{F}$. From **Claim 2** and **Claim 3**, C is simple and has center $F \otimes_F \overline{F} = \overline{F}$.

Therefore, by Artin-Wedderburn, $C = M_n(D_i)$ for some D_i division ring over $\overline{F}$. However, since $Z(D_i) = \overline{F}$, and $\overline{F}$ is algebraically closed, $D_i = \overline{F}$. Note D_i is finite dimensional over $\overline{F}$ by Artin-Wedderburn, and so it must be an algebraic extension, however $\overline{F}$ is algebraically closed so $D_i = \overline{F}$.

Thus, $C = M_n(\overline{F})$ and so by (a), $[C, C] \neq C$.

Since

$$\begin{aligned}
[C, C] &= [A \otimes_F \overline{F}, A \otimes_F \overline{F}] \\
&= \{\text{linear combinations of } (a \otimes f)(b \otimes g) - (b \otimes g)(a \otimes f)\} \\
&= \{\text{linear combinations of } ab \otimes fg - ba \otimes gf\} \\
&= \{\text{linear combinations of } ab \otimes fg - ba \otimes fg\} \\
&= \{\text{linear combinations of } (ab - ba) \otimes fg)\} \\
&= [A, A] \otimes_F \overline{F} \neq A \otimes_F \overline{F}
\end{aligned}$$

it must be that $[A, A] \neq A$.

✌

Problem 7. If $\varphi : A \to B$ is a surjective homomorphism of rings, show that the image of the Jacobson radical of A under φ is contained in the Jacobson radical of B.

Solution. First, let M be a maximal ideal of A. Let $\varphi(M) \subset N$ where $N \subset B$ is maximal.

Then we can define

$$\tilde{\varphi} : A \to B/N$$

defined by $\tilde{\varphi}(a) = \varphi(a) + N$.

Clearly $\tilde{\varphi}(M) \subset 0$ and so $M \subset \ker(\tilde{\varphi})$. Therefore, either $M = \ker \tilde{\varphi}$ or $\ker \tilde{\varphi} = A$.

In the first case, we get that $\varphi(M) = N$ since if $x \in N$, then φ is surjective so there exists $a \in A$ with $\varphi(a) = x$, namely, $\tilde{\varphi}(a) = 0$ and so $a \in M$.

In the second case, we get that $N = B$, else we could take $1 \in B \backslash N$ and again, there would exist some $a \in A$ such that $\tilde{\varphi}(a) = 1 + N \neq 0$.

Namely, φ sends maximal ideals to maximal ideals.

Therefore,

$$\begin{aligned}
\varphi(J(A)) &= \varphi\left(\bigcap_{M \text{ max } \subset A} M\right) \\
&= \bigcap_{M \text{ max } \subset A} \varphi(M) \\
&\subset \bigcap_{N \text{ max } \subset B} N \\
&= J(B)
\end{aligned}$$

✌