ALGEBRA I. TAKE-HOME FINAL.

Instructions: Do any 8 of these 13 questions and no more. Return your solutions to me in my office between 2 - 3 pm on Thursday, Dec 20 or email them to me by that time. Late exams will not be accepted. You may not work with others. Use your class notes, the class texts (Dummit & Foote, Lang) and no other sources. Each question is worth 10 points. Detailed proofs must be given - points will be lost if arguments are not fully justified. State any major results you use. Please email me if you have any questions about the exam.

#1 Let Q_8 be the quaternion group of order 8.
  (a) Show explicitly that Q_8 is isomorphic to a subgroup of S_8.
  (b) Draw the lattice of subgroups for Q_8.
  (c) Prove that Q_8 is not isomorphic to a subgroup of S_7. [If Q_8 acts on a set A of order $\leqslant 7$ show that the stabilizer of any $a \in A$ must contain the subgroup $\langle -1 \rangle$.]

#2 (a) Prove that a group of order 160 is not simple.
  (b) Prove that a group of order pqr is not simple for primes $p < q < r$.

#3 (a) Use Euler's Theorem to find the last 2 digits of $7^{7^{7^{100}}}$.
  (b) Find the number of non-isomorphic abelian groups of order 337500.

#4 Let X be a nonempty set with $\mathcal{P}(X)$ its power set. For $A, B \in \mathcal{P}(X)$, define $A + B$ as the symmetric difference of A and B and define $A \cdot B$ as their intersection.
  (a) Prove that these operations make $\mathcal{P}(X)$ into a commutative, Boolean ring with identity. (A ring is Boolean if $r^2 = r$ for all its elements r.)
  (b) Give an example of a nontrivial ideal I in $\mathcal{P}(X)$ and describe the quotient $\mathcal{P}(X)/I$.

#5 Let ω be the cube root of unity $e^{2\pi i/3}$. Then

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

is called the ring of Eisenstein Integers.
  (a) Prove that $\mathbb{Z}[\omega]$ is a Euclidean Domain with norm $N(a+b\omega) = a^2 - ab + b^2$ $(= |a+b\omega|^2)$.
  (b) Determine, with proof, all the units in $\mathbb{Z}[\omega]$.

#6 Let R be a subring of the commutative ring S with $1 \in R$. Recall that an S-algebra A is a ring, with identity, that is an S-module and satisfies

$$s(ab) = (sa)b = a(sb) \quad \text{for all} \quad s \in S,\ a, b \in A.$$

And recall that an S-algebra homomorphism $\phi : A \to B$ is a ring homomorphism (mapping identity to identity) such that $\phi(sa) = s\phi(a)$ for all $s \in S$ and $a \in A$.
  (a) Prove that $S \otimes_R R[x] \cong S[x]$ as S-modules.
  (b) Prove that $S \otimes_R R[x] \cong S[x]$ as S-algebras.

#7 Let M and N be finitely generated R-modules for R a commutative ring.
  (a) Prove that $M \oplus N$ is a projective R-module if and only if M and N are projective.
  (b) Prove that if M and N are projective then $M \otimes_R N$ is a projective R-module.

Date: Dec 13, 2012.

#8 Prove all parts of the *Lattice Isomorphism Theorem* for groups. Then show how it extends to rings and modules.

#9 Let A be an abelian group, considered as a $\mathbb{Z}$-module.

(a) If A is finitely generated, prove that for some $m \in \mathbb{Z}_{\geqslant 0}$ there is an isomorphism of $\mathbb{Q}$-modules

$$\mathbb{Q} \otimes_{\mathbb{Z}} A \cong \mathbb{Q}^m.$$

(b) If A is finite and p prime, prove that

$$\mathbb{Z}/p^k\mathbb{Z} \otimes_{\mathbb{Z}} A$$

is isomorphic to the Sylow p-subgroup of A for all k large enough.

#10 By using irreducible polynomials over a finite field $\mathbb{F}_p$ for p prime, construct finite fields of the following sizes:

(a) 49.

(b) 8.

(c) Provide generators for the multiplicative parts of each of the fields you constructed in parts (a) and (b).

#11 Let

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0 \tag{1}$$

be a short exact sequence of R-modules.

(a) Let D be an R-module. Prove that the sequence

$$0 \longrightarrow \mathrm{Hom}_R(N, D) \xrightarrow{\phi'} \mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D) \longrightarrow 0, \tag{2}$$

associated to (1), is exact except possibly at $\mathrm{Hom}_R(L, D)$.

(b) Give an example with (1) exact and (2) not exact at $\mathrm{Hom}_R(L, D)$.

(c) Give an example with (1) exact and

$$0 \longrightarrow D \otimes_R L \xrightarrow{1\otimes\psi} D \otimes_R M \xrightarrow{1\otimes\phi} D \otimes_R N \longrightarrow 0$$

not exact at $D \otimes_R L$ for D a right R-module.

#12 Hilbert's Basis Theorem implies that all ideals in $\mathbb{Z}[x]$ are finitely generated. In this question we exhibit ideals in $\mathbb{Z}[x]$ requiring arbitrarily large numbers of generators. Fix a prime p. Let I be the ideal (p, x) and consider I^k for $k \in \mathbb{Z}_{\geqslant 1}$.

(a) Prove that

$$I^k = (p^k,\ p^{k-1}x,\ \ldots,\ px^{k-1},\ x^k).$$

In other words, show I^k is generated by the subset $A_k = \{p^{k-i}x^i\}_{0\leqslant i\leqslant k}$ of $\mathbb{Z}[x]$.

(b) Show that I^k/I^{k+1} is an $\mathbb{F}_p$-module for $\mathbb{F}_p$ the finite field $\mathbb{Z}/p\mathbb{Z}$. So we may think of I^k/I^{k+1} as a vector space over $\mathbb{F}_p$.

(c) Let $\pi : I^k \to I^k/I^{k+1}$ be the projection map. Prove that $\pi(A_k)$ is a basis for I^k/I^{k+1}.

(d) If B_k is any generating set for I^k, show that $\pi(B_k)$ must span I^k/I^{k+1}.

(e) Deduce that I^k cannot be generated by fewer than $k + 1$ generators.

#13 Let V be a vector space over F, not necessarily finitely generated.

(a) Prove that V has a basis. [Use Zorn's Lemma.]

(b) Prove that any linearly independent set in V may be extended to a basis.